Appunti di

ALGEBRA LINEARE

Giovanni Zini

A.A. 2023/2024

Indice

1 Logica e insiemi **7**
1.1 Proposizioni e predicati 7
1.2 Dimostrazioni 12
1.3 Insiemi 14
1.4 Esercizi 19

2 Relazioni e funzioni **25**
2.1 Relazioni 25
2.2 Relazioni di equivalenza 31
2.3 Relazioni d'ordine e reticoli 34
2.4 Funzioni 40
2.5 Esercizi 47

3 Elementi di Calcolo Combinatorio **55**
3.1 Disposizioni, permutazioni, combinazioni 55
3.2 Alcune tecniche di conteggio 59
3.3 Applicazioni del principio di inclusione-esclusione 62
3.4 Esercizi 66

4 Operazioni e Strutture Algebriche **75**
4.1 Gruppi, Anelli, Domini, Campi 75
4.2 Elementi primi, elementi irriducibili, MCD e mcm 78
4.3 Esercizi 80

5 L'anello $\mathbb{Z}$ dei numeri interi **83**
5.1 Teorema fondamentale dell'aritmetica 83

5.2 Alcuni criteri di divisibilità 87
5.3 Algoritmo euclideo e massimo comun divisore 89
5.4 Esercizi 92

6 Polinomi univariati **95**
6.1 Esercizi 101

7 Spazi vettoriali $\mathbb{K}^n$ **105**
7.1 Lo spazio $\mathbb{K}^n$ e i suoi sottospazi vettoriali 105
7.2 Sistemi di generatori, lineare indipendenza, basi 108
7.3 Prodotto scalare standard in $\mathbb{R}^n$ 113
7.4 Esercizi 115

8 Matrici **121**
8.1 Matrici e operazioni 121
8.2 Matrici invertibili 129
8.3 Determinante di una matrice 132
8.4 Rango di una matrice 137
8.5 Esercizi 140

9 Sistemi Lineari **145**
9.1 Compatibilità di un sistema lineare 146
9.2 Rappresentazione di sottospazi vettoriali di $\mathbb{K}^n$ 148
9.3 Metodi di risoluzione per sistemi lineari 150
9.4 Sistemi Lineari Parametrici 153
9.5 Esercizi 155

10 Funzioni lineari **171**
10.1 Definizioni 171
10.2 Teoremi fondamentali 173
10.3 Isomorfismi 175
10.4 Esercizi 176

11 Autovalori e diagonalizzazione **189**
11.1 Autovalori e autovettori 189
11.2 Matrici diagonalizzabili 192

11.3 Matrici reali ortogonalmente diagonalizzabili 194
11.4 Esercizi 196

Capitolo 1

Logica e insiemi

1.1 Proposizioni e predicati

Definizione 1.1. *Una* proposizione *è una affermazione che è vera oppure è falsa, ma non contemporaneamente vera e falsa.*

Osservazione 1.2. *Il* valore di verità *di una proposizione è vero (V) oppure falso (F). Se si rappresenta il valore di verità con un bit, si denota vero con* 1*, e falso con* 0*.*

Esempio 1.3. *"L'Europa è un continente" è una proposizione. "1+1 è uguale a 3" è una proposizione. "x è maggiore di* 2*" non è una proposizione.*

Si possono formare *proposizioni composte* a partire da altre proposizioni, tramite alcuni *connettivi logici.*

Definizione 1.4. *Date due proposizioni p e q:*

- *La* negazione *di p è la proposizione* $\neg p$ *("non p", "NOT p", indicata anche con* $\overline{p}$*), che è vera quando p è falsa e falsa quando p è vera.*
- *La* congiunzione *di p e q è la proposizione* $p \wedge q$ *("p" e "q", "p AND q"), che è vera quando p e q sono emtrambi vere, falsa altrimenti.*
- *La* disgiunzione *di p e q è la proposizione* $p \vee q$ *("p o q", "p OR q", "p VEL q"), che è falsa quando p e q sono entrambi false, vera altrimenti.*
- disgiunzione esclusiva *di p e q è la proposizione* $p \dot{\vee} q$ *(*$p \oplus q$*, "p XOR q", "p AUT q"), che è vera quando esattamente una tra p e q è vera, falsa altrimenti.*

- *L'*implicazione $p \Longrightarrow q$ *("se p allora q", "p implica q", indicata anche con $p \longrightarrow q$) è falsa quando p è vera e q è falsa, vera altrimenti.*

- *La* coimplicazione $p \Longleftrightarrow q$ *("p se e solo se q", indicata anche con $p \longleftrightarrow q$) è vera quando p e q hanno lo stesso valore di verità, falsa altrimenti.*

Definizione 1.5. *Una proposizione priva dei connettivi logici sopra descritti si dice* primitiva *(o* elementare*).*

Osservazione 1.6. *L'implicazione $p \Longrightarrow q$ si dice anche nei seguenti modi: "p è condizione sufficente per q", "q è condizione necessaria per p", "p solo se q", "q segue da p".*

La coimplicazione $p \Longleftrightarrow q$ si legge anche "p è condizione necessaria e sufficiente per q".

L'ordine di priorità dei connettivi è il seguente: la negazione ha priorità maggiore; poi la congiunzione; poi le disgiunzioni; poi le implicazioni. Per cambiare la priorità dei connettivi (o anche solo per maggiore chiarezza), si usano le parentesi tonde.

La relazione tra il valore di verità di proposizioni composte e quello delle proposizioni primitive che le compongono si può visualizzare in una *tabella di verità*, come la seguente.

p	q	$\overline{p}$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \Longrightarrow q$	$p \Longleftrightarrow q$
V	V	F	V	V	F	V	V
V	F	F	F	V	V	F	F
F	V	V	F	V	V	V	F
F	F	V	F	F	F	V	V

Definizione 1.7. *Una proposizione composta si dice* tautologia *se è sempre vera indipendentemente dal valore di verità delle proposizioni primitive da cui è composta.*

Una proposizione composta si dice contraddizione *se è sempre falsa indipendentemente dal valore di verità delle proposizioni primitive da cui è composta.*

Due proposizioni p e q si dicono logicamente equivalenti*, e si indica con $p \equiv q$, quando p è vera se e solo se q è vera; cioè, quando la proposizione $p \Longleftrightarrow q$ è vera.*

Esempio 1.8. *Le* leggi de Morgan *sono le due equivalenze logiche*

$$\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}, \qquad \overline{p \vee q} \equiv \overline{p} \wedge \overline{q}.$$

La loro validità si deduce dalle seguenti tavole di verità:

$\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$:

p	q	$p \wedge q$	$\overline{p \wedge q}$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \vee \overline{q}$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

$\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$:

p	q	$p \vee q$	$\overline{p \vee q}$
V	V	V	F
V	F	V	F
F	V	V	F
F	F	F	V

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \wedge \overline{q}$
V	V	F	F	F
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Esempio 1.9. *Data una proposizione del tipo $p \Longrightarrow q$, la sua* contronominale *è la proposizione $\neg q \Longrightarrow \neg p$. Dimostra che le due proposizioni sono logicamente equivalenti.*

Definizione 1.10. *Una proposizione in* forma normale disgiuntiva *(DNF, "disjunctive normal form") consiste in una disgiunzione di congiunzioni, in cui ciascuna congiunzione contiene solo proposizioni primitive o negazioni di proposizioni primitive.*

Una proposizione in DNF si dice in DNF completa se ogni proposizione primitiva coinvolta, o la sua negazione, appare in ognuna delle congiunzioni.

Esempio 1.11. *Siano A, B, C, D prop. primitive. Le seguenti proposizioni sono in DNF:*

$$(A \wedge C) \vee (\neg B \wedge C \wedge D) \vee B, \qquad A, \qquad A \wedge \neg B \wedge \neg C.$$

La seguente proposizione in A, B, C è in DNF completa:

$$(A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C).$$

Le seguenti proposizioni non sono in DNF:

$$\neg(A \wedge B), \qquad \neg(A \vee B) \qquad \neg\neg B, \qquad ((A \vee B) \wedge C) \vee D.$$

Proposizione 1.12. *Ogni proposizione è logicamente equivalente a una proposizione in DNF, ed è anche logicamente equivalente a una proposizione in DNF completa.*

Per passare a una forma normale disgiuntiva tramite equivalenze logiche, si applicano le equivalenze logiche descritte sopra e in Esercizio 1.8; in particolare, le seguenti:

$$A \Rightarrow B \equiv B \vee \neg A, \qquad A \Leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B),$$

$$A \wedge B \equiv B \wedge A, \quad A \vee B \equiv B \vee A, \qquad \neg(A \wedge B) \equiv \neg A \vee \neg B, \quad \neg(A \vee B) \equiv \neg A \wedge \neg B,$$

$$\neg\neg A \equiv A, \qquad A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C), \quad A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C).$$

Esempio 1.13. *Troviamo una forma normale disgiuntiva di* $\neg((p \wedge q) \vee \neg r)$ *:*

$$\neg((p \wedge q) \vee \neg r) \quad \equiv \quad \neg(p \wedge q) \wedge \neg\neg r \quad \equiv \quad (\neg p \vee \neg q) \wedge r \quad \equiv \quad (\neg p \wedge r) \vee (\neg q \wedge r).$$

Passiamo da quest'ultima DNF a una DNF completa:

$$(\neg p \wedge r) \vee (\neg q \wedge r) \quad \equiv \quad \big((\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)\big) \vee \big((p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge r)\big)$$

$$(\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r).$$

Osservazione 1.14. *Una DNF completa di una proposizione* q *si può ottenere nel modo seguente: si costruisce la tabella di verità della proposizione* q*; si fa una disgiunzione dei casi (righe della tabella) in cui* q *è vera; ciascun caso è una congiunzione; in ciascuna congiunzione, per ogni proposizione primitiva* p*, si mette* p *(se* p *è vera in quella riga) oppure* $\neg p$ *(se* p *è falsa in quella riga).*

Si noti che questa maniera è "automatica" e porta sempre al risultato; tuttavia costruire la tabella di verità può essere costoso computazionalmente (se ci sono N *proposizioni primitive, la tabella ha* 2^N *righe).*

Esempio 1.15. *In Esercizio 1.3 si trova la tabella di verità della proposizione* $\neg p \longrightarrow \neg(\neg p \vee \neg q)$*. Dalla tabella di verità si vede che una sua forma normale disgiuntiva completa è* $(p \wedge q) \vee (p \wedge \neg q)$ *(che è poi logicamente equivalente a* p*).*

In maniera simile alla forma normale disgiuntiva, si può definire le proposizioni in forma normale congiuntiva.

Definizione 1.16. *Una proposizione in* forma normale congiuntiva *(CNF, "disjunctive normal form") consiste in una congiunzione di disgiunzioni, in cui ciascuna disgiunzione contiene solo proposizioni primitive o negazioni di proposizioni primitive.*

Una proposizione in CNF si dice in CNF completa se ogni proposizione primitiva o la sua negazione appare in ognuna delle disgiunzioni.

Proposizione 1.17. *Ogni proposizione è logicamente equivalente a una proposizione in CNF, ed è anche logicamente equivalente a una proposizione in CNF completa.*

Passiamo ora a trattare di predicati.

Definizione 1.18. *Un* predicato *è una frase che non ha un valore di verità definito, e dipende da una o più variabili libere.*

Un predicato è indicato con espressioni del tipo $P(x)$*, se dipende da una variabile libera* x*, o* $P(x_1, \ldots, x_n)$*, se dipende da* n *variabili libere* $x_1, \ldots, x_n$*.*

Il predicato $P(x)$ è anche detto il valore in x della "funzione proposizionale" P. Quando le variabili libere vengono sostituite da un valore determinato, il predicato diventa una proposizione con un valore di verità.

Esempio 1.19. *$P(x)$: "x divide 15" è un predicato; quando x assume il valore 7, si ottiene la proposizione (falsa) $P(7)$: "7 divide 15".*

Un'altro modo per formare proposizioni a partire da predicati è tramite i *quantificatori*.

Definizione 1.20. *Il* quantificatore universale *è il simbolo $\forall$, che si legge "per ogni". La proposizione $\forall x\, P(x)$ significa "$P(x)$ è vera per ogni valore di x (nell'universo del discorso)".*

Il quantificatore esistenziale *è il simbolo $\exists$, che si legge "esiste". La proposizione $\exists x\, P(x)$ significa " esiste un valore di x (nell'universo del discorso) tale che $P(x)$ è vera".*

Il simbolo $\exists!$ si legge "esiste ed è unico". La proposizione "$\exists! x\, P(x)$" significa "esiste uno e un solo x (nell'universo del discorso) tale che $P(x)$ è vera".

La negazione $\neg\exists$ del quantificatore esistenziale si scrive solitamente $\nexists$.

Osservazione 1.21. *La proposizione $\forall x\, P(x)$ è falsa quando esiste almeno un valore $\bar{x}$ per cui $P(\bar{x})$ è falsa. Vale la seguente equivalenza logica:*

$$\neg\forall x\, P(x) \;\equiv\; \exists x\, \neg P(x)$$

La proposizione $\exists x\, P(x)$ è falsa quando $P(\bar{x})$ è falsa per ogni valore $\bar{x}$. Vale la seguente equivalenza logica:

$$\neg\exists x\, P(x) \;\equiv\; \forall x\, \neg P(x)$$

L'osservazione precedente mostra che ciascuno dei due quantificatori può essere definito a partire dall'altro; ad esempio, il quantificatore esistenziale può essere definito dando a $\exists x\, P(x)$ il significato $\neg\forall x \neg P(x)$. Inoltre, la proposizione $\exists! x\, P(x)$ può essere definita tramite $\exists x\, (P(x) \wedge \forall y (P(y) \Rightarrow y = x))$.

Esempio 1.22. *Nell'universo dei numeri reali, la proposizione "$\forall x : x < x + 1$" è vera. La proposizione "$\exists x : x < 0$" è vera nell'universo dei numeri interi, ma è falsa nell'universo dei numeri naturali.*

Una proposizione può contenere due o più quantificatori annidati. Ad esempio, consideriamo il predicato $P(x, y)$: "$y < x$", e la proposizione p : "$\forall x \exists y : y < x$". La proposizione p è vera nell'ambiente dei numeri reali. La proposizione p è falsa nell'ambiente dei numeri naturali: infatti esiste un valore di x per cui non è vero che $\exists y : y < x$. Tale valore è $x = 0$.

Osservazione 1.23. *Per trasformare un predicato in una proposizione occorre che tutte le variabili libere siano vincolate, tramite quantificatori o tramite assegnazione di un valore specifico. Perciò l'enunciato di un* teorema *(che è semplicemente una proposizione vera) non può contenere variabili libere.*

1.2 Dimostrazioni

Un *teorema* è una proposizione che si dimostra essere vera. Vengono usati anche altri termini per indicare un teorema, come: *lemma*, se è un teorema più semplice, che serve a dimostrare altri teoremi; o *corollario*, se è un teorema che segue direttamente da un altro teorema.

La verità di un teorema è stabilità tramite una *dimostrazione*. Oltre alle *ipotesi* del teorema stesso e ad altri risultati già noti, una dimostrazione usa: degli *assiomi* (o *postulati*), che non si dimostrano, ma si assumono come veri nella teoria matematica all'interno della quale si sta lavorando; e delle *regole di inferenza*, che permettono di ricavare delle conclusioni a partire da delle ipotesi.

Osservazione 1.24. *Una* teoria assiomatica *può essere* incompleta*: possono esistere enunciati di cui non si può dimostrare né la verità né la falsità a partire da quegli assiomi (cioè, sono enunciati indipendenti da quegli assiomi). Ad esempio: usando come assiomi solo i primi quattro assiomi della geometria euclidea, non si può dimostrare né la verità né la falsità dell'enunciato noto come "quinto postulato di Euclide", o "postulato delle parallele". Allora uno può costruire teorie "più ampie", in cui ai quattro assiomi aggiunge il postulato delle parallele (e ottiene la geometria euclidea), oppure aggiunge la negazione del postulato delle parallele (e ottiene le geometrie non euclidee).*

La cosa più importante di una teoria assiomatica è che sia consistente*, cioè che non sia possibile dimostrare una contraddizione. Se invece è possibile dimostrare sia una proposizione che la sua negazione, la teoria è* inconsistente*.*

Una regola di inferenza si può indicare scrivendo le ipotesi in colonna, e la conclusione sotto una riga orizzontale, con la seguente notazione:

$$\begin{array}{l} p \\ q \\ \hline \therefore\ r \end{array}$$

Ciò significa che dalle ipotesi p e q si può ricavare la conclusione r. Una regola di inferenza è *valida* quando, se le ipotesi sono vere, allora la conclusione è vera; cioè, se è una tautologia

l'implicazione logica che ha come antecedente la congiunzione delle ipotesi e come conseguente la conclusione. Ad esempio, la regola di inferenza sopra è valida se la proposizione $(p \wedge q) \Longrightarrow r$ è una tautologia.

Più in generale, una argomentazione in cui si ricava una conclusione r a partire dalle ipotesi $p_1, \ldots, p_n$ è *valida* se $(p_1 \wedge \cdots \wedge p_n) \Longrightarrow r$ è una tautologia.

Elenchiamo alcune importanti regole di inferenza valide:

$$\therefore \ \frac{p}{p \vee q} \qquad \therefore \ \frac{p \wedge q}{p} \qquad \therefore \ \frac{\begin{array}{l} p \\ q \end{array}}{p \wedge q}$$

$$\therefore \ \frac{\begin{array}{l} p \\ p \Longrightarrow q \end{array}}{q} \quad \text{(“modus ponens”)} \qquad \therefore \ \frac{\begin{array}{l} p \Longrightarrow q \\ \neg q \end{array}}{\neg p} \quad \text{(“modus tollens”)}$$

$$\therefore \ \frac{\begin{array}{l} p \Longrightarrow q \\ q \Longrightarrow r \end{array}}{p \Longrightarrow r} \qquad \therefore \ \frac{\begin{array}{l} p \vee q \\ \neg p \end{array}}{q} \qquad \therefore \ \frac{\begin{array}{l} q \vee p \\ r \vee \neg p \end{array}}{q \vee r} \quad \text{(“risoluzione”)}$$

Altre regole di inferenza (usate implicitamente, e “ovvie”) coinvolgono i quantificatori:

$$\therefore \ \frac{\forall x \ P(x)}{P(c)} \qquad \therefore \ \frac{P(c) \text{ per qualsiasi } c}{\forall x \ P(x)}$$

$$\therefore \ \frac{\exists x \ P(x)}{P(c) \text{ per qualche } c} \qquad \therefore \ \frac{P(c) \text{ per qualche } c}{\exists x \ P(x)}$$

La scelta di una strategia efficace per dimostrare un teorema è in un certo senso “un'arte”. Elenchiamo alcuni esempi di strategie.

- dimostrazione “diretta” di $p \Longrightarrow q$: si mostra che se p è vera allora q è vera.

  Ad esempio, dimostriamo che il quadrato di ogni numero intero pari è pari. Il teorema da dimostrare è: $\forall x \, (D(x) \Longrightarrow D(x^2))$, dove il dominio del discorso è l'insieme dei numeri interi e $D(x)$ è il predicato “x è pari”. Per qualsiasi intero c, supponiamo che $D(c)$ è vera, cioè c è pari. Allora esiste un intero n tale che $c = 2n$. Perciò $c^2 = (2n)^2 = 4n^2 = 2 \cdot 2n^2$ è pari, cioè è vera $D(c^2)$. Quindi $D(c) \Longrightarrow D(c^2)$ è vera per qualsiasi c; dunque $\forall x \, (D(x) \Longrightarrow D(x^2))$.

- dimostrazione “indiretta” di $p \Longrightarrow q$: si mostra in modo diretto la proposizione *contronominale* $\neg q \Longrightarrow \neg p$ (che è logicamente equivalente alla proposizione iniziale).

  Ad esempio, dimostriamo che “dati N numeri interi, se la loro somma è uguale a $N+1$ allora almeno uno dei numeri è maggiore di 1”. Supponiamo che valga la negazione

della tesi, cioè che nessuno degli N numeri sia maggiore di 1. Questo significa che tutti gli N numeri non sono maggiori di 1, e dunque sono tutti minori o uguali a 1. Ne segue che la loro somma è minore o uguale a $1 + \cdots + 1 = N$, e quindi non è vero che la loro somma è $N + 1$.

- dimostrazione per assurdo di una proposizione q : si mostra che $\neg q \implies F$, cioè che assumendo $\neg q$ si ottiene una contraddizione.

  Ad esempio, dimostriamo che esistono infiniti numeri primi positivi. Supponiamo per assurdo che i numeri primi siano in numero finito N, e indichiamoli con $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_N$. Definiamo il numero $M := p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$. Chiaramente M è maggiore di tutti i numeri $p_1, \ldots, p_N$, e quindi per l'assunzione fatta M non è primo. Allora c'è un numero primo p_i che divide M. Poichè p_i divide sia M che $p_1 \cdot \ldots \cdot p_N$, allora p_i divide $M - (p_1 \cdot \ldots \cdot p_N) = 1$. Ma se p_i divide 1, allora p_i non è un numero primo, in contraddizione con quanto assunto prima.

- Dimostrazione "per casi" di una proposizione q : se vale sempre almeno una delle proprietà $p_1, \ldots, p_n$ (cioè se $p_1 \vee \cdots \vee p_n$ è una tautologia), allora basta dimostrare $(p_1 \Rightarrow q) \wedge \cdots (p_n \Rightarrow q)$ (infatti quest'ultima proposizione è equivalente a $(p_1 \vee \cdots \vee p_n) \Rightarrow q$).

  Ad esempio, dimostriamo che ogni numero reale c soddisfa $c^2 \geq 0$. Sappiamo che vale la tautologia $(c = 0) \vee (c < 0) \vee (c > 0)$ (ogni numero è zero, o negativo, o positivo). Se $c = 0$, allora $c^2 = 0 \cdot 0 = 0 \geq 0$; se $c < 0$, allora c^2 è il prodotto di due numeri negativi e quindi $c^2 > 0$, che implica $c^2 \geq 0$; se $c < 0$, allora c^2 è il prodotto di due numeri positivi e quindi $c^2 > 0$, che implica $c^2 \geq 0$.

- dimostrazioni di un "se e solo se" $p \iff q$: si mostra che $p \implies q$ e che $q \implies p$.

- dimostrazione per induzione (studiata nel corso di Analisi Matematica).

1.3 Insiemi

Un insieme è una collezione di oggetti, che sono elementi dell'insieme e appartengono all'insieme. Non possiamo dare una definizione vera e propria, perché nella teoria matematica degli insiemi i concetti di "insieme" e "appartenenza" sono primitivi, cioè non sono definibili in termini di concetti più semplici.

Il predicato "$x \in A$" significa "x appartiene a A", "x è un elemento di A".

Se $p(x)$ è un predicato, indichiamo la proposizione $\exists x((x \in A) \wedge p(x))$ semplicemente con $\exists x \in A : p(x)$. Indichiamo $\forall x((x \in A) \Rightarrow p(x))$ con $\forall x \in A : p(x)$, oppure $\forall x \in A \Rightarrow p(x)$. Indichiamo $\neg(x \in A)$ con $x \notin A$.

Gli insiemi possono essere rappresentati graficamente tramite *diagrammi di Eulero-Venn*. Un insieme può essere definito enumerando i suoi elementi (se sono in numero finito, oppure se sono infiniti ma è chiaro come li si sta elencando).

Un altro modo di definire un insieme è *per proprietà*, selezionando all'interno di un altro insieme quegli elementi che soddisfano un certo predicato, nella forma $A = \{x \in B \mid P(x)\}$.

Osservazione 1.25. *Una trattazione rigorosa degli insieme richiede degli assiomi, che qui non tratteremo, limitandoci a una teoria "ingenua" degli insiemi. Un esempio del fatto che occorra "mettere dei paletti" nel trattare gli insiemi è il seguente, noto come* paradosso di Russell. *Supponiamo di poter definire un insieme per proprietà in modo totalmente libero, senza selezionare gli elementi da un altro insieme (cosa che non si può fare nella teoria assiomatica degli insiemi), e sia U l'insieme i cui elementi sono tutti gli insiemi che non appartengono a sè stessi: $U = \{A \mid A \notin A\}$. Domandiamoci: U è un elemento di U ? Per definizione di U: se supponiamo $U \notin U$, allora $U \in U$; se supponiamo $U \in U$, allora $U \notin U$. In ogni caso abbiamo una contraddizione.*

Osservazione 1.26. *Due insiemi sono uguali quando hanno gli stessi elementi.*

In particolare, non importa l'ordine con cui gli elementi di un insieme sono elencati; ad esempio, $\{3, 5, 7\}$ e $\{5, 3, 7\}$ sono lo stesso insieme. Inoltre, non importa se un elemento è elencato più di una volta; ad esempio, $\{3, 5, 5, 7, 7, 7\}$ e $\{3, 5, 7\}$ sono lo stesso insieme.

I principali insiemi numerici sono:

- $\mathbb{N} = \{0, 1, 2, \ldots\}$, l'insieme dei numeri naturali;
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots, \}$, l'insieme dei numeri interi;
- $\mathbb{Q} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$, l'insieme dei numeri razionali;
- $\mathbb{R}$, l'insieme dei numeri reali;
- $\mathbb{C}$, l'insieme dei numeri complessi.

Con l'apice $^+$ o $^-$ su uno dei precedenti insiemi, indichiamo l'insieme dei suoi elementi positivi o negativi. Ad esempio: $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

Definizione 1.27. *Siano A e B due insiemi. B è detto* sottoinsieme *di A se*

$$\forall x \in B \Longrightarrow x \in A$$

e si indica $B \subseteq A$. Si dice anche che B è contenuto *in A.*

Tra i sottoinsiemi ci sono sempre l'insieme vuoto e l'insieme stesso: $\emptyset \subseteq A$, $A \subseteq A$.

Chiamiamo *insieme universo* un insieme che contenga tutti gli insiemi che stiamo trattando in quel momento.

Definizione 1.28. *Siano A, B due insiemi, e U un unsieme universo.*

- *L'*insieme delle parti *di A è l'insieme di tutti i sottoinsiemi di A:*

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

- *L'*unione *tra A e B è l'insieme*

$$A \cup B = \{x \mid x \in A \ \vee \ x \in B\}.$$

- *L'*intersezione *tra A e B è l'insieme*

$$A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}.$$

  A e B si dicono disgiunti *se $A \cap B = \emptyset$.*

- *La* differenza *tra A e B è l'insieme*

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

- *La* differenza simmetrica *tra A e B è l'insieme*

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = \{x \mid x \in A \,\dot{\vee}\, x \in B\}.$$

- *Il* prodotto cartesiano *tra A e B è l'insieme*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

  La coppia (a, b) è una coppia ordinata*, in cui conta l'ordine. Quindi $(a, b) \neq \{a, b\}$.*

- *Il* complementare *di A in U è l'insieme*

$$\overline{A}^U = U \setminus A = \{x \in U \mid x \notin A\}.$$

Se l'insieme universo è noto o non rilevante, indichiamo $\overline{A}^U$ semplicemente con $\overline{A}$.

Esempio 1.29. *Si consideri l'insieme $A = \{1, 2, 3, 4\}$. Allora l'insieme delle parti di A è*

$$\begin{aligned}\mathcal{P}(A) \quad = \quad & \Big\{\emptyset, \\ & \{1\}, \{2\}, \{3\}, \{4\}, \\ & \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \\ & \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \\ & \{1,2,3,4\}\Big\}.\end{aligned}$$

Esempio 1.30. *Dati gli insiemi $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ e $B = \{8, 9, 10, 11, 12, 13\}$, si ha che*

$$\begin{aligned} A \cup B &= \{1,2,3,4,5,6,7,8,9,10,11,12,13\}, \\ A \cap B &= \{8,9,10\}, \\ A \setminus B &= \{1,2,3,4,5,6,7\}, \\ B \setminus A &= \{11,12,13\}, \\ A \Delta B &= \{1,2,3,4,5,6,7,11,12,13\}. \end{aligned}$$

Esempio 1.31. *Dati gli insiemi $A = \{1, 2, 3\}$ e $B = \{\square, a, \pi\}$, si ha che*

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

In maniera analoga si definisce il prodotto cartesiano di un numero finito $n \geq 1$ di insiemi:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ per ogni } i = 1, 2, \ldots, n\}.$$

Per ogni numero naturale $n \geq 1$, si definisce $A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ volte}}$.

Definiamo l'unione e l'intersezione di una famiglia qualsiasi (anche infinita) di insiemi. Sia I un insieme qualsiasi, e consideriamo una famiglia di insiemi A_i, al variare di $i \in I$; diciamo che gli insiemi A_i sono indicizzati da I.

Definizione 1.32. *Sia $\{A_i \mid i \in I\}$ una famiglia di insiemi.*

- *L'unione degli insiemi A_i $(i \in I)$ è l'insieme*

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ per qualche } i \in I\}.$$

- *L'intersezione degli insiemi A_i $(i \in I)$ è l'insieme*

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ per tutti gli } i \in I\}.$$

Esempio 1.33. *Sia $I = \mathbb{N}$, e $A_i = \{i, -i\}$ per ogni $i \in I$. Allora $\bigcup_{i \in I} A_i = \mathbb{Z}$, $\bigcap_{i \in I} A_i = \emptyset$.*

Se gli insiemi A_i, con $i \in I$, sono a due a due disgiunti, allora la loro unione si dice *unione disgiunta* e si indica con $\bigsqcup_{i \in I} A_i$. In particolare, l'unione di due insiemi disgiunti A e B è l'unione disgiunta $A \sqcup B$.

Dati due insiemi A e B, si ha che

$$A = B \iff (A \subseteq B) \wedge (B \subseteq A).$$

Perciò, un modo per dimostrare l'uguaglianza di due insiemi A e B è mostrare che ogni elemento di A è un elemento di B, e ogni elemento di B è un elemento di A.

Esempio 1.34. *Le identità di De Morgan per gli insiemi sono le seguenti uguaglianze:*

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Dimostriamo la prima identità $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Dimostriamo la prima inclusione "$\subseteq$". Sia x un qualsiasi elemento di $\overline{A \cup B}$. Allora $x \notin A \cup B$, cioè è falso che $(x \in A) \vee (x \in B)$. Allora è falso che $x \in A$ ed è falso che $x \in B$. Allora $x \notin A$ e $x \notin B$. Perciò $x \in \overline{A}$ e $x \in \overline{B}$. Quindi $x \in \overline{A} \cap \overline{B}$.

Dimostriamo ora la seconda inclusione "$\supseteq$". Sia x un qualsiasi elemento di $\overline{A} \cap \overline{B}$. Allora $x \notin A$ e $x \notin B$. Perciò $x \notin A \cup B$, e dunque $x \in \overline{A \cup B}$.

Abbiamo dimostrato entrambi le inclusioni, e quindi vale l'uguaglianza $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Un altro modo per dimostrare un'identità insiemistica è tramite una *tavola di appartenenza*: si mette in una tabella ogni possibile combinazione di appartenenza di un generico

elemento x agli "insiemi elementari", con un 1 se x appartiene all'insieme e uno 0 se x non appartiene all'insieme; poi si riempiono le colonne degli "insiemi composti" e si mostra l'uguaglianza delle colonne dei due insiemi di cui bisognava dimostrare l'identità.

Esempio 1.35. *La seguente tavola dimostra la seconda legge di De Morgan* $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

A	B	$A \cap B$	$\overline{A \cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cup \overline{B}$
1	*1*	*1*	*0*	*0*	*0*	*0*
1	*0*	*0*	*1*	*0*	*1*	*1*
0	*1*	*0*	*1*	*1*	*0*	*1*
0	*0*	*0*	*1*	*1*	*1*	*1*

Osservazione 1.36. *C'è una corrispondenza tra la logica delle proposizioni e la teoria degli insiemi. Infatti, le equivalenze logiche dell'esercizio 1.8 corrispondono alle identità insiemistiche dell'esrcizio 1.15, tramite le seguenti identificazioni:*

logica delle proposizioni	*teoria degli insiemi*
$p \wedge q$	$A \cap B$
$p \vee q$	$A \cup B$
$\neg p$	$\overline{A}$
V	U *universo*
F	$\emptyset$

1.4 Esercizi

Esercizio 1.1. *Date le seguenti proposizioni* p *e* q*, scrivi la proposizione composta* $p \vee q$ *e determinane il valore di verità.*

1. p *:* 28 *è multiplo di* 7, q *:* 15 *è multiplo di* 5.
2. p *: l'angolo acuto è maggiore di* 90 *gradi,* q *: l'angolo retto è di* 90 *gradi.*
3. p *: il Po è un fiume,* q *: il Po è un monte.*
4. p *:* $5 < 2$, q *:* $-10 > 0$.

Svolgimento

1. $p \wedge q$: 28 è multiplo di 7 e 15 è multiplo di 5. p è vera e q è vera, quindi $p \wedge q$ è vera.
2. $p \wedge q$: l'angolo acuto è maggiore di 90 gradi e l'angolo retto è di 90 gradi.
   p è falsa e q è vera, quindi $p \wedge q$ è falsa.

3. $p \wedge q$: il Po è un fiume e un monte. p è vera e q è falsa, quindi $p \wedge q$ è falsa.

4. $p \wedge q$: $5 < 2$ e $-10 > 0$. p è falsa e q è falsa, quindi $p \wedge q$ è falsa.

Esercizio 1.2. *Date le seguenti proposizioni p e q, scrivi la proposizione composta $p \wedge q$ e determinane il valore di verità.*

- p : *Roma è una citta francese,* q : *Roma si trova in Emilia-Romagna.*
- p : 3 *divide* 15 , q : 4 *è un numero primo.*
- p : *Il rettangolo ha* 4 *angoli retti ,* q : *il trapezio è un quadrilatero.*

Esercizio 1.3. *Costruisci le tavole di verità delle seguenti espressioni logiche.*

1. $\overline{p} \Longrightarrow (\overline{\overline{p} \vee \overline{q}})$

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \vee \overline{q}$	$(\overline{\overline{p} \vee \overline{q}})$	$\overline{p} \Longrightarrow (\overline{\overline{p} \vee \overline{q}})$
V	V	F	F	F	V	V
V	F	F	V	V	F	V
F	V	V	F	V	F	F
F	F	V	V	V	F	F

2. $(p \Longrightarrow q) \Longrightarrow (\overline{p} \Longrightarrow \overline{q})$

p	q	$p \Longrightarrow q$	$\overline{p} \Longrightarrow \overline{q}$	$(p \Longrightarrow q) \Longrightarrow (\overline{p} \Longrightarrow \overline{q})$
V	V	V	V	V
V	F	F	V	V
F	V	V	F	F
F	F	V	V	V

3. $(p \Longrightarrow q) \vee p$

p	q	$p \Longrightarrow q$	$(p \Longrightarrow q) \vee p$
V	V	V	V
V	F	F	V
F	V	V	V
F	F	V	V

4. $p \wedge (p \vee q)$

5. $\overline{q} \wedge (p \vee q)$

6. $p \Longrightarrow (\overline{q} \vee p)$

7. $q \wedge (q \Longrightarrow \overline{p})$

8. $(p \vee q) \iff \overline{p}$

Esercizio 1.4. *Dimostra che l'espressione $(p \wedge q) \Longrightarrow p$ è una tautologia.*

Soluzione. Costruendo la seguente tavola di verità, si deduce dall'ultima colonna che $(p \wedge q) \Longrightarrow p$ è una tautologia:

p	q	$p \wedge q$	$(p \wedge q) \Longrightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

Esercizio 1.5. *Dimostra che l'espressione $p \Longrightarrow p$ è una tautologia.*

Esercizio 1.6. *Dimostra che l'espressione $(p \wedge q) \wedge (p \wedge \overline{q})$ è una contraddizione.*

Esercizio 1.7. *Dimostra che l'espressione $(p \Longrightarrow q) \wedge (p \wedge \overline{q})$ è una contraddizione.*

Esercizio 1.8. *Dimostra le seguenti equivalenze logiche (dove* **T** *indica una proposizione sempre vera e* **F** *indica una proposizione sempre falsa):*

$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	*prop. di identità*
$p \vee \mathbf{V} \equiv \mathbf{V}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	*prop. di dominazione*
$p \vee p \equiv p$ $p \wedge p \equiv p$	*prop. di idempotenza*
$\neg(\neg p) \equiv p$	*doppia negazione*
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	*prop. commutativa*
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	*prop. associativa*
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	*prop. distributiva*
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	*prop. di assorbimento*
$\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$ $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$	*leggi di De Morgan*
$p \vee \overline{p} \equiv \mathbf{V}$ $p \wedge \overline{p} \equiv \mathbf{F}$	

$p \Rightarrow q \ \equiv \ \overline{p} \vee q$
$p \Rightarrow q \ \equiv \ \overline{q} \Rightarrow \overline{p}$
$p \vee q \ \equiv \ \overline{p} \Rightarrow q$
$p \wedge q \ \equiv \ \neg(p \Rightarrow \neg q)$
$\neg(p \Rightarrow q) \ \equiv \ p \wedge \neg q$
$(p \Rightarrow q) \wedge (p \Rightarrow r) \ \equiv \ p \Rightarrow (q \wedge r)$
$(p \Rightarrow r) \wedge (q \Rightarrow r) \ \equiv \ (p \vee q) \Rightarrow r$
$(p \Rightarrow q) \vee (p \Rightarrow r) \ \equiv \ p \Rightarrow (q \vee r)$
$(p \Rightarrow r) \vee (q \Rightarrow r) \ \equiv \ (p \wedge q) \Rightarrow r$
$p \Leftrightarrow q \ \equiv \ (p \Rightarrow q) \wedge (q \Rightarrow p)$
$p \Leftrightarrow q \ \equiv \ \overline{p} \Leftrightarrow \overline{q}$
$p \Leftrightarrow q \ \equiv \ (p \wedge q) \vee (\overline{p} \wedge \overline{q})$
$\neg(p \Leftrightarrow q) \ \equiv \ p \Leftrightarrow \neg q$

Esercizio 1.9. *Dire quali delle seguenti proposizioni sono logicamente equivalenti.*

- $(p \wedge \neg r) \vee (q \wedge \neg p) \vee (r \wedge \neg q)$
- $(p \vee q) \wedge (\neg r \vee \neg q)$

- $(r \vee \neg(q \wedge \neg p)) \wedge \neg p$
- $\neg q \wedge (r \vee \neg(p \wedge \neg q))$
- $\neg(p \wedge q \wedge r) \wedge (p \vee q \vee r)$
- $((p \vee \neg q) \wedge \neg(q \wedge \neg r))$

Esercizio 1.10. *Per ciscuna delle proposizioni dell'esercizio 1.9, trovare una forma normale disgiuntiva, la forma normale disgiuntiva completa, e una forma normale congiuntiva.*

Esercizio 1.11. *Dati i predicati $p(x)$: x divide 27, $q(x)$: x divide 24, determinare tutti i numeri interi x che verificano*

$$p(x) \wedge q(x), \qquad p(x) \vee q(x), \qquad \overline{p(x)} \wedge q(x).$$

Esercizio 1.12. *Nel dominio dei numeri interi, determinare il valore di verità delle proposizioni:*

$$\forall x(x+1 > x), \qquad \exists x(2x = 3x), \qquad \exists x(x = -x), \qquad \forall x(x^2 \geq x).$$

Ripetere l'esercizio nel dominio dei numeri reali.

Esercizio 1.13. *Nell'universo di tutte le persone, consideriamo i predicati $P(x)$:"x è un professore", $Q(x)$: "x è ignorante", $R(x)$: "x è vanitoso". Esprimere con $P(x), Q(x), R(x)$, quantificatori e connettivi le seguenti proposizioni.*

1. *Nessun professore è ignorante.*
2. *Tutti gli ignoranti sono vanitosi.*
3. *Nessun professore è vanitoso.*

Stabilire se la proposizione 3 segue dalle proposizioni 1 e 2.

Esercizio 1.14. *Nel dominio di tutte le persone, consideriamo i predicati $P(x)$:"x è un bambino", $Q(x)$: "x è una persona logica", $R(x)$: "x è capace di afferrare un coccodrillo", $S(x)$:"x è disprezzato". Esprimere con $P(x), Q(x), R(x), S(x)$, quantificatori e connettivi le seguenti proposizioni.*

1. *I bambini sono persone illogiche.*
2. *Nessuno che sia capace di afferrare un coccodrillo disprezzato.*

3. *Le persone illogiche sono disprezzate.*

4. *I bambini non sanno afferrare i coccodrilli.*

Stabilire se la proposizione 4 segue dalle proposizioni 1, 2 e 3.

Esercizio 1.15. *Dimostra le seguenti identità insiemistiche (dove U indica un insieme universo):*

$A \cap U = A$ $A \cup \emptyset = A$	*prop. di identità*
$A \cup U = U$ $A \cap \emptyset = \emptyset$	*prop. di dominazione*
$A \cup A = A$ $A \cap A = A$	*prop. di idempotenza*
$\overline{\overline{A}} = A$	*complementazione*
$A \cup B = B \cup A$ $A \cap B = B \cap A$	*prop. commutativa*
$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	*prop. associativa*
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	*prop. distributiva*
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	*prop. di assorbimento*
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	*leggi di De Morgan*
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	

Capitolo 2

Relazioni e funzioni

2.1 Relazioni

Definizione 2.1. *Dati due insiemi A e B, una* relazione *(binaria) $\mathcal{R}$ da A a B è un sottoinsieme del prodotto cartesiano $A \times B$. Una relazione da A ad A si dice semplicemente una relazione su A. Se $(a, b) \in \mathcal{R}$, si dice che "a è in relazione con b" e lo si indica con $a \mathcal{R} b$. Se $(a, b) \notin \mathcal{R}$, scriviamo $a \not\mathcal{R} b$.*

Esempio 2.2. *Si considerino i seguenti insiemi $A = \{1, 2, 3, 4, 5\}$ e $B = \{a, b, c, d\}$. Una relazione $\mathcal{R}$ da A a B è la seguente:*

$$\mathcal{R} = \{(2, a), (2, c), (3, d), (1, a), (5, a), (5, c)\}.$$

Consideriamo due insiemi finiti A con m elementi e B con n elementi, in cui abbiamo dato un ordine agli elementi: $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$. Diamo due modi di rappresentare una relazione $\mathcal{R} \subseteq A \times B$.

Definizione 2.3. *Una* matrice *di tipo $m \times n$ a valori in un insieme I è una tabella M con m righe e n colonne e un elemento di I in ogni posizione; per ogni $i = 1, \ldots, m$ e $j = 1, \ldots, n$, l'elemento nella riga i-esima e colonna j-esima è indicato con m_{ij} ed è detto l'elemento di posto (i, j).*

La relazione $\mathcal{R}$ è rappresentata da una matrice $M_{\mathcal{R}}$ di tipo $m \times n$, definita da

$$m_{ij} = \begin{cases} 1 & \text{se } a_i \ \mathcal{R} \ b_j, \\ 0 & \text{se } a_i \ \not\mathcal{R} \ b_j. \end{cases}$$

Ad esempio, la relazione $\mathcal{R}$ dell'esempio 2.2 è rappresentata dalla matrice

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Se $\mathcal{R}$ è una relazione su A, allora la matrice associata è *quadrata* ed è definita da

$$m_{ij} = \begin{cases} 1 & \text{se } a_i \ \mathcal{R} \ a_j, \\ 0 & \text{se } a_i \ \not\mathcal{R} \ a_j. \end{cases}$$

Una relazione $\mathcal{R}$ su $A = \{a_1, \ldots, a_m\}$ può essere anche rappresentata tramite un grafo.

Definizione 2.4. *Un* grafo diretto *(o* grafo orientato*) G è costituito da un insieme V di elementi detti* vertici *(o* nodi*) e da insieme $E \subseteq V \times V$ di coppie ordinate dette* spigoli *(o* archi*).*

Il grafo è rappresentato graficamente disegnando un punto per ogni vertice e un arco per ogni spigolo (a, b), con una freccia ad indicare che a è il vertice iniziale *e b il* vertice finale *dello spigolo (a, b); se il vertice inziale e quello finale coincidono, il corrispondente spigolo $(a, a) \in E$ è detto un* cappio *(o* loop*).*

il grafo $G_{\mathcal{R}}$ che rappresenta la relazione $\mathcal{R} \subseteq A \times A$ è definito da $V = A$ e $E = \mathcal{R}$. Cioè, i vertici sono gli elementi di A, e c'è uno arco da a a b se e solo se $a \ \mathcal{R} \ b$.

Definizione 2.5. *Una relazione $\mathcal{R}$ su A è detta*

1. riflessiva *se* $\forall a \in A : \ a \ \mathcal{R} \ a$;
2. simmetrica *se* $\forall a, b \in A : \ a \ \mathcal{R} \ b \implies b \ \mathcal{R} \ a$;
3. transitiva *se* $\forall a, b, c \in A : \ a \ \mathcal{R} \ b \ \wedge \ b \ \mathcal{R} \ c \implies a \ \mathcal{R} \ c$;
4. antisimmetrica *se* $\forall a, b \in A : \ a \ \mathcal{R} \ b \ \wedge \ b \ \mathcal{R} \ a \implies a = b$.

Osservazione 2.6. *Sia $\mathcal{R}$ una relazione su A.*

- *$\mathcal{R}$ è riflessiva se solo se la matrice $M_{\mathcal{R}}$ ha tutti* 1 *sulla diagonale principale; cioè, $m_{ii} = 1$ per ogni i.*
- *$\mathcal{R}$ è riflessiva se e solo nel grafo $G_{\mathcal{R}}$ c'è un loop intorno a ogni vertice.*

- *$\mathcal{R}$ è simmetrica se e solo se la matrice $M_{\mathcal{R}}$ è simmetrica (rispetto alla diagonale principale); cioè, $m_{ij} = m_{ji}$ per ogni i e j.*
- *$\mathcal{R}$ è simmetrica se e solo se, nel grafo $G_{\mathcal{R}}$, per ogni arco (a, b) c'è anche l'arco (b, a).*
- *$\mathcal{R}$ è transitiva se e solo se, nella matrice $M_{\mathcal{R}}$, quando ci sono due 1 con l'indice di colonna del primo uguale all'indice di riga del secondo 1, allora c'è anche un 1 nella riga del primo e colonna del secondo.*
- *$\mathcal{R}$ è transitiva se e solo se, nel grafo $G_{\mathcal{R}}$, se ci sono un arco (a, b) e un arco (b, c) allora c'è anche l'arco (a, c).*
- *$\mathcal{R}$ è antisimmetrica se e solo se, per ogni $i \neq j$, si ha $m_{ij} \cdot m_{ji} = 0$, cioè al più uno tra m_{ij} e m_{ji} è uguale a 1.*
- *$\mathcal{R}$ è antisimmetrica se e solo se, nel grafo $G_{\mathcal{R}}$, due vertici distinti non sono mai congiunti da più di un arco.*

Poiché due relazioni binarie $\mathcal{R}_1, \mathcal{R}_2$ da A a B sono sottoinsiemi dello stesso insieme $A \times B$, possiamo effettuare operazioni insiemistiche e ottenere nuove relazioni:

- relazione unione: $\mathcal{R}_1 \cup \mathcal{R}_2 = \{(a, b) \in A \times B \colon (a, b) \in \mathcal{R}_1 \vee (a, b) \in \mathcal{R}_2\}$,
- relazione intersezione: $\mathcal{R}_1 \cap \mathcal{R}_2 = \{(a, b) \in A \times B \colon (a, b) \in \mathcal{R}_1 \wedge (a, b) \in \mathcal{R}_2\}$,
- relazione differenza: $\mathcal{R}_1 \setminus \mathcal{R}_2 = \{(a, b) \in A \times B \colon (a, b) \in \mathcal{R}_1 \wedge (a, b) \notin \mathcal{R}_2\}$
- relazione differenza simmetrica: $\mathcal{R}_1 \dot{\vee} \mathcal{R}_2 = (\mathcal{R}_1 \setminus \mathcal{R}_2) \cup (\mathcal{R}_2 \setminus \mathcal{R}_1)$

Di particolare interesse è la composizione di relazioni. Date una relazione $\mathcal{R}$ da A a B e una relazione $\mathcal{S}$ da B a C, si dice *relazione composta* la relazione $\mathcal{S} \circ \mathcal{R}$ da A a C definita da:

$$\mathcal{S} \circ \mathcal{R} = \{(a, c) \in A \times C \colon \text{ esiste un elemento } b \in B \text{ tale che } (a, b) \in \mathcal{R} \text{ e } (b, c) \in \mathcal{S}\}.$$

Se $\mathcal{R}$ è una relazione su A, la relazione composta $\mathcal{R} \circ \mathcal{R}$ su A indicata con $\mathcal{R}^2$; più in generale la relazione composta $\mathcal{R} \circ \cdots \circ \mathcal{R}$ (n volte) è indicata con $\mathcal{R}^n$.

Proposizione 2.7. *Siano $\mathcal{R}$ e $\mathcal{R}'$ due relazioni su $A = \{a_1, \ldots, a_n\}$, rappresentate dalle matrici $M_{\mathcal{R}} = (m_{ij})$ e $M_{\mathcal{R}'} = (m'_{ij})$. Allora, indicando 1=vero e 0=falso,*

- *$\mathcal{R} \cup \mathcal{R}'$ è rappresentata dalla matrice $M_{\mathcal{R}} \vee M_{\mathcal{R}'}$ che nel posto (i, j) ha $m_{ij} \vee m'_{ij}$,*

- *$\mathcal{R} \cap \mathcal{R}'$ è rappresentata dalla matrice $M_{\mathcal{R}} \wedge M_{\mathcal{R}'}$ che nel posto (i,j) ha $m_{ij} \wedge m'_{ij}$.*

Se $\mathcal{R}$ è una relazione da $A = \{a_1, \dots, a_n\}$ a $B = \{b_1, \dots, b_m\}$ e $\mathcal{S}$ è una relazione da B a $C = \{c_1, \dots, c_\ell\}$, rappresentate dalle matrici $M_{\mathcal{R}} = (r_{ij})_{j=1,\dots,m}^{i=1,\dots,n}$ e $M_{\mathcal{S}} = (s_{ij})_{j=1,\dots,\ell}^{i=1,\dots,m}$, allora la relazione composta $\mathcal{S} \circ \mathcal{R} \subseteq A \times C$ è rappresentata dalla matrice $M_{\mathcal{R}} \circ M_{\mathcal{S}} = (t_{ij})_{j=1,\dots,\ell}^{i=1,\dots,n}$, dove

$$t_{ij} = (r_{i1} \wedge s_{1j}) \vee (r_{i2} \wedge s_{2j}) \vee \cdots \vee (r_{im} \wedge s_{mj}).$$

In particolare, indichiamo con $M_{\mathcal{R}}^{[n]}$ la matrice $M_{\mathcal{R}} \circ \cdots \circ M_{\mathcal{R}}$ associata alla relazione $\mathcal{R}^n$.

Esempio 2.8. *Siano $\mathcal{R} \subseteq A \times B$ e $\mathcal{S} \subseteq B \times C$ relazioni rappresentate rispettivamente da*

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad M_{\mathcal{S}} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Allora la relazione $\mathcal{S} \circ \mathcal{R} \subseteq A \times C$ è rappresentata da

$$M_{\mathcal{S} \circ \mathcal{R}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

Definizione 2.9. *Data una relazione $\mathcal{R}$ su un insieme A, si dice:*

- chiusura riflessiva *di $\mathcal{R}$ la più piccola relazione riflessiva $\mathcal{R}'$ su A che contiene $\mathcal{R}$; cioè, $\mathcal{R}'$ è riflessiva, $\mathcal{R} \subseteq \mathcal{R}'$, e se $\mathcal{S}$ è una relazione riflessiva su A tale che $\mathcal{R} \subseteq \mathcal{S}$, allora $\mathcal{R}' \subseteq \mathcal{S}$;*

- chiusura simmetrica *di $\mathcal{R}$ la più piccola relazione simmetrica $\mathcal{R}'$ su A che contiene $\mathcal{R}$; cioè, $\mathcal{R}'$ è simmetrica, $\mathcal{R} \subseteq \mathcal{R}'$, e se $\mathcal{S}$ è una relazione simmetrica su A tale che $\mathcal{R} \subseteq \mathcal{S}$, allora $\mathcal{R}' \subseteq \mathcal{S}$;*

- chiusura transitiva *di $\mathcal{R}$ la più piccola relazione transitiva $\mathcal{R}'$ su A che contiene $\mathcal{R}$; cioè, $\mathcal{R}'$ è transitiva, $\mathcal{R} \subseteq \mathcal{R}'$, e se $\mathcal{S}$ è una relazione transitiva su A tale che $\mathcal{R} \subseteq \mathcal{S}$, allora $\mathcal{R}' \subseteq \mathcal{S}$.*

Il seguente risultato è di facile verifica.

Proposizione 2.10. *Data una relazione $\mathcal{R}$ su A,*

- *la sua chiusura riflessiva è $\mathcal{R} \cup \Delta$, dove $\Delta = \{(a,a) \colon a \in A\}$ è la* diagonale *su A;*

- *la sua chiusura simmetrica è $\mathcal{R} \cup \mathcal{R}^{-1}$, dove $\mathcal{R}^{-1} = \{(b,a) \colon (a,b) \in \mathcal{R}\}$.*

Osservazione 2.11. *In termini del grafo $G_{\mathcal{R}}$, la chiusura riflessiva si ottiene aggiungendo i cappi a tutti i vertici, e la chiusura simmetrica si ottiene mettendo un arco in entrambe le direzioni ogni volta che due vertici distinti sono collegati da un arco.*

In termini della matrice $M_{\mathcal{R}}$, la chiusura riflessiva si ottiene ponendo tutti 1 *sulla diagonale principale, e la chiusura simmetrica si ottiene ponendo $m_{ij} = 1$ quando $m_{ji} = 1$.*

Per fare ciò, iniziamo considerando un grafo $G_{\mathcal{R}}$, due vertici a e b del grafo, e definendo un *cammino* di lunghezza n da a a b come una sequenza $v_0, v_1, \ldots, v_n$ dove (v_0, v_1), (v_1, v_2), $\ldots$, (v_{n-1}, v_n) sono archi di $G_{\mathcal{R}}$ tale che $v_0 = a$ e $v_n = b$. In termini della relazione $\mathcal{R}$, ciò significa che

$$(v_0, v_1), (v_1, v_2) \ldots, (v_{n-1}, v_n) \in \mathcal{R}.$$

Un cammino chiuso, cioè un cammino da a a a, è detto un *circuito*.

Proposizione 2.12. *Sia $\mathcal{R}$ una relazione su A e siano $a, b \in A$. Esiste un cammino di lunghezza n da a a b se e solo se $(a, b) \in \mathcal{R}^n$.*

Dimostrazione. Dimostriamo la tesi per induzione su n. Se $n = 1$, allora ovviamente esiste un cammino di lunghezza 1 da a a b se e solo se $(a, b) \in \mathcal{R} = \mathcal{R}^1$. Supponiamo vera la tesi per n. Un cammino di lunghezza $n + 1$ da a a b esiste se e solo se esiste un $c \in A$ tale che esiste un cammino di lunghezza n da a a c e $(c, b) \in \mathcal{R}$. Per ipotesi induttiva, questo succede se e solo se esiste un $c \in A$ tale che $(a, c) \in \mathcal{R}^n$ e $(c, b) \in \mathcal{R}$, cioè se e solo se $(a, b) \in \mathcal{R}^n \circ \mathcal{R} = \mathcal{R}^{n+1}$. □

Risulta perciò chiaro che

$$\mathcal{R}^* := \bigcup_{n=1}^{\infty} \mathcal{R}^n$$

è la *relazione di connettività* di $\mathcal{R}$, cioè $(a, b) \in \mathcal{R}^*$ se e solo se esiste un cammino da a a b.

Mostriamo ora che la relazione di connettività di $\mathcal{R}$ è la sua chiusura transitiva.

Proposizione 2.13. *Sia $\mathcal{R}$ una relazione su A. La sua chiusura transitiva è uguale alla relazione di connettività $\mathcal{R}^*$.*

Dimostrazione. Per definizione, $\mathcal{R} \subseteq \mathcal{R}^*$ (basta prendere $n = 1$).

Mostriamo ora che $\mathcal{R}^*$ è transitiva. Se $(a, b), (b, c) \in \mathcal{R}^*$, allora esistono $i, j \geq 1$ tali che $(a, b) \in \mathcal{R}^i$ e $(b, c) \in \mathcal{R}^j$, cioè (Proposizione 2.12) esiste un cammino di lunghezza i da a a b e un cammino di lunghezza j da b a c; perciò esiste un cammino di lunghezza $i + j$ da a a c, cioè $(a, c) \in \mathcal{R}^{i+j} \subseteq \mathcal{R}^*$.

Mostriamo ora che ogni relazione transitiva $\mathcal{S}$ che contiene $\mathcal{R}$ deve contenere anche $\mathcal{R}^*$. Sia $(a,b) \in \mathcal{R}^*$. Allora $(a,b) \in \mathcal{R}^N$ per qualche $N \geq 1$, cioè esistono $a_0, a_1, \ldots, a_N$ tali che $a_0 = a$, $a_N = b$, e $(a_0,a_1),(a_1,a_2),\ldots,(a_{N-1},a_N) \in \mathcal{R}$. Da $(a_0,a_1),(a_1,a_2) \in \mathcal{R} \subseteq \mathcal{S}$ e la transitività di $\mathcal{S}$ segue $(a_0,a_2) \in \mathcal{S}$, e iterando questo ragionamento si ottiene infine $(a_0,a_N) \in \mathcal{S}$, cioè $(a,b) \in \mathcal{S}$. □

Se A è un insieme finito con n elementi, è sufficiente esaminare i cammini di lunghezza al più n, come mostra il seguente lemma.

Lemma 2.14. *Sia A un insieme di n elementi, $\mathcal{R}$ una relazione su A, e siano $a,b \in A$. Se esiste un cammino da a a b, allora esiste un cammino da a a b di lunghezza al più n. Se in aggiunta $a \neq b$, allora esiste un cammino da a a b di lunghezza al più $n-1$.*

Dimostrazione. Sia m la minima lunghezza tra tutti i cammini da a a b, e sia $a_0, a_1, \ldots, a_m$ un cammino di lunghezza m da $a_0 = a$ a $a_n = b$.

Iniziamo con il caso $a \neq b$, e supponiamo per assurdo che $m \geq n$, cosicché $m+1 > n$. Allora tra gli $m+1$ elementi $a_1, a_1, \ldots, a_m \in A$ ce ne sono almeno due uguali, diciamo a_i e a_j con $i < j$. Allora il cammino iniziale contiene il circuito $a_i, a_{i+1}, \ldots, a_j$, che ha lunghezza $j - i \geq 1$. Rimuovendo questa parte di cammino, otteniamo un cammino $a_0, a_1, \ldots, a_i, \ldots, a_{j+1}, \ldots, a_m$ da a a b di lunghezza minore di m, in contraddizione con la minimalità di m.

Nel caso $a = b$ si dimostra che $m \leq n$ in maniera analoga, osservando che il cammino $a = a_0, a_1, \ldots, a_m = a$ contiene m elementi di A. □

Il precedente lemma implica che, se A ha n elementi, allora

$$\mathcal{R}^* = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \cdots \cup \mathcal{R}^n.$$

In questo caso, la chiusura transitiva $\mathcal{R}^*$ di $\mathcal{R}$ ha come matrice associata

$$M_{\mathcal{R}^*} = M_{\mathcal{R}} \vee M_{\mathcal{R}}^{[2]} \vee M_{\mathcal{R}}^{[3]} \vee \cdots \vee M_{\mathcal{R}}^{[n]}.$$

Questa equazione permette di calcolare $M_{\mathcal{R}^*}$, e quindi la chiusura trasitiva di $\mathcal{R}$, tramite all'incirca n^4 operazioni elementari (perché il prodotto di due matrici $n \times n$ richiede all'incirca n^3 operazioni elementari). Vediamo ora un algoritmo più efficiente di quello appena descritto per calcolare la chiusura transitiva di $\mathcal{R}$, noto come algoritmo di Warshall.

Sia $\mathcal{R}$ una relazione binaria su un insieme $A = \{a_1, a_2, \ldots, a_n\}$ di n elementi. Siano $a,b \in A$. Definiamo le relazioni $\mathcal{R}^{(0)}, \mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(n)}$ su A come segue: $\mathcal{R}^{(0)} := \mathcal{R}$; per ogni

$k = 1, 2, \ldots, n$, la coppia $(a, b) \in A^2$ appartiene a $\mathcal{R}^{(k)}$ se e solo se esiste un cammino da a a b che, a parte gli estremi a e b, usa solo elementi in $\{a_1, a_2, \ldots, a_k\}$. In particolare, per ogni $a, b \in A$, si ha $(a, b) \in \mathcal{R}^{(n)}$ se e solo esiste un cammino da a a b; cioè $\mathcal{R}^{(n)}$ è la relazione di connettività $\mathcal{R}^*$, e quindi (per la Proposizione 2.13) $\mathcal{R}^{(n)}$ è la chiusura transitiva di $\mathcal{R}$.

L'algoritmo di Warshall costruisce ricorsivamente le relazioni $\mathcal{R}^{(1)}, \mathcal{R}^{(2)}, \ldots, \mathcal{R}^{(n)}$ a partire da $\mathcal{R}^{(0)} = \mathcal{R}$ come segue. Sia $k \in \{1, \ldots, n\}$. Per ogni scelta di $i, j \in \{1, \ldots, n\}$, $(a_i, a_j) \in \mathcal{R}^{(k)}$ se e solo se: $(a_i, a_j) \in \mathcal{R}^{(k-1)}$; oppure, $(a_i, a_k) \in \mathcal{R}^{(k-1)}$ e $(a_k, a_j) \in \mathcal{R}^{(k-1)}$.

In termini di matrici, indicando con $M_{\mathcal{R}^{(k)}} = (m_{ij}^{(k)})$ la matrice associata a $\mathcal{R}^{(k)}$, si pone

$$m_{ij}^{(k)} := m_{ij}^{(k-1)} \vee (m_{ik}^{(k-1)} \wedge m_{kj}^{(k-1)}).$$

Riassumiamo quindi l'algoritmo:

- $M_{\mathcal{R}^{(0)}} := M_{\mathcal{R}}$,
- per ogni k da 1 a n,
  - per ogni i da 1 a n,
    - per ogni j da 1 a n :
      $m_{ij}^{(k)} := m_{ij}^{(k-1)} \vee (m_{ik}^{(k-1)} \wedge m_{kj}^{(k-1)})$
- $M_{\mathcal{R}^{(n)}}$ è la matrice associata alla chiusura transitiva di $\mathcal{R}$.

Il costo di questo algoritmo è dell'ordine di n^3 operazioni logiche elementari: l'operazione più annidata richiede 2 operazioni, ed è annidata in 3 cicli di lunghezza n; quindi le operazioni totali da effettuare sono $2n^3$.

2.2 Relazioni di equivalenza

Definizione 2.15. *Una relazione $\mathcal{R}$ su A si dice* relazione di equivalenza *se è riflessiva, simmetrica e transitiva.*

Data una relazione di equivalenza $\mathcal{R}$ su A e un elemento $a \in A$, definiamo classe di equivalenza *di a l'insieme*

$$[a]_{\mathcal{R}} = \{b \in A \mid a \ \mathcal{R} \ b\}.$$

Esempio 2.16. *Si consideri l'insieme $A = \{1, 2, 3, 4\}$ e la seguente relazione $\mathcal{R}$ su A:*

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

Tale relazione non è riflessiva perché $(2,2) \notin \mathcal{R}$. *Non è simmetrica perché* $(1,3) \in \mathcal{R}$ *ma* $(3,1) \notin \mathcal{R}$. *Infine non è transitiva perché* $(4,1) \in \mathcal{R}$ *e* $(1,3) \in \mathcal{R}$, *ma* $(4,3) \notin \mathcal{R}$.

Definiamo ora le *partizioni* di un insieme A, che vedremo corrispondere alle relazioni di equivalenza su A.

Definizione 2.17. *Una* partizione *di* A *è un insieme* $\mathcal{P} \subset \mathcal{P}(A)$ *di sottoinsiemi di* A *tali che*

1. $\forall B \in \mathcal{P} \implies B \neq \emptyset$,
2. $\bigcup_{B \in \mathcal{P}} B = A$,
3. $\forall B_1, B_2 \in \mathcal{P} : B_1 \neq B_2 \implies B_1 \cap B_2 = \emptyset$.

Esempio 2.18. *Si consideri l'insieme* $A = \{1,2,3,4,5,6,7,8,9,10\}$. *Allora*

$$\mathcal{P} = \{\{1,3,5,6\}, \{2\}, \{4,7,8,9,10\}\}$$

è una partizione di A.

Proposizione 2.19. *Sia* $\mathcal{R}$ *una relazione di equivalenza su* A. *Allora*

$$A/\mathcal{R} := \{[a]_{\mathcal{R}} \mid a \in A\}$$

è una partizione di A, *detta* insieme quoziente di A rispetto a $\mathcal{R}$.

Dimostrazione. Dobbiamo dimostrare che ogni classe di equivalenza è non vuota, che ogni elemento di A appartiene a qualche classe di equivalenza, e che due classi di equivalenza o coincidono o sono disgiunte.

La prima affermazione è vera perché ogni $[a]_{\mathcal{R}} \in A/\mathcal{R}$ contiene almeno l'elemento a (per la proprietà riflessiva di $\mathcal{R}$). La seconda affermazione è vera perché ogni elemento $a \in A$ appartiene a $[a]_{\mathcal{R}} \in A/\mathcal{R}$.

Prendiamo ora due classi di equivalenza distinte $[a]_{\mathcal{R}}$ e $[b]_{\mathcal{R}}$. Supponiamo che $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$ e sia c un elemento di $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}}$. Allora per definizione di classe di equivalenza $a \mathcal{R} c$ e $b \mathcal{R} c$. Poiché $\mathcal{R}$ è simmetrica e transitiva, allora $a \mathcal{R} b$. Ma allora $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$, contro l'ipotesi. □

Esempio 2.20. *Si consideri sull'insieme* $A = \{1,2,3,4,5\}$ *la relazione di equivalenza*

$$\mathcal{R} = \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}.$$

Allora

$$\begin{aligned}[1] &= \{1,2,4\},\\ [2] &= \{1,2,4\},\\ [3] &= \{3\},\\ [4] &= \{1,2,4\},\\ [5] &= \{5\}.\end{aligned}$$

L'insieme quoziente di A rispetto a $\mathcal{R}$ è $\{\{1,2,4\},\{3\},\{5\}\}$.

Proposizione 2.21. *Sia $n \geq 1$. La* congruenza modulo n *definita da*

$$a \equiv_n b \iff n \mid (b-a)$$

è una relazione d'equivalenza su $\mathbb{Z}$. Inoltre l'insieme quoziente $\mathbb{Z}/\equiv_n$ è

$$\mathbb{Z}_{\equiv_n} = \mathbb{Z}_n := \{[0]_{\equiv_n}, [1]_{\equiv_n}, \ldots, [n-1]_{\equiv_n}\}.$$

Dimostrazione. Si ha che la relazione $\equiv_n$ soddisfa le proprietà

1. riflessiva: $a \equiv_n a$ in quanto $n \mid (a-a) = 0$,
2. simmetrica: se $a \equiv_n b$ allora $n \mid (b-a) = -(a-b)$, ma dunque $n \mid (a-b)$ e $b \equiv_n a$;
3. transitiva: se $a \equiv_n b$ e $b \equiv_n c$ allora $n \mid (b-a)$ e $n \mid (c-b)$ allora $n \mid (b-a)+(c-b) = (c-a)$ e dunque $a \equiv_n c$.

Pertanto $\equiv_n$ è una relazione di equivalenza.

Si ha che $[a]_{\equiv_n} = \{a+kn \mid k \in \mathbb{Z}\}$. Dunque ogni classe $[j]_{\equiv_n}$ coincide con una delle classi $[0]_{\equiv_n}, [1]_{\equiv_n}, \ldots, [n-1]_{\equiv_n}$ perché posso trovare un intero $a+kn \in \{0,\ldots,n-1\}$. Queste classi inoltre sono tutte distinte, in quanto se $[i]_{\equiv_n} = [j]_{\equiv_n}$, $i,j \in \{0,\ldots,n-1\}$, allora $n \mid (i-j)$. Siccome $-n < i-j < n$, l'unica possibilità è $i = j$. □

Proposizione 2.22. *Sia $\mathcal{P}$ una partizione di A. La relazione $\mathcal{R}_\mathcal{P}$ definita da*

$$a \mathcal{R}_\mathcal{P} b \iff \exists B \in \mathcal{P} : a, b \in B$$

è una relazione di equivalenza su A.

Dimostrazione. Si ha che la relazione $\mathcal{R}_\mathcal{P}$ soddisfa le proprietà

1. riflessiva: $a \mathcal{R}_{\mathcal{P}} a$ in quanto $a \in B$ per qualche $B \in \mathcal{P}$ (per la prop. 2 delle partizioni);
2. simmetrica: se $a \mathcal{R}_{\mathcal{P}} b$ allora $a, b \in B$ per qualche $B \in \mathcal{P}$, che è come dire $b, a \in B$, e dunque $b \mathcal{R}_{\mathcal{P}} a$;
3. transitiva: se $a \mathcal{R}_{\mathcal{P}} b$ e $b \mathcal{R}_{\mathcal{P}} c$ allora $a, b \in B$ e $b, c \in B'$, con $B, B' \in \mathcal{P}$. Siccome $b \in B \cap B'$, allora $B \cap B' \neq \emptyset$, e dunque (per la prop. 3 delle partizioni) $B = B'$. Allora $a, b, c \in B = B'$, e quindi anche $a \mathcal{R}_{\mathcal{P}} c$.

Pertanto $\mathcal{R}_{\mathcal{P}}$ è una relazione di equivalenza. □

Le Proposizioni 2.19 e 2.22 mostrano che esiste una corrispondenza uno ad uno tra l'insieme di tutte le relazioni di equivalenza su A e l'insieme di tutte le partizioni di A: la corrispondenza che alla relazione $\mathcal{R}$ associa la partizione $A/\mathcal{R}$, e che viceversa alla partizione $\mathcal{P}$ associa la relazione $\mathcal{R}_{\mathcal{P}}$.

2.3 Relazioni d'ordine e reticoli

Definizione 2.23. *Una relazione $\mathcal{R}$ su un insieme A si dice* relazione d'ordine (parziale) *se è riflessiva, antisimmetrica e transitiva.*

L'insieme A, munito di una relazione d'ordine $\mathcal{R}$, è detto insieme parzialmente ordinato *o* poset *(per* partially ordered set*), e $\mathcal{R}$ è detto un* ordine parziale *su A. Si indica il poset con $(A, \mathcal{R})$.*

Esempio 2.24. *Indicato con $\leq$ l'usuale "minore o uguale" tra numeri, si ha che $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ sono poset.*

Indicata con $|$ la divisibilità tra numeri interi, si ha che $(\mathbb{N}, |)$ e $(\mathbb{Z}, |)$ sono poset.

Se A è un insieme, l'inclusione insiemistica $\subseteq$ è un ordine parziale sull'insieme delle parti $\mathcal{P}(A)$.

Esempio 2.25. *Siano $(A_1, \preccurlyeq_1)$ e $(A_2, \preccurlyeq_2)$ due poset e sia $A = A_1 \times A_2$. L'*ordine lessicografico *su A è definito da*

$$(a_1, a_2) \preccurlyeq (b_1, b_2) \quad \iff \quad (a_1 \prec_1 b_1) \ \vee \ (a_1 = b_1 \ \wedge \ a_2 \preccurlyeq_2 b_2)$$

Più in generale, dati n poset $(A_1, \preccurlyeq_1), \ldots, (A_n, \preccurlyeq_n)$, l'ordine lessicografico su $A = A_1 \times \cdots \times A_n$ è l'ordine in cui $(a_1, \ldots, a_n) \preccurlyeq (b_1, \ldots, b_n)$ se e solo se

$$(a_1 \prec_1 b_1) \ \vee \ (\exists i > 0 \ : \ a_1 = b_1, \ldots, a_i = b_i \ \wedge \ a_{i+1} \preccurlyeq_{i+1} b_{i+1})$$

Ad esempio, se $A_1 = \cdots = A_n = \mathcal{A}$ è l'alfabeto con l'usuale ordinamento tra le lettere, e la n-upla $(a_1, \ldots, a_n) = \mathcal{A}^n$ è identificata con la stringa $a_1 a_2 \cdots a_n$, allora l'ordine lessicografico tra le stringhe di n lettere è quello usuale del dizionario.

Una relazione d'ordine è spesso indicata con il simbolo $\preccurlyeq$ (a ricordare l'usuale relazione d'ordine "minore o uguale" tra numeri), e $a \preccurlyeq b$ si legge "a è minore o uguale di b". Se $a \preccurlyeq b$ e $a \neq b$, si scrive $a \prec b$ e si dice che "a è minore strettamente di y".

Un poset finito e non vuoto può essere rappresentato graficamente tramite il suo *diagramma di Hasse*: gli elementi di A sono indicati da punti; se $a \prec b$ e non esiste $c \in A$ tale che $a \prec c \prec b$, si collega a e b con una linea continua, e si pone b più in alto di a (si dice che a *è coperto da* b, o che b *copre* a).

Definizione 2.26. *Sia $(A, \preccurlyeq)$ un poset.*

- *Due elementi a, b si dicono* confrontabili *se $a \preccurlyeq b$ oppure $b \preccurlyeq a$.*
- *Se tutti gli elementi $a, b \in A$ sono confrontabili, allora $(A, \preccurlyeq)$ si dice* totalmente ordinato*, o* catena *($\preccurlyeq$ è detto un* ordine totale *su A).*
- *Un elemento $a \in A$ è detto* massimo *di A se $x \preccurlyeq a$ per ogni $x \in A$; si scrive $a = \max A$.*
- *Un elemento $b \in A$ è detto* minimo *di A se $b \preccurlyeq x$ per ogni $x \in A$; si scrive $b = \min A$.*
- *Un elemento $c \in A$ è detto un* elemento massimale *di A se $\nexists x \in A$ tale che $c \prec x$.*
- *Un elemento $d \in A$ è detto un* elemento minimale *di A se $\nexists x \in A$ tale che $x \prec d$.*

Esempio 2.27. *Il poset $(\mathbb{N}, \leq)$ ha minimo 0 e non ha massimo.*

L'intervallo aperto di numeri reali $]0, 1[$, con l'usuale ordine totale $\leq$, non ha né elementi massimali né minimali, né massimo né minimo.

Il poset $([0, 1], \leq)$ ha massimo 1 e minimo 0.

Il poset $(\mathbb{Z}^+, |)$ non ha né minimo né massimo.

Il poset $(\mathcal{P}(B), \subseteq)$ ha minimo $\emptyset$ e massimo B.

L'insieme $\{2, 3, 4, 5, 6, 7, 8, 9, 10\}$, ordinato da $a \leq b \iff a \mid b$, non ha né minimo né massimo, ha $2, 3, 5, 7$ come elementi minimali e $6, 7, 8, 9, 10$ come elementi massimali.

Valgono le seguenti proprietà.

Proposizione 2.28. *Sia $(A, \preccurlyeq)$ un poset.*

1. *Il massimo di A, se esiste, è unico; il minimo di A, se esiste, è unico.*

2. *Se A ha massimo, allora* $\max A$ *è massimale, ed è l'unico elemento massimale di A. Analogamente, se A ha minimo, allora* $\min A$ *è minimale, ed è l'unico elemento minimale di A.*

3. *Se $(A, \preccurlyeq)$ è totalmente ordinato e c è massimale in A, allora $c = \max A$. Analogamente, se $(A, \preccurlyeq)$ è totalmente ordinato e d è minimale in A, allora $d = \min A$.*

4. *Se A è non vuoto e finito, allora A ha elementi massimali e minimali.*

5. *Se A è non vuoto, finito e totalmente ordinato, allora A ha massimo e minimo.*

Dimostrazione. (1.) Siano a, a' massimi di A. Allora $a \preccurlyeq a'$ (perché $a' = \max A$) e $a' \preccurlyeq a$ (perché $a = \max A$). Quindi $a = a'$ e $\max A$ è unico. Analogamente per l'unicità del minimo.

(2.) Sia $a = \max A$. Allora per ogni $x \in A$ vale $x \preccurlyeq a$ e quindi $a \not\prec x$, cioè a è massimale. Se c è un massimale di A, allora $c \not\prec a$. Poiché $c \preccurlyeq a$, segue $c = a$. Analogamente per il minimo.

(3.) Sia $(A, \preccurlyeq)$ totalmente ordinato e c massimale in A. Per ogni $x \in A$ vale $c \not\prec x$ (per massimalità di c) e quindi $x \preccurlyeq c$ (perché l'ordine è totale). Perciò $c = \max A$. Analogamente per il minimo.

(4.) Sia $x_1 \in A$. Se x_1 non è massimale, allora esiste $x_2 \in A$ tale che $x_1 \prec x_2$. Se x_2 non è massimale, procediamo allo stesso modo. Troviamo una catena di elementi distinti $x_1 \prec x_2 \prec \cdots \prec x_i$. Poiché A è finito, esiste un $i \geq 1$ tale che x_i è massimale. Analogamente per la minimalità.

(5.) Segue dai punti (3.) e (4.). □

Esempio 2.29. *L'intervallo aperto di numeri reali $]0, 1[$, con l'usuale ordine totale $\leq$, non ha né elementi massimali né minimali (e quindi, per la proprietà 3., né massimo né minimo). Invece il poset $([0, 1], \leq)$ ha massimo e minimo.*

Su ogni sottoinsieme B di A possiamo considerare l'ordinamento indotto, che indichiamo sempre con $\preccurlyeq$, e quindi lavorare sul poset indotto $(B, \preccurlyeq)$.

Definizione 2.30. *Un insieme ordinato $(A, \preccurlyeq)$ è detto* ben ordinato *($\preccurlyeq$ è detto un* buon ordine *su A) se ogni suo sottoinsieme non vuoto ammette minimo:*

$$(A, \preccurlyeq) \text{ ben ordinato} \iff \forall B \subseteq A : \ B \neq \emptyset \implies \exists \min B.$$

Esempio 2.31. $(\mathbb{N}, \leq)$ *è ben ordinato.* $(\mathbb{Z}, \leq)$ *non è ben ordinato.*

Proposizione 2.32. *Ogni insieme ben ordinato è totalmente ordinato.*

Dimostrazione. Comunque scelti $x, y \in A$, il sottoinsieme $B = \{x, y\}$ ha minimo. Se $x = \min B$, allora $x \preccurlyeq y$; se $y = \min B$, allora $y \preccurlyeq x$. In ogni caso x e y sono confrontabili. □

Definizione 2.33. *Sia* $(A, \preccurlyeq)$ *un insieme ordinato e* X *un sottoinsieme non vuoto di* A.

- *Un elemento* $a \in A$ *è detto un* maggiorante *di* X *se* $x \preccurlyeq a$ *per ogni* $x \in X$.
- *Un elemento* $b \in A$ *è detto un* minorante *di* X *se* $b \preccurlyeq x$ *per ogni* $x \in X$.
- *Se esiste il minimo* $c \in A$ *dell'insieme dei maggioranti di* X, c *è detto l'*estremo superiore *di* X, *indicato con* $\sup X$*:*

$$c = \sup X \iff \begin{cases} x \preccurlyeq c \ \text{ per ogni } \ x \in X, \\ \text{se } \ x \preccurlyeq a \ \text{ per ogni } \ x \in X, \ \text{allora } \ c \preccurlyeq a. \end{cases}$$

- *Se esiste il massimo* $d \in A$ *dell'insieme dei minoranti di* X, d *è detto l'*estremo inferiore *di* X, *indicato con* $\inf X$*:*

$$d = \inf X \iff \begin{cases} d \preccurlyeq x \ \text{ per ogni } \ x \in X, \\ \text{se } \ b \preccurlyeq x \ \text{ per ogni } \ x \in X, \ \text{allora } \ b \preccurlyeq d. \end{cases}$$

Osservazione 2.34. *Sia* $(A, \preccurlyeq)$ *un poset e* $X \subseteq A$. *Se il poset* $(X, \preccurlyeq)$ *ammette minimo* a, *allora* $a = \inf X$. *Se il poset* $(X, \preccurlyeq)$ *ammette massimo* b, *allora* $b = \sup X$.

Esempio 2.35. *Sia* I *un insieme e consideriamo il poset* $(\mathcal{P}(I), \subseteq)$. *Ogni sottoinsieme non vuoto* $\mathcal{S}$ *di* $\mathcal{P}(I)$ *ammetto estremo inferiore ed estremo superiore, che sono*

$$\inf \mathcal{S} = \bigcap_{B \in \mathcal{S}} B \qquad \sup \mathcal{S} = \bigcup_{B \in \mathcal{S}} B$$

Definizione 2.36. *Un* reticolo *(in inglese,* lattice*) è un insieme parzialmente ordinato* $(L, \preccurlyeq)$ *tale che, per ogni* $x, y \in L$, *l'insieme* $\{x, y\}$ *ammette estremo inferiore e estremo superiore.*

Esempio 2.37. $(\mathbb{Z}^+, |)$ *è un reticolo, dove* $\inf\{x, y\}$ *è il massimo comun divisore tra* x *e* y, *e* $\sup\{x, y\}$ *è il minimo comune multiplo di* x *e* y.

$(\mathcal{P}(I), \subseteq)$ *è un reticolo, dove* $\inf\{X, Y\} = X \cap Y$ *e* $\sup\{X, Y\} = X \cup Y$.

Esempio 2.38. *In molti ambienti il passaggio delle informazioni da un soggetto a un altro è sottoposto ad autorizzazione. Descriviamo tramite un reticolo una delle modalità di gestione del passaggio delle informazioni, la "mltilevel security policy".*

Ogni informazione è assegnata a una "security class", che è rappresentata da una coppia (a, c), dove a è un "authority level" e c una "category". L'insieme A delle authority level è fatto da numeri naturali, ordinati con l'ordine usuale $\leq$; l'insieme C delle category è fatto da sottoinsiemi di un insieme finito di comparti, ordinato dall'inclusione insiemistica $\subseteq$. Ordiniamo in modo lessicografico le security class tramite $(a_1, c_1) \preccurlyeq \iff a_1 \leq a_2$ e $c_1 \subseteq c_2$. Dimostrare che l'insieme di tutte le security class, ordinate da $\preccurlyeq$, è un reticolo.

Ogni soggetto può accedere a uno specifico insieme di security class (in generale non a tutte). L'informazione può essere trasmessa da (a_1, c_1) a (a_2, c_2) se solo se $(a_1, c_1) \preccurlyeq (a_2, c_2)$. Ad esempio: le authority level sono 0 "unclassified", 1 "confidential", 2 "secret", 3 "top secret"; l'insieme dei comparti è {spie, talpe, doppiogiochisti}. In questo caso, l'informazione nella security class (secret,{spie,talpe}) può essere trasmessa alla security class (top secret,{spie,taple,doppiogiochisti}) ma non alla classe (secret,{spie,doppiogiochisti}).

Teorema 2.39. *Sia $(L, \preccurlyeq)$ un reticolo, e per ogni $x, y \in L$ definiamo*

$$x \vee y := \sup\{x, y\} \text{ ("join")}, \qquad x \wedge y := \inf\{x, y\} \text{ ("meet").}$$

Allora, per ogni $x, y \in L$ valgono le seguenti proprietà:

- $x \vee x = x, \quad x \wedge x = x$ *(idempotenza);*
- $x \vee y = y \vee x, \quad x \wedge y = y \wedge x$ *(commutativa);*
- $x \vee (y \vee z) = (x \vee y) \vee z, \quad x \wedge (y \wedge z) = (x \wedge y) \wedge z$ *(associativa);*
- $x \vee (x \wedge y) = x, \quad x \wedge (x \vee y) = x$ *(assorbimento).*

Dimostrazione. Lasciata come esercizio. □

Il seguente teorema mostra che vale anche il viceversa del Teorema 2.39.

Teorema 2.40. *Sia L un insieme non vuoto munito di due operazioni interne $\vee$ e $\wedge$ (cioè, per ogni $x, y \in L$ è definito uno e un solo elemento $x \vee y \in L$, e uno e un solo elemento $x \wedge y \in L$).*

Supponiamo che le due operazioni $\vee$ e $\wedge$ verifichino le proprietà di idempotenza, commutativa, associativa e di assorbimento descritte sopra. Allora $y = x \vee y$ se e solo se $x = x \wedge y$. Inoltre, la relazione

$$x \preccurlyeq y \iff x = x \wedge y \quad (\iff y = x \vee y)$$

è una relazione d'ordine su L, e $(L, \preccurlyeq)$ è un reticolo, in cui per ogni $x, y \in L$ vale $x \vee y = \sup\{x, y\}$ e $x \wedge y = \inf\{x, y\}$.

Dimostrazione. Se $y = x \vee y$, allora per assorbimento $x = x \wedge (x \vee y) = x \wedge y$; analogamente, se $x = x \wedge y$ allora $y = x \vee y$.

Dimostriamo che $\preccurlyeq$ è un ordine su L. Proprietà riflessiva di $\preccurlyeq$: segue dall'idempotenza $x = x \wedge x$. Proprietà antisimmetrica di $\preccurlyeq$: se $x \preccurlyeq y$ e $y \preccurlyeq x$ allora $x = x \wedge y = y \wedge x = y$ (per la commutatività di $\wedge$). Proprietà transitiva di $\preccurlyeq$: se $x \preccurlyeq y$ e $y \preccurlyeq$, cioè $x = x \wedge y$ e $y = y \wedge z$, allora $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$ (per l'associatività di $\wedge$), cioè $x \preccurlyeq z$. Quindi $\preccurlyeq$ è una relazione d'ordine su L.

Per ogni $x, y \in L$, dimostriamo che $x \vee y = \sup\{x, y\}$. Vale $x \vee (x \vee y) = (x \vee x) \vee y = x \vee y$ (prop. associativa e di idempotenza), che significa $x \preccurlyeq x \vee y$. Analogamente si ha $y \preccurlyeq x \vee y$. Quindi $x \vee y$ è un maggiorante di $\{x, y\}$. Se $z \in L$ è un maggiorante di $\{x, y\}$, vale $x \preccurlyeq z$ e $y \preccurlyeq z$, cioè $x \vee z = z$ e $y \vee z = z$. Perciò $z = y \vee z = y \vee (x \vee z) = (y \vee x) \vee z = (x \vee y) \vee z$, da cui $x \vee y \preccurlyeq z$. Quindi $x \vee y$ è il minimo dei maggioranti di $\{x, y\}$, vale a dire $x \vee y = \inf\{x, y\}$.

In modo del tutto analogo (usando le proprietà di $\wedge$ invece che quelle di $\vee$) si dimostra che $x \wedge y = \inf\{x, y\}$. □

Osservazione 2.41.

- *Un insieme totalmente ordinato è un reticolo. Infatti x e y sono sempre confrontabili, e quindi $\{x, y\}$ ha massimo e minimo.*

- *Un reticolo ha non può avere più di un elemento massimale; se un massimale esiste, è il massimo. Analogamente, un reticolo ha al più un elemento minimale; se un minimale esiste, è il minimo.*

  Da ciò, usando il punto 4 della Prooposizione 2.28, segue che un reticolo finito ha sempre massimo e minimo.

Sia $\mathcal{R}$ una relazione d'ordine parziale e $\preccurlyeq$ una relazione d'ordine totale sullo stesso insieme A. L'ordine totale $\preccurlyeq$ si dice *compatibile* con l'ordine parziale $\mathcal{R}$ se vale la seguente proprietà: per ogni $a, b \in A$, se $a \mathcal{R} b$ allora $a \preccurlyeq b$.

Teorema 2.42. *Sia $A \neq \emptyset$ un insieme finito e $\mathcal{R}$ un ordine parziale su A. Allora esiste un ordine totale $\preccurlyeq$ su A tale che $\preccurlyeq$ è compatibile con $\mathcal{R}$.*

Dimostrazione. Diamo una dimostrazione costruttiva del teorema, andando a definire l'ordine totale $\preccurlyeq$ compatibile con $\mathcal{R}$. La proprietà fondamentale che usiamo è che ogni poset finito e non vuoto ammette elementi minimali (Proposizione 2.28, punto 4).

Il poset $(A, \mathcal{R})$ ammette elementi minimali; scegliamo un tale elemento a_1. Ora sia $A_1 := A \setminus \{a_1\}$ e consideriamo $(A_1, \mathcal{R})$, che è un poset ed è finito; se è non vuoto, scegliamo un suo elemento minimale a_2. Se $A_2 := A \setminus \{a_1, a_2\}$ è non vuoto, scegliamo un elemento minimale a_3 di $A_2, \mathcal{R})$. Iteriamo il procedimento estraendo un minimale a_{i+1} da $A_i := A \setminus \{a_1, \ldots, a_i\}$ finché è possibile farlo, cioè finché $A_i \neq \emptyset$. Poiché A è finito, il procedimento termina dopo un numero finito di estrazioni, pari al numero n di elementi di A.

Definiamo l'ordine totale su A tramite $a_1 \preccurlyeq a_2 \preccurlyeq \cdots \preccurlyeq a_n$, cioè $a_i \preccurlyeq a_j \iff i \leq j$ $(i, j = 1, \ldots, n)$. Allora $\preccurlyeq$ è compatibile con $\mathcal{R}$, infatti: se due elementi $a_i, a_j \in A$ soddisfano $a_i \,\mathcal{R}\, a_j$, allora a_j non può essere minimale in un insieme A_k finché $a_i \in A_k$. Perciò a_j viene estratto solo se a_i è già stato estratto in precedenza, cioè se $i < j$, che implica $a_i \preccurlyeq a_j$. □

L'ordine totale $\preccurlyeq$ compatibile con l'ordine parziale $\mathcal{R}$ è detto un *ordinamento topologico* (*topological sorting*) del poset $(A, \mathcal{R})$, e quello descritto nella dimostrazione è un algoritmo di ordinamento topologico. Equivalentemente, si parla di ordinamento topologico del grafo diretto $G_{\mathcal{R}}$ associato a $(A, \mathcal{R})$.

2.4 Funzioni

Definizione 2.43. *Siano A e B due insiemi. Una funzione f da A a B è una relazione di A su B tale che*

$$\forall a \in A \Longrightarrow \exists! \, b \in B : a \; f \; b.$$

Se $a \; f \; b$ scriveremo più semplicemente $f(a) = b$. Scriviamo inoltre $f : A \to B$, $a \mapsto f(a)$.

L'insieme A si dice dominio *di f. L'insieme B si dice* codominio *di f. L'insieme*

$$Im(f) := \{f(a) \mid a \in A\}$$

prende il nome di immagine *della funzione f. L'*immagine *di un sottoinsieme $C \subseteq A$ è*

$$f(C) := \{f(a) : a \in C\}.$$

Dato un elemento $b \in B$, la controimmagine *di b è l'insieme (eventualmente vuoto)*

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}.$$

Dato un sottoinsieme $D \subseteq B$, la controimmagine *di D è l'insieme (eventualmente vuoto)*

$$f^{-1}(D) := \bigcup_{b \in D} f^{-1}(b).$$

Osservazione 2.44. *Due funzioni f, g sono la stessa funzione quando hanno lo stesso dominio A e $f(a) = g(a)$ per ogni $a \in A$. Perciò una funzione viene univocamente definita specificando i valori che assume per tutti gli elementi del dominio.*

Definizione 2.45. *Una funzione $f : A \to B$ è detta:*

1. iniettiva *se $\forall x_1 \neq x_2 \in A \Longrightarrow f(x_1) \neq f(x_2)$;*
   (equivalentemente: $\forall x_1, x_2 \in A$, se $f(x_1) = f(x_2)$ allora $x_1 = x_2$)
2. suriettiva *se $\forall y \in B \Longrightarrow \exists x \in A \ : \ f(x) = y$;*
3. biettiva *se è iniettiva e suriettiva.*

Esempio 2.46. *La funzione "floor" associa ad un numero reale la sua parte intera inferiore:*

$$\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

La funzione "ceiling" associa ad un numero reale la sua parte intera superiore:

$$\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \geq x\}.$$

$\lfloor \cdot \rfloor$ e $\lceil \cdot \rceil$ sono suriettive ma non iniettive.

Osservazione 2.47. *Una funzione è iniettiva se e solo se $f^{-1}(b)$ contiene al più un elemento per ogni $b \in B$. Una funzione è suriettiva se e solo se $Im(f) = B$.*

Definizione 2.48. *Siano $f : A \to B$ e $g : C \to D$ due funzioni tali che $Im(f) \subseteq C$. Allora la* funzione composta *$g \circ f : A \to D$ è definita da $(g \circ f)(a) = g(f(a))$ per ogni $a \in A$.*

Si può notare che la funzione composta $g \circ f$ è esattamente la relazione composta definita più sopra, una volta che f e g sono viste come relazioni.

Proposizione 2.49. *Siano date due funzioni $f : A \to B$ e $g : B \to C$.*

1. *Se f e g sono entrambi iniettive, allora $g \circ f$ è iniettiva.*
   Se $g \circ f$ è iniettiva, allora f è iniettiva.

2. *Se f e g sono entrambi suriettive, allora $g \circ f$ è suriettiva.*
   Se $g \circ f$ è suriettiva, allora g è suriettiva.

3. *Se f e g sono entrambi biettive, allora $g \circ f$ è biettiva.*
   Se $g \circ f$ è biettiva, allora f è iniettiva e g è suriettiva.

Dimostrazione. (1.) Supponiamo f, g iniettive. Se $x_1, x_2 \in A$ sono tali che $(g \circ f)(x_1) = (g \circ f)(x_2)$, cioè $g(f(x_1)) = g(f(x_2))$, allora $f(x_1) = f(x_2)$ per l'iniettività di g, e dunque $x_1 = x_2$ per l'iniettività di f. Supponiamo $g \circ f$ iniettiva. Se $x_1, x_2 \in A$ hanno $f(x_1) = f(x_2)$, allora $g(f(x_1)) = g(f(x_2))$, cioè $(g \circ f)(x_1) = (g \circ f)(x_2)$. Essendo $g \circ f$ iniettiva, segue $x_1 = x_2$.

(2.) Supponiamo f, g suriettive. Sia $c \in C$. Per la suriettività di g, esiste $b \in B$ tale che $g(b) = c$; per la suriettività di f, esiste $a \in A$ tale che $f(a) = b$. Dunque esiste $a \in A$ tale che $(g \circ f)(a) = g(f(a)) = g(b) = c$. Supponiamo $g \circ f$ suriettiva. Allora per ogni $c \in C$ esiste $a \in A$ con $(g \circ f)(a) = c$, cioè $f(a) \in B$ verifica $g(f(a)) = c$; quindi g è suriettiva.

(3.) Segue dai punti (1.) e (2.). □

Definizione 2.50. *Sia A un insieme. La* funzione identità *di A è definita da*

$$\begin{array}{rccc} id_A : & A & \to & A, \\ & a & \mapsto & a. \end{array}$$

Osservazione 2.51. *La funzione identità è biettiva.*

Definizione 2.52. *Sia $f : A \to B$. La funzione f si dice* invertibile a destra *se esiste $g : B \to A$ (detta* inversa destra *di f) tale che*

$$f \circ g = id_B.$$

f si dice invertibile a sinistra *se esiste $g : B \to A$ (detta* inversa sinistra *di f) tale che*

$$g \circ f = id_A.$$

La funzione f si dice invertibile *se esiste $g : B \to A$ (detta* inversa *di f) tale che*

$$f \circ g = id_B \qquad g \circ f = id_A.$$

Teorema 2.53. *Sia $f : A \to B$.*

1. *f è invertibile a destra se e solo se f è suriettiva.*

2. *f è invertibile a sinistra se e solo se f è iniettiva.*

3. *f è invertibile se e solo se f è biettiva.*

Dimostrazione. (1.) Sia f invertibile a destra, e sia g una sua inversa destra. Poiché id_B è suriettiva, allora f è suriettiva per il punto 2. della Proposizione 2.49. Viceversa, sia f suriettiva. Definiamo $g : B \to A$ come segue: per ogni $b \in B$ scegliamo un $a \in A$ tale che $f(a) = b$ (almeno un a siffatto esiste, per la suriettività di f) e poniamo $g(b) = a$. Allora g è una inversa destra di f.

(2.) Se f è invertibile a sinistra, allora l'iniettività di f segue dal punto 1. della Proposizione 2.49. Viceversa, sia f iniettiva. Allora per ogni $b \in B$ definiamo $g(b)$ come segue: se $b \in \mathrm{Im}(f)$ e $b = f(a)$, poniamo $g(b) = a$ (tale a è unico per l'iniettività di f); se $b \notin \mathrm{Im}(f)$ scegliamo come $g(b)$ un qualsiasi elemento di A. Allora g è una inversa sinistra di f.

(3.) Sia f invertibile, con inversa g. Allora g è inversa destra e inversa sinistra per f, e quindi dai punti (1.) e (2.) segue che f è suriettiva e iniettiva, quindi biettiva. Viceversa, sia f biettiva. Per i punti (1.) e (2.), esistono l'inversa destra g_1 e l'inversa sinistra g_2 di f. Dimostriamo che $g_1 = g_2$, mostrando per ogni $b \in B$ che $g_1(b) = g_2(b)$. Sia $a_1 = g_1(b)$, $a_2 = g_2(b)$, e sia a l'unico elemento di A tale che $f(a) = b$. Allora $b = id_B(b) = (f \circ g_1)(b) = f(g_1(b)) = f(a_1)$; per l'iniettività di f, ne segue $a_1 = a$. Inoltre $a = id_A(a) = (g_2 \circ f)(a) = g_2(f(a)) = g_2(b) = a_2$. Quindi $a_1 = a_2$, e la tesi è dimostrata. □

Notare che in alcuni punti della dimostrazione precedente abbiamo "scelto" un elemento all'interno di un insieme, dando per buono di poter fare "infinite scelte". La possibilità di farlo, che appare del tutto naturale, è esplicitamente assicurata dal cosiddetto "assioma della scelta".

Proposizione 2.54. *Siano $f : A \to B$, $g : B \to C$, $h : C \to D$.*

- *Se f è invertibile, allora la sua inversa è unica, e viene indicata con f^{-1}.*
- *Se f è invertibile, allora anche f^{-1} lo è, con inversa $(f^{-1})^{-1} = f$.*
- *La composizione di funzioni è associativa: $(h \circ g) \circ f = h \circ (g \circ f)$.*

Definizione 2.55. *Sia $A \subseteq B$. La funzione* inclusione canonica *di A in B è definita da*

$$\begin{array}{rccc} i_{A\subseteq B} : & A & \to & B, \\ & a & \mapsto & a. \end{array}$$

Osservazione 2.56. *L'inclusione canonica è iniettiva.*

Definizione 2.57. *Sia $A \subset B$ un sottoinsieme. La* funzione caratteristica *di A è definita da*

$$\begin{array}{rccl} \chi_A: & B & \to & \{0,1\} \\ & a & \mapsto & \begin{cases} 0, & a \notin A; \\ 1, & a \in A. \end{cases} \end{array}$$

Esempio 2.58. *Sia $A = \{a, f, g, h\} \subset \{a, b, c, d, e, f, g, h\} = B$. Allora*

$$\begin{array}{rccl} \chi_A: & B & \to & \{0,1\} \\ & a & \mapsto & 1 \\ & b & \mapsto & 0 \\ & c & \mapsto & 0 \\ & d & \mapsto & 0 \\ & e & \mapsto & 0 \\ & f & \mapsto & 1 \\ & f & \mapsto & 1 \\ & g & \mapsto & 1 \end{array} .$$

Teorema 2.59. *Sia A un insieme. Allora esiste una biezione tra $\mathcal{P}(A)$ e l'insieme di tutte le funzioni tra A e $\{0,1\}$.*

Dimostrazione. Consideriamo la seguente funzione φ definita da

$$\begin{array}{rccl} \varphi: & \mathcal{P}(A) & \to & \{f : A \to \{0,1\}\} \\ & B & \mapsto & \chi_B \end{array} .$$

Ora proviamo che questa funzione è una biezione.

Si ha che φ è iniettiva: se B_1 e B_2 sono due sottoinsiemi distinti di A allora ci sarà almeno un elemento di B_1 che non appartiene a B_2 o un elemento di B_2 che non appartiene a B_1. Sia x tale elemento. Allora per definizione di funzione caratteristica $\chi_{B_1}(x) \neq \chi_{B_2}(x)$ e quindi $\varphi(B_1) \neq \varphi(B_2)$.

Inoltre φ è suriettiva: ogni funzione $f : A \to \{0,1\}$ può essere vista come la funzione caratteristica dell'insieme

$$B = \{b \in A : f(b) = 1\}.$$

□

Ogni funzione deve essere "ben definita": il modo con cui descriviamo la funzione deve rispettare la definizione stessa di funzione, cioè ad ogni elemento del dominio deve associare

essatamente un elemento del codominio. Un caso in cui bisogna assicurarsi che la definizione data sia una "buona definizione" è il seguente.

Sia $\mathcal{R}$ una relazione di equivalenza su A, e $A/\mathcal{R} = \{[a]_\mathcal{R} \mid a \in A\}$ l'insieme quoziente. Vogliamo definire una funzione f con dominio $A/\mathcal{R}$, tramite una "legge" $a \mapsto f([a]_\mathcal{R})$ che dipende da a. Bisogna allora verificare che f sia ben posta, cioè che la legge che la definisce non dipende dal rappresentante scelto per $[a]_\mathcal{R}$. In sostanza, bisogna mostrare che, se $[a']_\mathcal{R} = [a]_\mathcal{R}$ (che significa $a \,\mathcal{R}\, a'$), allora $f([a]_\mathcal{R}) = f([a']_\mathcal{R})$.

Esempio 2.60. *Consideriamo su $\mathbb{R}$ la relazione di equivalenza $x \,\mathcal{R}\, y \iff |x| = |y|$. Definiamo $f : \mathbb{R}/\mathcal{R} \to \mathbb{R}$, $[x]\mathcal{R} \mapsto x^2$. Allora f è ben posta. Infatti: se $[x] = [x']$, allora $|x| = |x'|$, e quindi $x^2 = (x')^2$.*

Consideriamo su $\mathbb{Z}$ la relazione di equivalenza $a \mathcal{R}, b \iff 2 \mid (a - b)$; le classi di equivalenza sono $[0] = \{2k \mid k \in \mathbb{Z}\}$ e $[1] = \{2k + 1 \mid k \in \mathbb{Z}\}$. Definiamo $f : \mathbb{Z}/\mathcal{R} \to \mathbb{N}$ tramite $[a] \mapsto a + 1$. Allora f non è ben posta, perché $[0] \mapsto 1$ e $[2] \mapsto 3$, mentre $[0] = [2]$.

Nel resto della sezione accenniamo ad alcune nozioni riguardanti la cardinalità degli insiemi, omettendo le dimostrazioni dei risultati enunciati.

Definizione 2.61. *Due insiemi A e B hanno la stessa* cardinalità *se esiste una funzione biettiva $f : A \to B$. Si dice anche che A e B sono* equipotenti. *Si indica con $|A| = |B|$.*

Osserviamo che "avere la stessa cardinalità" è una relazione di equivalenza. Infatti, la funzione identità $id : A \to A$ è biettiva (riflessività); se $f : A \to B$ è biettiva, allora f è invertibile e $f^{-1} : B \to A$ è biettiva (simmetria); se $f : A \to B$ e $g : B \to C$ sono biettive, allora $g \circ f : A \to C$ è biettiva (transitività).

Definizione 2.62. *Se A ha la stessa cardinalità dell'insieme $\{1, \ldots, n\}$ dei primi n numeri naturali positivi, si scrive $|A| = n$ e si dice che A è un insieme finito di ordine n (cioè, A ha esattamente n elementi). Se $A = \emptyset$, scriviamo che $|A| = 0$.*

Se $|A| \neq n$ per ogni numero naturale n, si dice che A è un insieme infinito.

Un insieme A si dice numerabile *se $|A| = |\mathbb{N}|$.*

Il motivo del nome "numerabile" è chiaro: se $|A| = |\mathbb{N}|$, allor esiste una biezione $\mathbb{N} \to A$, $n \mapsto f(n)$; e quindi $f(0), f(1), f(2), \ldots$ è una "enumerazione" di tutti gli elementi di A.

Esempio 2.63. *Sia $\square := \{0, 1, 4, 9, \ldots\} = \{k^2 \mid k \in \mathbb{N}\}$. Allora la funzione $\mathbb{N} \to \square$, $n \mapsto n^2$, è una biezione.*

La funzione $\mathbb{N} \to \mathbb{Z}$, $n \mapsto (-1)^n \lceil n/2 \rceil$, *è una biezione (l'"enumerazione" di* $\mathbb{Z}$ *qui è:* $0, -1, 1, -2, 2, \ldots$*).*

Si dimostra che anche l'insieme $\mathbb{Q}$ *dei numeri razionali è numerabile.*

Invece l'insieme $\mathbb{R}$ *dei numeri reali non è numerabile, ma è equipotente all'insieme* $\mathcal{P}(\mathbb{N})$ *di tutti i sottoinsiemi di* $\mathbb{N}$.

L'esempio precedente mostra una proprietà, che vale in generale.

Proposizione 2.64. *Un insieme* A *è infinito se e solo ammette un sottoinsieme proprio* $B \subsetneq A$ *tale che* $|A| = |B|$.

Il confronto tra cardinalità è definito come segue.

Definizione 2.65. *Dati due insiemi* A *e* B*, si dice che la cardinalità di* A *e minore o uguale alla cardinalità di* B*, e si scrive* $|A| \leq |B|$*, se esiste una funzione iniettiva* $f : A \to B$.

Tutte le cardinalità sono confrontabili (questo risultato è noto come teorema di Hartogs, ed è equivalente al cosidetto *assioma della scelta*).

Proposizione 2.66. *Dati due insiemi* A *e* B*, si ha sempre* $|A| \leq |B|$ *oppure* $|B| \leq |A|$.

Possiamo ora enunciare il teorema di Cantor-Schröder-Bernstein.

Teorema 2.67. *Siano* A *e* B *due insiemi qualunque. Se* $|A| \leq |B|$ *e* $|B| \leq |A|$*, allora* $|A| = |B|$*. In altre parole: se esistono due funzioni iniettive* $f : A \to B$ *e* $g : B \to A$*, allora esiste una funzione biettiva* $h : A \to B$.

Dimostriamo infine che l'insieme delle parti di un insieme ha cardinalità maggiore dell'insieme stesso.

Proposizione 2.68. *Sia* A *un insieme. Allora* $|A| < |\mathcal{P}(A)|$.

Dimostrazione. Dobbiamo dimostrare che $|A| \leq |\mathcal{P}(A)|$ e $|A| \neq |\mathcal{P}(A)|$, cioè esiste una funzione iniettiva di A in $\mathcal{P}(A)$, ma non esiste nessuna funzione biettiva da A a $\mathcal{P}(A)$.

La funzione $A \to \mathcal{P}(A)$, $x \mapsto \{x\}$ è chiaramente iniettiva. Supponiamo ora per assurdo che esiste una funzione biettiva $f : A \to \mathcal{P}(A)$. In particolare, f è suriettiva. Definiamo il seguente sottoinsieme di A:

$$B := \{x \in A \colon x \notin f(x)\} \subseteq A.$$

Poiché f è suriettiva, esiste $a \in A$ tale che $f(a) = B$. Per definizione di B, tale a soddisfa

$$a \in f(a) \iff a \notin f(a),$$

che è chiaramente una contraddizione. □

2.5 Esercizi

Esercizio 2.1. *Dato un insieme con tre elementi $A = \{a, b, c\}$, stabilire quali delle seguenti relazioni su A sono riflessive, simmetriche, antisimmetriche o transitive:*

$$\mathcal{R}_1 = \{(a,a),(b,b),(c,c),(b,c)\}, \quad \mathcal{R}_2 = \{(b,c),(c,b)\}, \quad \mathcal{R}_3 = \{(a,b),(b,a),(a,a),(b,b)\}.$$

Rappresentare $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$ con un grafo diretto e con una matrice $0-1$.

Esercizio 2.2. *Per ogni relazione binaria $\mathcal{R}$ su $\mathbb{N}$ descritta nel seguito, stabilire se $\mathcal{R}$ è una relazione riflessiva, simmetrica o transitiva.*

- $\mathcal{R} = \{(x,y) \in \mathbb{N}^2 \ : \ (2 \mid x) \wedge (2 \mid y)\}$.
- $\mathcal{R} = \{(x,y) \in \mathbb{N}^2 \ : \ x \geq y\}$.
- $\mathcal{R} = \{(x,y) \in \mathbb{N}^2 \ : \ (x \mid y) \vee (y \mid x)\}$.

Esercizio 2.3. *Sia data la seguente relazione $\mathcal{R}$ su $\mathbb{Z}$ definita da*

$$a\mathcal{R}b \quad \iff \quad 2 \mid a+b.$$

Tale relazione è una relazione di equivalenza? In caso affermativo determinare l'insieme quoziente.

Soluzione. La relazione $\mathcal{R}$ è riflessiva perché $2 \mid (a+a) = 2a$ per ogni $a \in \mathbb{Z}$. Inoltre è simmetrica, in quanto se $2 \mid a+b$ allora $2 \mid b+a$. Infine, è transitiva: se $2 \mid a+b$ e $2 \mid b+c$ allora $2 \mid (a+b+b+c) = a+2b+c$. Poiché 2 divide $2b$, allora 2 divide anche $a+c$. Quindi $\mathcal{R}$ è una relazione di equivalenza. In particolare, due numeri sono in relazione se e solo se sono entrambi pari o entrambi dispari. Pertanto l'insieme quoziente è $\mathbb{Z}/\mathcal{R} = \{[0],[1]\}$.

Esercizio 2.4. *La relazione binaria $\mathcal{R}$ su $\mathbb{Z}$ definita da*

$$x\mathcal{R}y \iff 2 \nmid (x+y)$$

è una relazione di equivalenza su $\mathbb{Z}$?

Esercizio 2.5. *La relazione binaria $\mathcal{R}$ su $\mathbb{N}^* \times \mathbb{N}^*$ definita da*

$$(a,b)\mathcal{R}(c,d) \iff ad = bc$$

è una relazione di equivalenza su $\mathbb{N}^* \times \mathbb{N}^*$? Se sì, qual è la classe di equivalenza di $(1,1)$?

Esercizio 2.6. *Sia data la seguente relazione $\mathcal{R}$ su $\mathbb{Z} \setminus \{0\}$ definita da*

$$a\mathcal{R}b \quad \iff \quad ab > 0.$$

Tale relazione è una relazione di equivalenza? Se sì, determinare l'insieme quoziente.

Soluzione. la relazione è riflessiva poiché $a^2 > 0$ per ogni $a \neq 0$. Inoltre se $ab > 0$ allora chiaramente anche $ba > 0$. Infine, se $ab > 0$ e $bc > 0$ allora

$$(ab)(bc) = ab^2c > 0.$$

Siccome $b^2 > 0$ per ogni $b \neq 0$, anche $ac > 0$. La relazione è dunque una relazione di equivalenza. Ogni numero positivo è in relazione con ogni altro numero positivo. D'altra parte ogni numero negativo è in relazione con ogni altro numero negativo. Pertanto l'insieme quoziente $\mathbb{Z}^*/\mathcal{R} = \{[1],[-1]\}$.

Esercizio 2.7. *Si consideri l'insieme $E = \{1,2,3,4,5,6\}$. La seguente relazione $\mathcal{R}$ definita da*

$$x\mathcal{R}y \quad \iff \quad 5 \mid 2x + 3y$$

Scrivere una matrice $M_{\mathcal{R}}$ e disegnare un grafo $G_{\mathcal{R}}$ che rappresentano $\mathcal{R}$.
$\mathcal{R}$ è una relazione di equivalenza? In caso affermativo esibire il relativo insieme quoziente.

Soluzione. Descriviamo esplicitamente le coppie di elementi in relazione:

$$\mathcal{R} = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(1,6),(6,1)\}.$$

Si vede chiaramente che la relazione è riflessiva e simmetrica. Inoltre è transitiva dato che non ci sono coppie $a\mathcal{R}b$, $b\mathcal{R}c$ formate da tre elementi distinti. La relazione è di equivalenza e l'insieme quoziente è

$$E/\mathcal{R} = \{[1],[2],[3],[4],[5]\}.$$

Esercizio 2.8. *La relazione binaria $\mathcal{R}$ su $\mathbb{Z}$ definita da*

$$x\mathcal{R}y \iff x^2 = y^2$$

è una relazione di equivalenza su $\mathbb{Z}$?

Esercizio 2.9. *La relazione binaria $\mathcal{R}$ su $\mathbb{R}$ definita da*

$$x\mathcal{R}y \iff x - y \in \mathbb{Z}$$

è una relazione di equivalenza su $\mathbb{R}$?

Esercizio 2.10. *La relazione binaria $\mathcal{R}$ su $\mathbb{R}^2$ definita da*

$$(x, y)\mathcal{R}(z, t) \iff x + y = z + t$$

è una relazione di equivalenza su $\mathbb{R}^2$?

Esercizio 2.11. *La relazione binaria $\mathcal{R}$ su $A = \{f : \mathbb{R} \to \mathbb{R}\}$ definita da*

$$f\mathcal{R}g \iff f(1) = g(1)$$

è una relazione di equivalenza su A?

Soluzione. È necessario fare attenzione agli oggetti sui quali è definita la relazione, in quanto queste sono funzioni. La relazione è riflessiva dato che $f(1) = f(1)$ e quindi $f\mathcal{R}g$. Inoltre è simmetrica, in quanto se $f\mathcal{R}g$ allora $f(1) = g(1)$ che è equivalente a $g(1) = f(1)$, ovvero $g\mathcal{R}f$. Infine $\mathcal{R}$ è transitiva, in quanto se $f(1) = g(1)$ e $g(1) = h(1)$ allora necessariamente $f(1) = h(1)$ e dunque $f\mathcal{R}h$.

Esercizio 2.12. *La relazione binaria $\mathcal{R}$ su $A = \{f : \mathbb{N} \to \mathbb{N}\}$ definita da*

$$f\mathcal{R}g \iff \exists k \in \mathbb{N} : (\forall n \geq k \implies f(n) = g(n))$$

è una relazione di equivalenza su A?

Esercizio 2.13. *Sia data la seguente relazione $\mathcal{R}$ su $\mathbb{Z}^2$ definita da*

$$(a, b)\mathcal{R}(c, d) \quad \iff \quad a + d = b + c.$$

Tale relazione è una relazione di equivalenza? In caso affermativo determinare l'insieme quoziente.

Soluzione. La relazione è riflessiva perché $a + b = b + a$. Inoltre è simmetrica poiché se $a + d = b + c$ allora $c + b = d + a$. Infine, se $a + d = b + c$ e $c + f = d + e$ si ha che $a + d + c + f = b + c + d + e$, ovvero $a + f = b + e$. La relazione è quindi di equivalenza. Si può notare che due coppie (a, b) (c, d) e sono in relazione se e solo se $a - b = c - d$, ovvero se e solo se la differenza tra il primo e il secondo elemento di ogni coppia è costante. Pertanto l'insieme quoziente è

$$\mathbb{Z}^2/\mathcal{R} = \{[(a, 0)] \mid a \in \mathbb{Z}\}.$$

Esercizio 2.14. *Si consideri la seguente relazione σ su $\mathbb{R}$:*

$$x\mathcal{R}y \iff |x-y| \in \mathbb{N}.$$

Si dica se tale relazione è riflessiva, transitiva, simmetrica. Se è di equivalenza determinare l'insieme quoziente.

Soluzione. Mostriamo che $\mathcal{R}$ è riflessiva: dato che per ogni $x \in \mathbb{R}$ si cha che $|x - x| = 0 \in \mathbb{N}$ allora $\mathcal{R}$ è riflessiva. Poiché $|x-y| = |y-x|$ per ogni $x, y \in \mathbb{R}$ allora $\mathcal{R}$ è simmetrica. Supponiamo ora che $x\mathcal{R}y$ e $y\mathcal{R}z$, cioè che $|x-y| \in \mathbb{N}$ e $|y-z| \in \mathbb{N}$. Allora $|x-z| = |x-y| \pm |y-z|$ e quindi appartiene sempre a $\mathbb{N}$. Un modo per vedere questo è il seguente: dire $|x-y| \in \mathbb{N}$ equivale a dire $x = y+k$, con $k \in \mathbb{Z}$. Allora $|x-y| \in \mathbb{N}$ e $|y-z| \in \mathbb{N}$ equivalgono a $x = y+k$ e $y = z+j$ per qualche $k, j \in \mathbb{Z}$. Allora $x = y+k = z+j+k$, ovvero $x - z = k + j \in \mathbb{Z}$, e dunque $|x-z| \in \mathbb{N}$.

Dunque $\mathcal{R}$ è di equivalenza. Dato un certo $x \in \mathbb{R}$ la sua classe di equivalenza è

$$[x] = \{x + a \mid a \in \mathbb{Z}\}.$$

Dunque l'insieme quoziente è

$$\mathbb{R}/\mathcal{R} = \{\{x + a \mid a \in \mathbb{Z}\} \quad | \quad x \in \mathbb{R}\}.$$

Esercizio 2.15. *Nell'insieme $\mathbb{Z}$ dei numeri interi si consideri la relazione $\mathcal{R}$ definita da $a\rho b \iff a^2 - b^2 = 4b - 4a$ per ogni $a, b \in \mathbb{Z}$.*

1. *Dimostrare che la relazione $\mathcal{R}$ è di equivalenza.*
2. *Determinare esplicitamente almeno un numero $c \in \mathbb{Z}$ tale che c non sia $\mathcal{R}$–equivalente a 4 (cioè tale che c non appartiene alla classe di equivalenza di 4).*
3. *Determinare esplicitamente un numero $c \in \mathbb{Z}$ tale che c sia $\mathcal{R}$-equivalente a 4.*

Esercizio 2.16. *Indicato con $D(n) \subseteq \mathbb{N}$ l'insieme di tutti i divisori di n e con $|$ la relazione di divisibilità, disegnare i diagrammi di Hasse dei seguenti insiemi ordinati: $(D(36), |)$, $(D(30), |)$, $(D(18), |)$, $(D(32), |)$, $(D(35), |)$, $D(24), |)$.*

Esercizio 2.17. *Sia $A = \{0, 1, 2, \ldots, 11\}$, e sia $\mathcal{R}$ la relazione su A definita da*

$$a\,\mathcal{R}\,b \quad \iff \quad a = b \text{ oppure } 5a < 2b,$$

dove $\leq$ indica l'ordine usuale su $\mathbb{N}$.

- *Verificare che $\mathcal{R}$ è una relazione d'ordine su A.*
- *Disegnare il diagramma di Hasse di $(A, \mathcal{R})$.*
- *Stabilire se $(A, \mathcal{R})$ è ben ordinato.*
- *Determinare gli eventuali elementi massimali, minimali, massimo e minimo di $(A, \mathcal{R})$.*
- *Determinare tutti i maggioranti in A del sottoinsieme $\{1, 2\}$.*
- *Determinare, se esistono, l'estremo superiore e l'estremo inferiore di $\{1, 2\}$.*

Esercizio 2.18. *Considerare il poset*

$$(\{\{1\}, \{2\}, \{4\}, \{1, 2\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}, \subseteq)$$

- *Trovare gli elementi massimali e minimali.*
- *Trovare, se esistono, massimo e minimo.*
- *Dato l'insieme $\{\{2\}, \{4\}\}$, trovarne tutti i maggioranti e, se esiste, l'estremo superiore.*
- *Dato $\{\{1, 3, 4\}, \{2, 3, 4\}\}$, trovarne tutti i minoranti e, se esiste, l'estremo inferiore.*

Esercizio 2.19. *Un poset $(P, \preccurlyeq)$ è detto* ben fondato *se non ammette sequenze infinite strettamente decrescenti, cioè se non ammette sottoinsiemi infiniti $A = \{x_1, x_2, x_3, \ldots\}$ tali che $\cdots \prec x_3 \prec x_2 \prec x_1$. Un poset $(P, \preccurlyeq)$ è detto* denso *se per ogni $x, y \in P$ con $x \prec y$ esiste un elemento $z \in P$ tale che $x \prec z \prec y$.*

1. *Dimostrare che $(\mathbb{Z}, \preccurlyeq)$ con $x \preccurlyeq y \iff x = y \vee |x| < |y|$ è ben fondato ma non totalmente ordinato.*
2. *Dimostrare che un poset denso con almeno due elementi distinti confrontabili non è ben fondato.*
3. *Dimostrare che il poset $(\mathbb{Q}, \leq)$ è denso.*
4. *Dimostrare che un poset è ben ordinato se solo se è totalmente ordinato e ben fondato.*
5. *Dimostrare che $(\mathbb{Z}, \preccurlyeq)$ con $x \preccurlyeq y \iff |x| < |y| \ \vee \ (|x| = |y| \wedge x \leq y)$ è un poset ben ordinato.*

6. Si consideri il poset $(\mathbb{Z}, \preccurlyeq)$ con $x \preccurlyeq y$ se e solo se

$$(x = 0) \ \vee \ (x > 0 \wedge y < 0) \ \vee \ (x > 0 \wedge y > 0 \wedge x \leq y) \ \vee \ (x < 0 \wedge y < 0 \wedge |x| \leq |y|).$$

Dimostrare che $(\mathbb{Z}, \preccurlyeq)$ è un poset ben ordinato.

Soluzione. (1) Il poset $(\mathbb{Z}, \preccurlyeq)$ non è totalmente ordinato perché due elementi distinti con lo stesso valore assoluto (ad esempio, 1 e -1) non sono confrontabili. Se $\cdots \prec x_3 \prec x_2 \prec x_1$, allora i numero naturali $|x_i|$ verificano $\cdots < |x_3| < |x_2| < |x_1|$. Poiché $\mathbb{N}$ ha un numero finito di elementi minori strettamente di $|x_1|$, allora la sequenza degli x_i è finita. Quindi $(\mathbb{Z}, \preccurlyeq)$ è ben fondato.

(2) Se $(P, \preccurlyeq)$ è denso e $x, x_1 \in P$ verificano $x \prec x_1$, allora esiste $x_2 \in P$ con $x \prec x_2 \prec x_1$. Sempre per densità, esiste $x_3 \in P$ tale che $x \prec x_3 \prec x_2$. Continuando in questo modo a inserire strettamente un elemento x_i tra x e x_{i-1}, si trova la sequenza infinita $x_1, x_2, x_3, \ldots \in P$ con $x_i \prec x_{i-1}$ per ogni i, quindi $(P, \preccurlyeq)$ non è ben fondato.

(3) La densità dei numeri razionali rispetto all'ordinamento usuale è una ben nota proprietà: siano $x, y \in \mathbb{Q}$ con $x < y$, allora $z = (x + y)/2$ verifica $x < z < y$. Quindi $(\mathbb{Q}, \leq)$ è denso.

(4) Sia $(P, \preccurlyeq)$ ben ordinato. Se per assurdo P non fosse ben fondato, allora esisterebbe un sottoinsieme infinito $A = \{x_1, x_2, \ldots\} \subseteq P$ con $x_{i+i} \prec x_i$ per ogni $i \geq 1$; in tal caso, A non ammette minimo, contro l'ipotesi di buon ordine di P. Quindi P è ben fondato. Inoltre, P è è totalmente ordinato per la Proposizione 2.32 (cioé: per ogni $x, y \in P$, $\{x, y\}$ ammette massimo e minimo, che sono x e y o viceversa, e quindi x e y sono confrontabili).

Viceversa, sia $(P, \preccurlyeq)$ totalmente ordinato e ben fondato. Supposiamo per assurdo che esista un sottoinsieme non vuoto $B \subseteq P$ che non ammette minimo. Sia $x_1 \in B$. Poichè x_1 non è il minimo di B, e tutti gli elementi di B sono confrontabili con x_1 (P è totalmente ordinato), allora esiste $x_2 \in B$ con $x_2 \neq x_1$ e $x_1 \not\prec x_2$. Poiché A è totalmente ordinato, questo implica che $x_2 \prec x_1$. Poiché x_2 non è il minimo di B e tutti gli elementi di B sono confrontabili con x_2, esiste $x_3 \in B$ con $x_3 \prec x_2 \prec x_1$. Iterando il ragionamento, si trova una sequenza infinita $x_1, x_2, \ldots \in B$ tale che $x_{i+1} \prec x_i$ per ogni $i \geq 1$, che è assurdo perché P è ben fondato. Quindi ogni sottoinsieme non vuoto di P ha minimo, e P è ben ordinato.

(5) La dimostrazione è lasciata per esercizio. Si noti che questo ordine su $\mathbb{Z}$ può essere visalizzato come segue:

$$0 \prec -1 \prec 1 \prec -2 \prec 2 \prec -3 \prec 3 \prec \ldots$$

(6) La dimostrazione è lasciata per esercizio. Si noti che questo ordine su $\mathbb{Z}$ può essere visualizzato come segue:

$$0 \prec 1 \prec 2 \prec 3 \prec \ldots \prec -1 \prec -2 \prec -3 \prec \ldots$$

Esercizio 2.20. *Date le seguenti relazioni da $\mathbb{N}$ a $\mathbb{Z}$, determinare quali di esse sono funzioni (motivando la risposta), e in tal caso se sono iniettive suriettive, biettive:*

$$n\mathcal{R}_1 z \iff n+z=3, \quad n\mathcal{R}_2 z \iff n+4=z, \quad n\mathcal{R}_3 z \iff n=z^3 \quad n\mathcal{R}_4 z \iff z=-n^2,$$

$$n\mathcal{R}5z \iff n=|z|, \quad n\mathcal{R}_6 z \iff z+11=n, \quad n\mathcal{R}_7 z \iff n+4>z.$$

Esercizio 2.21. *Date le seguenti relazioni da $\mathbb{N}$ a $\mathbb{Q}$, determinare quali di esse sono funzioni (motivando la risposta), e in tal caso se sono iniettive suriettive, biettive:*

$$x\mathcal{R}_1 y \iff 5x^2=4y, \quad x\mathcal{R}_2 y \iff 5x=4|y|, \quad x\mathcal{R}_3 y \iff 5x=4y \quad x\mathcal{R}_4 y \iff 5x=4y^2.$$

Esercizio 2.22. *Determinare quali delle seguenti funzioni sono iniettive e/o suriettive. In caso non lo siano, restringere il dominio o il codominio affinché la nuova funzione sia biiettiva. $f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^3-1$.*

Soluzione. Per determinare l'eventuale iniettività della funzione procediamo seguendo la definizione. Siano $x_1, x_2 \in \mathbb{R}$ tali che $f(x_1)=f(x_2)$, se l'unica soluzione è $x_1=x_2$ allora f è iniettiva. Si ha allora

$$x_1^3-1=x_2^3-1$$

$$x_1^3-x_2^3=0$$

$$(x_1-x_2)(x_1^2+xy+x_2^2)=0.$$

Per la legge di annullamento del prodotto si ha che

$$x_1-x_2=0 \text{ cioè } x_1=x_2,$$

oppure

$$x_1^2+xy+x_2^2=0, \text{ che implica } x_1=x_2=0.$$

In entrambi i casi si ha $x_1=x_2$, pertanto f è iniettiva nel suo dominio. Per avere la suriettività dobbiamo vedere se $\forall y\in\mathbb{R}$, $\exists x\in\mathbb{R}$ tale che $y=x^3-1$. Risolvendo l'equazione secondo x si trova facilmente $x=\sqrt[3]{y+1}$, che è la soluzione cercata. Quindi f è suriettiva.

Esercizio 2.23. *Determinare quali delle seguenti funzioni sono iniettive e/o suriettive. In caso non lo siano, restringere il dominio o il codominio affinché la nuova funzione sia biiettiva.*

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$.
- $f : \mathbb{R}^+ \to \mathbb{R}$, $f(x) = x^3$.
- $f : \mathbb{Z}^- \to \mathbb{R}$, $f(x) = x^2 - 1$.
- $f : \mathbb{N} \to \mathbb{Q}$, $f(x) = \frac{3}{5}x^4$.
- $f : \mathbb{N} \to \mathbb{Q}$, $f(x) = \frac{3}{5}x^3$.

Capitolo 3

Elementi di Calcolo Combinatorio

In questo capitolo presentiamo alcune tecniche di conteggio, elementari ma molto utili. Ricordiamo che, se A è finito, la cardinlità $|A|$ è il numero di elementi di A.

3.1 Disposizioni, permutazioni, combinazioni

Definizione 3.1. *Sia n un intero positivo. Si definisce* fattoriale *di n il numero*

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

Si assume per definizione che $0! = 1$.

Definizione 3.2. *Siano h, n numeri naturali con $h \leq n$. Si definisce* coefficiente binomiale*, e si indica con $\binom{n}{h}$, il numero*

$$\binom{n}{h} = \frac{n(n-1)\dots(n-h+1)}{h!} = \frac{n!}{h!(n-h)!}$$

Definizione 3.3. *Una* disposizione semplice *di n oggetti in gruppi di k, con $k \leq n$, è una lista ordinata di k elementi distinti scelti tra gli n oggetti.*

Quindi, nelle disposizioni semplici non ci sono ripetizioni, e l'ordine è importante.

Definizione 3.4. *Una* permutazione *di n oggetti è una disposizione semplice di n oggetti in gruppi di n.*

Il numero delle permutazioni di k oggetti viene indicato con $P_k = k!$.

Proposizione 3.5. *Il numero di disposizioni semplici di n oggetti in gruppi di k è dato da*

$$D_{n,k} = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

Dimostrazione. Consideriamo la lista da costruire come una sequenza di k caselle da riempire con un elemento dagli n di partenza. La prima casella può ospitare uno qualsiasi degli n elementi. Una volta riempita questa casella, la seconda può contenere un elemento scelto tra i rimanenti $n-1$, in quanto non sono ammesse ripetizioni. Nella terza le possibilità scendono a $n-2$ e così via fino ad arrivare alla k-esima casella in cui possiamo mettere un oggetto a scelta tra $n-k+1$ non ancora scelti. Si noti che due liste differenti possono contenere anche gli stessi elementi ma posti in ordine differente. □

Esempio 3.6. *Sia A un insieme con k elementi e B un insieme con n elementi, con $k \leq n$.*

Allora il numero di funzioni iniettive da A a B è $D_{n,k} = \frac{n!}{(n-k)!}$. In particolare, il numero di permutazioni di B (cioè, biezioni da B a B) è $n!$.

Definizione 3.7. *Una* combinazione semplice *di n oggetti in gruppi di k, con $k \leq n$, è un insieme di k elementi distinti scelti tra gli n oggetti.*

Quindi, nelle combinazioni semplici non ci sono ripetizioni, e l'ordine non conta.

Si dice anche che una combinazione semplice è un k-sottoinsieme (= sottoinsieme di cardinalità k) di un insieme di n oggetti.

Proposizione 3.8. *Il numero di combinazioni semplici di n oggetti in gruppi di k è dato da*

$$C_{n,k} = \binom{n}{k} = \frac{D_{n,k}}{k!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1} = \frac{n!}{(n-k)!k!}.$$

Dimostrazione. Consideriamo il numero di liste ordinate di lunghezza k che possiamo formare con k elementi distinti a partire dagli n oggetti. Questo numero equivale a $D_{n,k}$. Data una lista ordinata ci sono esattamente $D_{k,k} = P_k$ liste ordinate che hanno esattamente gli stessi elementi e differiscono solo per l'ordine. Pertanto il numero di insiemi di k oggetti senza ripetizioni sono $\frac{D_{n,k}}{P_k}$. □

$C_{n,k} = \binom{n}{k}$ significa quindi che $\binom{n}{k}$ è il numero di k-sottoinsiemi in un n-insieme.

Definizione 3.9. *Una* disposizione con ripetizione *di n oggetti in gruppi di k è una lista ordinata di k elementi, eventualmente ripetuti, scelti tra gli n.*

Proposizione 3.10. *Il numero di disposizioni con ripetizione di n oggetti in gruppi di k è*

$$D'_{n,k} = n^k.$$

Dimostrazione. Consideriamo la lista da costruire come una sequenza di k caselle da riempire con un elemento dagli n di partenza. Ogni casella può ospitare uno qualsiasi degli n elementi. Il numero totale è dato quindi da $n \cdot n \cdots n = n^k$. Si noti che due liste differenti possono contenere anche gli stessi elementi ma posti in ordine differente. □

Osservazione 3.11. *$D'_{n,k}$ è uguale al numero di funzioni da un insieme di k elementi a un insieme di n elementi.*

Esempio 3.12. *Sia A un insieme finito con m elementi.*

Il numero di relazioni (binarie) su A è uguale a $D'_{2,m} = 2^{m^2}$. Infatti una relazione $\mathcal{R}$ su A è definita univocamente dalla matrice $M_{\mathcal{R}}$ con m righe e m colonne a valori 0 e 1; quindi nella matrice ci sono m^2 posizioni in cui insrire uno dei due oggetti 0 e 1.

Il numero di relazioni riflessive su A, così come il numero di relazioni antiriflessive, è 2^{m^2-m}, perché possiamo scegliere il valore 0 o 1 per tutti gli m^2 posti nella matrice tranne gli m posti sulla diagonale principale.

Il numero di relazioni simmetriche su A è $2^{m+(m-1)+\cdots+2+1} = 2^{m(m+1)/2}$, perché il valore 0 o 1 nelle posizioni (i, j) con $i \leq j$ (dalla diagonale principale in su) le possiamo scegliere liberamente, ma poi le altre sono determinate dalla condizione $m_{ji} = m_{ij}$.

Definizione 3.13. *Una* permutazione con ripetizione *di k oggetti $a_1, \ldots, a_k$ in cui a_1 si ripete n_1 volte, …, a_k si ripete n_k volte, è una lista ordinata di n elementi, $n = n_1 + \cdots + n_k$, di cui n_1 coincidono con a_1, …, n_k coincidono con a_k.*

Proposizione 3.14. *Il numero di permutazioni con ripetizioni di elementi $a_1 \ldots, a_k$ ripetuti rispettivamente $n_1, \ldots, n_k$ volte è*

$$P'_{n_1,\ldots,n_k} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}.$$

Dimostrazione. Construiamo tutte le $n!$ permutazioni come se gli elementi delle n-uple fossero tutti distinti. Comunque permutiamo in tutti gli $n_1!$ modi possibili gli n_1 elementi uguali ad a_1, la n-upla non cambia (abbiamo scambiato tra loro elementi uguali ad a_1). Perciò dividiamo $n!$ per $n_1!$. Procedendo in questo modo, si ottiene il risultato. □

Definizione 3.15. *Una* combinazione con ripetizione *di n oggetti in gruppi di k è un multi-insieme di k elementi, eventualmente ripetuti, scelti tra gli n oggetti. Conta il numero di ripetizioni di ogni oggetto, ma non conta l'ordine degli elementi nel multi-insieme.*

Abbiamo usato il termine "multi-insieme" per descrivere il fatto che si tiene conto di quante volte un elemento appare nel multi-insieme (a differenza di quanto succede in un normale insieme).

Proposizione 3.16. *Il numero di combinazioni con ripetizione di n oggetti in gruppi di k è dato da*

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

Dimostrazione. Ordiniamo il multi-insieme di k oggetti (con ripetizioni) in modo tale che gli oggetti dello stesso tipo siano successivi. Per semplicità supponiamo che gli oggetti siano $a_1, \dots, a_n$. Un multi-insieme può quindi essere rappresentato come

$$\underbrace{a_1, a_1, \dots, a_1}_{\alpha_1}, \dots, \underbrace{a_n, a_n, \dots, a_n}_{\alpha_n},$$

con $\alpha_1 + \cdots + \alpha_n = k$. Di fatto quello che ci serve è solo sapere in che posizione si passa dall'elemento a_i all'elemento a_{i+1}. A tale scopo utilizziamo $n-1$ simboli nuovi Y_i: l'insieme precedente può essere quindi rappresentato come

$$\underbrace{x, x, \dots, x}_{\alpha_1}, Y_2, \dots, Y_n, \underbrace{x, x, \dots, x}_{\alpha_n}.$$

Si noti che ora il nostro insieme è descritto mediante una $n+k-1$ upla, di cui a noi interessa sapere solo dove si posizionano i simboli Y_i. Pertanto determinare il numero di tali insiemi è equivalente a trovare il numero di combinazioni di di $n+k-1$ oggetti in gruppi di $n-1$. □

Un utilizzo importante del coefficiente binomiale è il seguente.

Teorema 3.17. (Binomio di Newton) *Siano x, y due indeterminate, e $n \in \mathbb{N}$. Allora*

$$\begin{aligned}(x+y)^n &= \textstyle\sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i \\ &= \textstyle\binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.\end{aligned}$$

Dimostrazione. $(x+y)^n$ è un prodotto di n fattori uguali a $x+y$, il cui sviluppo si ottiene scegliendo x oppure y da ogni fattore $x+y$, e moltiplicandoli tutti tra di loro. Quindi lo sviluppo di $(x+y)^n$ contiene solo monomi del tipo $x^j y^i$, dove i è il numero di fattori $x+y$

da cui si è scelto y, mentre $j = n - i$ è il numero di fattori $x + y$ da cui si è scelto x. Perciò il coefficiente di $x^{n-i}y^i$ coincide con il numero di possibili scelte di i fattori tra gli n fattori disponibili, e questo numero è $\binom{n}{i}$. □

Corollario 3.18. *Ponendo nel binomio di Newton $x = y = 1$, si ottiene*

$$2^n = \sum_{i=0}^{n} \binom{n}{i}.$$

Valgono anche le seguenti proprietà: per ogni $h = 0, \ldots, n$ e $k = 1, \ldots, n$,

$$\binom{n}{h} = \binom{n}{n-h}, \qquad \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

Il *triangolo di Tartaglia* è la rappresentazione dei coefficienti binomiali come segue:

$$\begin{array}{ccccc} \binom{1}{0} & \binom{1}{1} & & & \\ \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & \\ \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

Nella prima riga ci sono i coefficienti per lo sviluppo di $(x+y)^1$, nella seconda riga i coefficienti per lo sviluppo di $(x + y)^2$, e così via.

3.2 Alcune tecniche di conteggio

Teorema 3.19. (Principio di moltiplicazione) *Se A e B sono insiemi finiti, allora*

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

Se $A_1, \ldots, A_k$ ($k \geq 2$) sono insiemi finiti, allora

$$|A_1 \times \cdots \times A_k| = |A_1| \cdot \ldots \cdot |A_k|.$$

Possiamo interpretare il principio di moltiplicazione in questo modo: se dobbiamo fare k scelte indipendenti tra loro, e abbiamo a_i possibilità per ciascuna scelta ($i = 1, \ldots, k$), allora il numero totale delle scelte è $a_1 \cdot a_2 \cdot \ldots \cdot a_k$.

Esempio 3.20. *Dati due insiemi finiti A e B, il numero delle funzioni da A a B è*

$$|\{f : A \to B \text{ funzione}\}| = |B|^{|A|}$$

Infatti, se $n = |A|$ e $A = \{a_1, \dots, a_n\}$, allora ogni funzione $f : A \to B$ è univocamente determinata dalla scelta delle immagini degli a_i, cioè dalla n-upla $(f(a_1), \dots, f(a_n))$. Poiché ogni $f(a_i)$ può assumere $|B|$ valori, il numero delle funzioni è $\underbrace{|B| \cdot \ldots \cdot |B|}_{n \text{ volte}} = |B|^{|A|}$.

Corollario 3.21. *Il numero di sottoinsiemi di un insieme finito A è*

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Infatti, per il Teorema 2.59, $|\mathcal{P}(A)|$ è uguale al numero di funzioni da A a $\{0, 1\}$, che per l'esempio precedente vale $|\{0, 1\}|^{|A|} = 2^{|A|}$.

Osservazione 3.22. *Un'altra tecnica è quella del* doppio conteggio*:*
siano X, Y due insiemi finiti, $\mathcal{R}$ una relazione da X a Y, e

$$I = \{(x, y) \in X \times Y \mid x \mathcal{R} y\}.$$

Allora $|I|$ si può contare in due modi: enumerando prima gli elementi di X, oppure enumerando prima gli elementi di Y. Uguagliando i due modi, otteniamo:

$$\sum_{x \in X} |\{y \in Y : x \mathcal{R} y\}| = \sum_{y \in Y} |\{x \in X : x \mathcal{R} y\}|.$$

Ad esempio, supponiamo per semplicità per ogni elemento $x \in X$ ci siano esattamente r elementi $y \in Y$ tali che $x \mathcal{R} y$, e che per ogni elemento $y \in Y$ ci siano esattamente s elementi $x \in X$ tali che $x \mathcal{R} y$.

$$|X| \cdot r = |Y| \cdot s.$$

Se conosco già tre delle quantità $|X|, r, |Y|, s$, posso usare questa uguaglianza per trovare la quarta quantità.

Esempio 3.23. *Il lemma delle strette di mano è il seguente: in un grafo non diretto, il numero di vertici di grado dispari è pari. Enunciato in altri termini: in un gruppo di persone in cui alcuni si stringono la mano, il numero di persone che ha stretto la mano a un numero disparti di altre persone è pari.*

Dimostriamolo con un doppio conteggio. Sia P l'insieme di tutte le persone e $s(p)$ il numero di persone a cui la persona $p \in P$ ha stretto la mano, e contiamo il numero totale N

di coppie (persona, stretta di mano effettuata). Contando prima le persone e poi le strette di mano per ciascuno di loro, si ha $N = \sum_{p \in P} s(p)$*. D'altra parte, contando tutte le strette di mano e per ciascuna di esse le due mani coinvolte, si ha* $N = 2S$*, dove* S *è il numero totale delle strette di mano. Quindi* $\sum_{p \in P} s(p) = 2S$*, e quindi la sommatoria è pari. Perciò il numero di suoi addendi dispari deve essere pari, che è la tesi.*

Esempio 3.24. *Il corollario 3.18 poteva anche essere dimostrato tramite* doppio conteggio*, contando tutti i sottoinsiemi di un insieme di cardinalità* n*. Infatti, sappiamo che questo numero è* 2^n *(membro di sinistra). D'altra parte, i sottoinsiemi possiamo enumerarli (membro di destra) in base a quanti elementi di* A *contengono: per ogni* $i = 0, \dots, n$*, ci sono esattamente* $\binom{n}{i}$ *sottoinsiemi con* i *elementi; infine sommiamo.*

Teorema 3.25. (Principio dei cassetti, "pigeonhole principle") *Se* N *oggetti vengono messi in* k *cassetti, e* $N > k$*, allora c'è almeno un cassetto con più di un oggetto.*

In forma un po' più forte: c'è almeno un cassetto con almeno $\lceil N/k \rceil$ *oggetti.*

Esempio 3.26. *In un gruppo di* N *persone* $(N > 1)$*, ci sono almeno due persone che hanno lo stesso numero di amici tra le altre persone.*

Infatti, ogni persona può avere da 0 *a* $N - 1$ *amici. Tuttavia, non possono esserci contemporaneamente una persona che ha* 0 *amici e una persona che ha* $N-1$ *amici (altrimenti, la persona con* $N - 1$ *amici sarebbe amica con tutti gli altri, anche con quello con* 0 *amici, assurdo). Quindi il numero di amici che una persona può avere è* $0, 1, \dots, N-1$ *(*N *numeri), con gli estremi non entrambi inclusi; le possibilità sono quindi* $k < N$*. Per il principio dei cassetti, ci sono due persone con lo stesso numero di amici.*

Proposizione 3.27. (Principio della somma) *Se* A *e* B *sono insiemi finiti disgiunti, allora*

$$|A \cup B| = |A| + |B|.$$

Più in generale, vale il seguente principio.

Teorema 3.28. (Principio di inclusione-esclusione) *Se* A, B *sono due insiemi finiti, allora*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Più in generale: se $A_1, \dots, A_k$ *(*$k \geq 2$*) sono insiemi finiti, allora*

$$\Big|\bigcup_{i=1}^{k} A_i\Big| = \sum_{i=1}^{k} |A_i| - \sum_{1 \leq i < j \leq k} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{k-1} \Big|\bigcap_{i=1}^{k} A_i\Big|.$$

Questo significa che la cardinalità dell'unione è dato dalla somma delle cardinalità dei singoli insiemi, meno le cardinalità delle intersezioni a coppie, più le cardinalità delle intersezioni a triplette, e così via.

Esempio 3.29. *Quanti sono i numeri interi positivi minori di 31 e divisibili per* 2 *o per* 3 *?*

Se $A = \{x \in \mathbb{N} \mid x < 31,\ 2 \text{ divide } x\}$ *e* $B = \{x \in \mathbb{N} \mid x < 31,\ 3 \text{ divide } x\}$*, allora* $A \cup B = \{x \in \mathbb{N} \mid x < 31,\ 2 \text{ divide } x \text{ o } 3 \text{ divide } x\}$ *e* $A \cap B = \{x \in \mathbb{N} \mid x < 31,\ 6 \text{ divide } x\}$*. Poiché* $|A| = 30/2 = 15$*,* $|B| = 30/3 = 10$ *e* $|A \cap B| = 30/6 = 5$*, vale che* $|A \cup B| = 15 + 10 - 5 = 20$*.*

3.3 Applicazioni del principio di inclusione-esclusione

Proposizione 3.30. *Siano* A *e* B *due insiemi finiti di cardinalità* $|A| = n$ *e* $|B| = k$*. Il numero delle funzioni suriettive da* A *a* B *è*

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$

Dimostrazione. L'insieme delle funzioni suriettive è uguale a $\mathcal{F} \setminus \mathcal{N}$, dove $\mathcal{F}$ è l'insieme di tutte le funzioni $A \to B$ e $\mathcal{N}$ è l'insieme delle funzioni $A \to B$ non suriettive. Qundi il numero cercato è $|\mathcal{F} \setminus \mathcal{N}| = |\mathcal{F}| - |\mathcal{N}| = k^n - |\mathcal{N}|$.

Siano $b_1, \ldots, b_k$ i k elementi di B. Allora una funzione $f : A \to B$ è non suriettiva (cioè $\mathrm{Im}(f) \neq B$) se e solo se $b_i \notin \mathrm{Im}(f)$ per qualche i. Perciò $\mathcal{N} = \mathcal{E}_1 \cup \cdots \cup \mathcal{E}_k$, dove $\mathcal{E}_j = \{f : A \to B \mid b_j \notin \mathrm{Im}(f)\}$. Pertanto $|\mathcal{N}|$ si può calcolare tramite il principio di inclusione-esclusione, una volta che conosciamo le cardinalità delle intersezioni tra insiemi del tipo $\mathcal{E}_j$.

Per ogni j, le funzioni in $\mathcal{E}_j$ possono essere identificate con le funzioni da A a $B \setminus \{b_j\}$, perciò il loro numero è $|\mathcal{E}_j| = (k-1)^n$; inoltre, ci sono $k = \binom{k}{1}$ scelte per l'insieme $\mathcal{E}_j$. Similarmente, le funzioni in $\mathcal{E}_j \cap \mathcal{E}_\ell$ $(j \neq \ell)$ sono tante quante le funzioni da A a $B \setminus \{b_j, b_\ell\}$, quindi il loro numero è $(k-2)^n$; inoltre, ci sono $\binom{k}{2}$ scelte per l'intersezione $\mathcal{E}_j \cap \mathcal{E}_\ell$, al variare degli indici distinti k, ℓ. Proseguendo in questo modo e applicando il principio di inclusione-esclusione a $\mathcal{N} = \mathcal{E}_1 \cup \cdots \mathcal{E}_k$, si ottiene:

$$|\mathcal{N}| = \binom{k}{1}(k-1)^n - \binom{k}{2}(k-2)^n + \binom{k}{3}(k-3)^n - \cdots + (-1)^{k-1}\binom{k}{k}(k-k)^n.$$

Quindi il numero cercato è

$$k^n - |\mathcal{N}| = \binom{k}{0}(k-0)^n - \binom{k}{1}(k-1)^n + \binom{k}{2}(k-2)^n - \binom{k}{3}(k-3)^n + \cdots + (-1)^k\binom{k}{k}(k-k)^n$$

$$= \sum_{i=0}^{n}(-1)^i\binom{k}{i}(k-i)^n$$

□

Definizione 3.31. *Dati due interi positivi n, k con $n \geq k$, definiamo $S(n,k)$ come il numero delle partizioni in k sottoinsiemi di un insieme di n elementi. Il numero $S(n,k)$ è detto* numero di Stirling di seconda specie *relativo a n e k.*

I numeri di Stirling $S(n,k)$ soddisfano la seguente proprietà ricorsiva.

Proposizione 3.32. *Per ogni n e k con $n \geq k > 1$, si ha:*

$$S(n+1,k) = S(n,k-1) + k \cdot S(n,k)$$

Dimostrazione. Fissiamo un insieme $A = \{a_1, \ldots, a_n, a_{n+1}\}$ di cardinalità $n+1$, vogliamo contare le partizioni di A in k sottoinsiemi. Ciascuna partizione $\mathcal{P}$ soddisfa una e una sola tra le due opzioni seguenti: o il singoletto $\{a_{n+1}\}$ appartiene a $\mathcal{P}$; oppure $\{a_{n+1}\}$ non appartiene a $\mathcal{P}$.

Nel primo caso, i $k-1$ elementi di $\mathcal{P}$ diversi da $\{a_{n+1}\}$ formano una partizione dell'insieme $A \setminus \{a_{n+1}\}$, che ha cardinalità n. Chiaramente, questa corrispondenza è biunivoca, e quindi le partizioni $\mathcal{P}$ di A in k elementi tali che $a_{n+1} \in \mathcal{P}$ sono tante quante le partizioni di $A \setminus \{a_{n+1}\}$ in $k-1$ sottoinsiemi, cioè $S(n,k-1)$.

Nel secondo caso, la partizione $\mathcal{P}$ è identificata come segue: si sceglie una qualunque partizione $\mathcal{P}'$ di $A \setminus \{a_{n+1}\}$ in k sottoinsiemi, e poi si ottiene $\mathcal{P}$ aggiungendo a_{n+1} a uno dei k elementi di $\mathcal{P}'$. Ci sono $S(n,k)$ modi di scegliere $\mathcal{P}'$, e per ciascun $\mathcal{P}'$ ci sono k modi di estenderlo a $\mathcal{P}$. Quindi il numero totale è $k \cdot S(n,k)$.

Sommando i due casi, la formula è dimostrata. □

Proposizione 3.33. *Per ogni scelta di $n \geq k$, il numero di funzioni suriettive da un insieme di cardinalità n a un insieme di cardinalità k è uguale a $k! \cdot S(n,k)$. Perciò*

$$S(n,k) = \frac{1}{k!}\sum_{i=0}^{n}(-1)^i\binom{k}{i}(k-i)^n$$

Dimostrazione. Una volta dimostrata la prima parte dell'enunciato, la formula per $S(n,k)$ segue direttamente dalla proposizione 3.30.

Siano A e B insiemi con $|A| = n$ e $|B| = k$, e sia $B = \{b_1, \ldots, b_k\}$. Ogni funzione $f : A \to B$ è identificata univocamente dalla k-upla ordinata $(f^{-1}(b_1), \ldots, f^{-1}(b_k))$ delle controimmagini $f^{-1}(b_i) \subseteq A$ degli elementi di B.

Notiamo che i sottoinsiemi $f^{-1}(b_1), \ldots, f^{-1}(b_k)$ di A sono disgiunti (perché l'immagine tramite f di un elemento di A è unica) e la loro unione è tutto A (perché ogni elemento di A ha un'immagine tramite f). Inoltre, f è suriettiva se e solo se i sottoinsiemi $f^{-1}(b_1), \ldots, f^{-1}(b_k)$ sono tutti non vuoti. Quindi, al variare delle funzioni f, l'insieme non ordinato $\{f^{-1}(b_1), \ldots, f^{-1}(b_k)\}$ fornisce tutte le partizioni di A fatte da k sottoinsiemi.

Ad ogni partizione $\{C_1, \ldots, C_k\}$ di A in k sottoinsiemi, sono associate tante funzioni suriettive $f : A \to B$ quanti sono i modi di ordinare $C_1, \ldots, C_k$; infatti, determinare f significare dire in $\{C_1, \ldots, C_k\}$ chi è $f^{-1}(b_1)$, chi è $f^{-1}(b_2)$, eccetera. I modi di riordinare $\{C_1, \ldots, C_k\}$ sono $k!$ (permutazioni di n oggetti), mentre il numero delle partizioni è $S(n,k)$. Quindi il numero di funzioni suriettive $f : A \to B$ è il loro prodotto $k! \cdot S(n,k)$. □

Definizione 3.34. *Il numero delle partizioni di un insieme di n elementi è indicato con $\mathcal{B}_n$, ed è detto* numero di Bell *relativo a n.*

Chiaramente le partizioni possono essere da $1, 2, \ldots, n$ sottoinsiemi del nostro fissato insieme di n elementi. Perciò

$$\mathcal{B}_n = \sum_{k=1}^{n} S(n,k)$$

e quindi, usando la proposizione 3.33,

$$\mathcal{B}_n = \sum_{k=1}^{n} \left(\frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n \right)$$

Diamo ora un altro esempio di applicazione del principio di inclusione-esclusione, contando i cosiddetti *derangement* di n oggetti.

Definizione 3.35. *Un* derangement *di n oggetti è una permutazione di n oggetti che non fissa nessun elemento. In altre parole, un* derangement *di $\{1, \ldots, n\}$ è una funzione biettiva $p : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tale che $p(i) \neq i$ per ogni $i \in \{1, \ldots, n\}$.*

Il numero di derangement di n oggetti è indicato con $!n$ ed è detto il *subfattoriale* di n.

Proposizione 3.36. *Il numero di derangement di n oggetti è*

$$!n \;=\; n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Dimostrazione. Il numero di derangement di $\{1, \ldots, n\}$ è uguale al numero $n!$ di tutte le permutazioni di $\{1, \ldots, n\}$ meno il numero di permutazioni che fissano i per qualche $i \in \{1, \ldots, n\}$. Quindi, indicato con F_i l'insieme delle permutazioni che fissano i, si ha che

$$!n \;=\; n! \;-\; |P_1 \cup \cdots \cup P_n|.$$

Le permutazioni che fissano un dato i sono in corrispondenza biunivoca con tutte le permutazioni di $\{1, \ldots, n\} \setminus \{i\}$, e quindi $|P_1| = (n-1)!$. I modi per scegliere i tra $1, \ldots, n$ sono $C_{n,1} = \binom{n}{1}$. Quindi $\sum_{1 \le i \le n} |P_i| = \binom{n}{1}(n-1)! = \frac{n!}{1!}$.

Con lo stesso ragionamento, si arriva a $\sum_{1 \le i < j \le n} |P_i \cap P_j| \;=\; \binom{n}{2}(n-2)! \;=\; \frac{n!}{2!}$, poi $\sum_{1 \le i < j < k \le n} |P_i \cap P_j \cap P_k| = \frac{n!}{3!}$, avanti fino a $P_1 \cap \cdots \cap P_n = \frac{n!}{n!}$. Perciò, per inclusione-esclusione,

$$!n \;=\; n! - \left(\frac{n!}{1!} - \frac{n!}{2!} + \frac{n!}{3!} - \cdots + (-1)^{n+1} \frac{n!}{n!} \right)$$

$$=\; n! \cdot \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{n!}{3!} - \cdots + (-1)^n \frac{1}{n!} \right) = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

□

Si può dimostrare che per $n \to \infty$ la sommatoria $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ ha limite $\frac{1}{e}$, dove e è il numero di Nepero. Quindi, la probabilità che una permutazione casuale sia un derangement, data dal numero di derangement diviso per il numero di permutazioni, vale

$$\frac{!n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \underset{n \to \infty}{\longrightarrow} \frac{1}{e} \approx 0,368$$

3.4 Esercizi

Esercizio 3.1. *In quanti modi* 7 *buste* numerate *possono essere assegnate a* 7 *persone, se ognuna di esse riceve una busta?*

Soluzione. Queste sono esattamente le permutazioni di 7 oggetti, in quanto ogni persona ne deve ricevere una.

Esercizio 3.2. *In quanti modi* 7 *buste* numerate *possono essere assegnate a* 7 *persone?*

Soluzione. In questo caso la prima busta può essere data a ognuna delle sette persone, la seconda busta ugualmente, e così via. Quindi il numero di distribuzioni è pari al numero di disposizioni con ripetizione di 7 oggetti in gruppi di 7, ovvero 7^7.

Esercizio 3.3. *In quanti modi* 7 *buste* identiche *possono essere assegnate a* 7 *persone?*

Soluzione. 1. Corrispondono alle combinazioni con ripetizione di 7 oggetti (le persone, distinte) in gruppi di 7 (le buste), ovvero $C_{13,7}$.

Esercizio 3.4. 10 *giocatori di tennis decidono di giocare un doppio.*

1. *Quante coppie distinte si possono formare?*
2. *Una volta formate le* 5 *coppie, quante distinte partite (coppia contro coppia) si possono giocare?*

Soluzione. Il numero di coppie distinte è $C_{10,2} = \binom{10}{2}$. Il numero di partite che è possibile disputare è $C_{5,2} = \binom{5}{2}$.

Esercizio 3.5. *Si consideri un mazzo di* 40 *carte (*10 *carte distinte per ciascuno dei quattro semi).*

1. *Quanti insiemi di* 5 *carte si possono avere?*
2. *Quanti insiemi di* 5 *carte possono avere* 4 *assi?*
3. *Quanti insiemi di* 5 *carte possono avere* 4 *carte di uguale valore?*
4. *Quanti insiemi di* 5 *carte possono avere* 2 *assi?*
5. *Quanti insiemi di* 5 *carte possono avere almeno* 2 *assi?*

6. *Quanti insiemi di* 5 *carte possono avere due coppie di carte di uguale valore, ma distinte fra loro?*

Soluzione. 1. $C_{40,5} = \binom{40}{5}$.
2. Fissando i quattro assi, la quinta carta può essere scelta in 36 modi distinti.
3. Le quattro carte uguali possono essere di 10 tipi differenti e ragionando come nel punto precedente in totale sia hanno $10 \cdot 36 = 360$ insiemi.
4. I due assi possono essere scelti in $C_{4,2} = \binom{4}{2} = 6$ modi mentre le rimanenti 3 carte possono essere scelte in $C_{36,3} = \binom{36}{3}$ modi distinti. In tutto $C_{4,2} \cdot C_{36,3}$.
5. Ragionando come nel punto precedente, tale numero è dato da $C_{4,2} \cdot C_{36,3} + C_{4,3} \cdot C_{36,2} + C_{4,4} \cdot C_{36,1}$.
6. Ogni coppia può essere scelta in $C_{4,2}$ modi distinti e possiamo scegliere due coppie distinte in $C_{10,2}$ modi. La quinta carta ha 32 possibilità. In tutto quindi $C_{10,2} \cdot C_{4,2} \cdot C_{4,2} \cdot 32$.

Esercizio 3.6. 10 *copie di un libro vengono distribuite in* 5 *scuole.*

1. *In quanti modi possono essere distribuiti i libri fra le scuole?*

2. *E se ad ogni scuola viene assegnato almeno un libro?*

Soluzione. 1. Corrispondono alle combinazioni con ripetizione di 5 oggetti (il nome delle scuole) in gruppi di 10 (il numero dei libri), ovvero $C_{14,10}$.
2. Corrispondono alle combinazioni con ripetizione di 5 oggetti in gruppi di 5, in quanto dobbiamo distribuire solo 5 dei dieci libri, ovvero $C_{9,5}$.

Esercizio 3.7. *Un'urna contiene* 20 *palline bianche e* 10 *palline nere.*

1. *Eseguendo* 5 *estrazioni senza reimbussolamento, in quanti casi si ottiene come esito dell'estrazione* 3 *palline bianche e* 2 *nere?*

2. *E se ad ogni estrazione segue il reimbussolamento?*

Soluzione. 1. Le palline bianche sono indistinguibili tra loro, come le nere. Quindi si hanno $C_{20,3}$ modi di estrarre 3 bianche e $C_{10,2}$ di estrarre 2 nere. In tutto $C_{20,3} \cdot C_{10,2}$.
2. In questo caso le combinazioni sono con ripetizione, ovvero $C_{22,3} \cdot C_{11,2}$.

Esercizio 3.8. *Si consideri un mazzo di* 40 *carte (*10 *carte distinte per ciascuno dei quattro semi). Alice, Bianca e Carlo estraggono dal mazzo rispettivamente* 5, 4 *e* 3 *carte.*

1. *Quante sono le possibili estrazioni in cui nessuno dei tre ha estratto coppe?*

2. *Quante sono le possibili estrazioni in cui Alice e Bianca non hanno estratto spade, mentre Carlo ne ha estratte esattamente* 2*?*

3. *Quante sono le possibili estrazioni in cui Alice e Bianca non hanno estratto spade, mentre Carlo ne ha estratte almeno* 2*?*

4. *Quante sono le possibili estrazioni in cui le carte di Alice e Bianca sono tutte carte di denari?*

5. *Quante sono le possibili estrazioni in cui Alice ha estratto* 2 *carte di denari e* 2 *carte di coppe?*

Soluzione. 1. Hanno a disposizione 30 carte. Non essendoci reimmissione le possibili estrazioni sono $C_{30,5} \cdot C_{25,4} \cdot C_{21,3}$.
2. $C_{30,5} \cdot C_{25,4} \cdot C_{10,2} \cdot C_{21,1}$.
3. $C_{30,5} \cdot C_{25,4} \cdot (C_{10,2} \cdot C_{21,1} + C_{10,3})$.
4. $C_{10,5} \cdot C_{5,4} \cdot C_{31,3}$.
5. $C_{10,2} \cdot C_{10,2} \cdot 20 \cdot C_{35,4} \cdot C_{31,3}$.

Esercizio 3.9. *Si consideri un mazzo di* 52 *carte (*13 *carte distinte per ciascuno dei quattro semi). Vengono estratte* 13 *carte dal mazzo.*

1. *Quante sono le possibili estrazioni in cui le* 13 *carte hanno tutte valore diverso?*

2. *Quante sono le possibili estrazioni in cui le* 13 *carte sono tutte dello stesso seme?*

3. *Quante sono le possibili estrazioni in cui* 8 *delle* 13 *carte hanno lo stesso seme?*

Soluzione. 1. Per ognuno dei 13 valori deve essere estratta una sola carta, quindi 4^{13}.
2. Tanti quanti i semi distinti, ovvero 4.
3. Il seme può essere scelto in 4 modi distinti, quindi $4 \cdot C_{13,8} \cdot C_{39,5}$.

Esercizio 3.10. *La biglietteria di un teatro dispone di* 100 *biglietti numerati.*

1. *Scegliendone* 4 *a caso, quante sono le possibilità di avere estratto dei biglietti con numeri consecutivi?*

2. *E se si considera anche l'ordine con cui i biglietti vengono scelti?*

Soluzione. 1. Il biglietto con il numero più piccolo può essere nell'intervallo $1 - -97$, quindi in tutto sono 97.
2. $4! \cdot 97$.

Esercizio 3.11. *Una band composta da* 4 *ragazzi possiede* 4 *strumenti musicali.*

1. *Se ognuno di essi sa suonare ogni strumento, in quanti modi possono ripartirsi gli strumenti?*

2. *E se* 2 *dei suonatori sanno suonare solo* 2 *strumenti (gli stessi per entrambi)?*

Soluzione. 1. Ad ogni ragazzo può essere assegnato qualsiasi strumento libero, perciò 4!.
2. I due ragazzi devono suonare quei due strumenti, gli altri i rimanenti, perciò $2! \cdot 2!$.

Esercizio 3.12. *Un bambino possiede dei mattoncini lego colorati: ne ha* 6 *rossi,* 4 *gialli,* 1 *verde e* 1 *blu. In quanti modi il bambino può riarrangiarli in* 2 *colonne a formare una torre?*

Soluzione. Bisogna ordinare i dodici mattoncini, tuttavia i mattoni dello stesso colore tra loro sono indistinguibili, quindi $\frac{12!}{6!4!}$.

Esercizio 3.13. *In quanti modi le lettere delle parole seguenti possono essere riarrangiate per formare altre parole (non necessariamente con senso)?*

- *PASTO*
- *PANINO*
- *PANNA*
- *ANNA*

Soluzione. $5!$, $\frac{6!}{2!}$, $\frac{5!}{2!2!}$, $\frac{4!}{2!2!}$.

Esercizio 3.14.

1. *In quanti modi* 3 *ragazzi e* 3 *ragazze possono disporsi per ordine su di una panchina?*

2. *In quanti modi se ragazzi e ragazze sono tutti vicini fra loro?*

3. *In quanti modi se solo i ragazzi siedono tutti vicini fra loro?*

4. *In quanti modi se non vi sono persone dello stesso sesso sedute a fianco?*

Soluzione. 1. $6!$.
2. $2 \cdot 3!3!$.
3. $4 \cdot 3!3!$.
4. $2 \cdot 3!3!$.

Esercizio 3.15. *1. In quanti modi* 8 *persone possono sedersi per ordine su di una panchina?*

2. In quanti modi se le persone A e B vogliono sedersi vicine?

3. In quanti modi se vi sono 4 *uomini e* 4 *donne e non vi sono persone dello stesso sesso sedute a fianco?*

4. In quanti modi se vi sono 5 *uomini tutti seduti vicini?*

5. In quanti modi se vi sono 4 *coppie sposate, e ciascuna coppia è seduta assieme?*

Soluzione. 1. $8!$.
2. $7 \cdot 2!6!$.
3. $2 \cdot 4!4!$.
4. $4 \cdot 5!3!$.
5. $4!2!2!2!2!$.

Esercizio 3.16. *Si dispone di* 3 *libri di letteratura,* 2 *libri di informatica ed* 1 *libro di matematica.*

1. In quanti modi possono essere ordinati i libri su di uno scaffale?

2. In quanti modi se i libri di letteratura e quelli di matematica sono tutti vicini fra loro?

3. In quanti modi se i libri di letteratura sono tutti vicini?

Soluzione. 1. $6!$.
2. $3!3!2!$.
3. $4 \cdot 3!3!$.

Esercizio 3.17. *Uno studente ha deciso di vendere* 2 *libri fra i* 6 *di matematica,* 7 *di scienze,* 4 *di economia che possiede. Quante sono le scelte possibili se*

1. i libri devono trattare lo stesso argomento;

2. i libri devono trattare argomenti diversi.

Soluzione. 1. $C_{6,2} + C_{7,2} + C_{4,2}$.
2. $6 \cdot 7 + 6 \cdot 4 + 7 \cdot 4$.

Esercizio 3.18. *Da un gruppo di* 8 *donne e* 6 *uomini deve essere scelta una commissione formata da* 3 *donne e* 3 *uomini.*

1. Quante diverse commissioni si possono formare?

2. E se 2 *degli uomini rifiutano di lavorare insieme?*

3. E se 2 *delle donne rifiutano di lavorare insieme?*

4. E se 1 *uomo e* 1 *donna rifiutano di lavorare insieme?*

Soluzione. 1. $C_{8,3}C_{6,3}$.
2. $C_{8,3}(C_{6,3} - 4)$.
3. $(C_{8,3} - 6)C_{6,3}$.
4. $C_{8,3}C_{6,3}$-$C_{7,2}C_{5,2}$.

Esercizio 3.19. *Se* 12 *persone sono divise a formare* 3 *commissioni, rispettivamente di* 3, 4 *e* 5 *persone, quante sono le possibili divisioni?*

Soluzione. $C_{12,5}C_{7,4}$.

Esercizio 3.20. *In quanti modi* 8 *professori possono essere assegnati a* 4 *distinte scuole?*

1. E se ad ogni scuola viene assegnato almeno 1 *professore?*

2. E se ad ogni scuola vengono assegnati 2 *professori?*

Soluzione. 1. 4^8.
2. $4^8 - 4 \cdot 3^8 - C_{4,2}2^8 - 4$.
3. $C_{8,2}C_{6,2}C_{4,2}$.

Esercizio 3.21. *Vi sono* 20000 *euro da investire su* 4 *possibili titoli azionari. Ogni investimento deve essere un multiplo di* 1000 *euro, ma c'è un investimento minimo che dipende dal titolo azionario. Gli investimenti minimi sono rispettivamente di* 4, 3, 2 *e* 1 *migliaio di euro. Quante differenti strategie di investimento sono possibili se*

1. *si vuole investire su ciascuno dei* 4 *titoli azionari;*

2. *si vuole investire su almeno* 3 *dei* 4 *titoli azionari.*

Soluzione. 1. I 9000 euro rimanenti sono indistinguibili, quindi bisogna considerare combinazioni con ripetizioni $C'_{9,4} = C_{12,8}$.
2. Le possibilità in questo caso sono: i 9000 euro sono ripartiti tra tutti i fondi tranne il primo, tranne il secondo, tranne il terzo, o tranne il quarto, oppure tra tutti e quattro i fondi. Quindi il numero totale di possibilità è pari a

$$C'_{9,4} + C'_{11,3} + C'_{11,3} + C'_{12,3} + C'_{13,3} = C_{12,8} + C_{13,10} + C_{13,10} + C_{14,11} + C_{15,12}.$$

Esercizio 3.22. *Un'urna contiene* 10 *palline rosse,* 5 *nere e* 5 *bianche. Si estraggono due palline contemporaneamente. Calcolare quante coppie di palline è possibile ottenere*

1. *di colore bianco;*

2. *di colore non rosso;*

3. *di uguale colore;*

4. *di diverso colore.*

Soluzione. 1. $C_{5,2}$. 2. $C_{10,2}$. 3. $C_{10,2} + C_{5,2} + C_{5,2}$. 4. $10 \cdot 5 + 10 \cdot 5 + 5 \cdot 5$.

Esercizio 3.23. *Si consideri un mazzo (standard) di* 52 *carte.*

1. *Quante possibili combinazioni di 5 carte di valore consecutivo esistono?*

2. *Quante possibili combinazioni di 5 carte di valore consecutivo e dello stesso seme esistono?*

Soluzione. 1. Vi sono nove possibili tipi di scale (la carta più bassa può essere 1, 2, ..., 9). Per ognuna di queste nove tipologie vi sono 4^5 possibilità in quanto ogni carta può essere di qualsiasi seme. In tutto sono quindi $9 \cdot 4^5$ combinazioni.
2. Per ognuna delle nove possibilità di scala ci sono questa volta solo 4 possibilità (una per ogni seme). In totale le combinazioni sono $9 \cdot 4$.

Esercizio 3.24. *Quante partite di basket vengono disputate in un campionato a 18 squadre considerando sia l'andata che il ritorno?*

Soluzione. Le possibili partite del girone di andata coincidono con le possibili coppie che si possono formare a partire dalle 18 squadre, dato che ad ogni ogni coppia di squadre si associa una partita. Tali coppie sono $C_{18,2}$,considerando entrambi i gironi si ha $2 \cdot C_{18,2} = 306$.

Esercizio 3.25. *Una classe è formata da 27 alunni: 15 femmine e 12 maschi. Si deve costruire una delegazione di 5 alunni, di cui 3 femmine e due maschi. Quante sono le possibili delegazioni?*

Soluzione. La scelta delle 3 femmine a partire dalle 15 presenti si può fare in $C_{15,3}$ modi, la scelta dei 2 maschi a partire dai 12 totali si può fare in $C_{12,2}$ modi. Poichè le due scelte sono indipendenti si ha $C_{15,3} \cdot C_{12,2} = 30030$.

Esercizio 3.26. *Si considerino gli insiemi $A = \{1, 2, 3, 4\}$ e $B = \{a, b, c\}$. Quante sono le funzioni da A in B?*

Soluzione. Sia $f : A \longrightarrow B$, si hanno tre possibilità per la scelta di $f(1)$, 3 possibilità per la scelta di $f(2)$ e così via. Le scelte sono tra loro tutte indipendenti perciò esistono $3 \cdot 3 \cdot 3 \cdot 3 = 3^4$ possibili funzioni da A in B.

Esercizio 3.27. *Le targhe automobilistiche sono costituite da 2 lettere, seguite da 3 cifre, seguite a loro volta da 2 lettere. Sapendo che le due lettere possono essere scelte tra le 26 dell'alfabeto anglosassone, si calcoli quante automobili è possibile targare.*

Soluzione. Partiamo dalla prima coppia di lettere, ci sono $k = 2$ elementi che possono essere scelti tra $n = 26$, siamo di fronte a disposizioni con ripetizione $D'_{26,2} = 26^2 = 676$. Questo vale anche per la seconda coppia de lettere presente chiaramente. Le cifre sono raggruppamenti di 3 scelti tra $n = 10$, anche qui abbiamo disposizioni con ripetizione, quindi $D'_{10,3} = 10^3 = 1000$. Avendo tre raggruppamenti scelti indipendentemente il numero di targhe possibili è $D'_{26,2} \cdot D'_{10,3} \cdot D'_{26,2}$.

Esercizio 3.28. *24 amici vanno a cena e a fine serata per salutarsi ognuno stringe la mano a tutti gli altri. Quante strette di mano ci saranno?*

Soluzione. Le strette di mano totali sono pari a $C_{24,2} = 276$.

Esercizio 3.29. *Quanti sono i numeri di 5 cifre divisibili per 5, minori di 50000 e contenenti solo le cifre 1, 3, 5 e 7?*

Capitolo 4

Operazioni e Strutture Algebriche

4.1 Gruppi, Anelli, Domini, Campi

Definizione 4.1. *Una* operazione binaria interna $\oplus$ *su un insieme* A *è una funzione*

$$\oplus : A \times A \to A.$$

- *L'operazione* $\oplus$ *si dice* associativa *se*

$$\forall a, b, c \in A \ : \quad (a \oplus b) \oplus c = a \oplus (b \oplus c).$$

- *Si dice* elemento neutro *di* $\oplus$ *(se esiste) un elemento* $u \in A$ *tale che*

$$\forall a \in A \ : \quad a \oplus u = u \oplus a = a.$$

  Si verifica facilmente che l'elemento neutro, se esiste, è unico.

- *Un elemento* $a \in A$ *si dice* invertibile *se esiste un elemento* $\overline{a} \in A$ *tale che*

$$a \oplus \overline{a} = \overline{a} \oplus a = u.$$

  In tal caso, l'elemento $\overline{a}$ *si dice* inverso *di* a *(rispetto a* $\oplus$*).*

- *L'operazione* $\oplus$ *si dice* commutativa *se*

$$\forall a, b \in A \ : \quad a \oplus b = b \oplus a.$$

Osservazione 4.2. *Per indicare una operazione binaria generica si usano simboli come* $\oplus, \odot, *, \star ...$

Se usiamo la notazione additiva*, l'operazione è indicata con "+" (oppure* $\oplus$*) ed è detta* somma*, l'eventuale neutro è indicato con* 0 *ed è detto* zero*, l'eventuale inverso di* a *è indicato con* $-a$ *ed è detto* opposto *di* a*.*

Se usiamo la notazione moltiplicativa*, l'operazione è indicata con "·" (oppure* $\odot$*) ed è detta* prodotto*, l'eventuale neutro è indicato con* 1 *ed è detto* uno*, l'eventuale inverso di* a *è indicato con* a^{-1}*.*

Definizione 4.3. *Un* gruppo $(G, *)$ *è dato da un insieme* $G \neq \emptyset$ *munito di un'operazione binaria interna* $*$ *tale che:*

- $*$ *è associativa,*
- *esiste l'elemento neutro* $u \in G$ *rispetto a* $*$*,*
- *ogni elemento di* G *ammette inverso rispetto a* $*$*.*

Se inoltre $*$ *è commutativa, allora* G *è detto* gruppo abeliano *(o* gruppo commutativo*).*

Definizione 4.4. *Un* anello $(A, \oplus, \odot)$ *è dato da insieme* $A \neq \emptyset$ *munito di due operazioni binarie interne* $\oplus$ *e* $\odot$ *tali che:*

- A *con* $\oplus$ *è un gruppo abeliano,*
- $\odot$ *è associativa,*
- $\odot$ *è* distributiva *a destra e a sinistra rispetto a* $\oplus$*, cioè:*

$$\forall a, b, c \in A \ : \qquad a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c), \qquad (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c).$$

Se $\odot$ *è commutativa allora* A *è detto* anello commutativo*.*

Se esiste un elemento neutro $1 \in A$ *rispetto a* $\odot$ *(cioè* $1 \odot a = a \odot 1 = a$ *per ogni* $a \in A$*) allora* A *è detto* anello unitario*.*

Definizione 4.5. *Dato un anello* $(A, \oplus, \odot)$*, un elemento* $a \in A$ *si dice* invertibile *se è invertibile rispetto a* $\odot$*, cioè se esiste* $a^{-1} \in A$ *tale che* $a \odot a^{-1} = a^{-1} \odot a = 1$*.*

In un anello con $0 \neq 1$, si ha che 0 non è invertibile, mentre 1 e -1 sono invertibili.

Definizione 4.6. *Un* dominio di integrità *è un anello commutativo unitario con* $1 \neq 0$ *tale che*

$$a \odot b \neq 0 \quad \forall a, b \in A \setminus \{0\}.$$

Un elemento $a \neq 0$ di un anello A si dice *divisore dello zero* se esiste $b \in A$ con $a \odot b = 0$.

Quindi un dominio di integrità è privo di divisori dello zero.

Osservazione 4.7. *In un dominio di integrità* $(A, \oplus, \odot)$ *vale la* legge di cancellazione*: se* $a, b, c \in A$ *con* $a \neq 0$ *verificano* $a \odot b = a \odot c$*, allora* $b = c$*.*

Esempio 4.8. *L'insieme* $\mathbb{Z}$ *dei numeri interi rispetto alle usuali operazioni di somma e prodotto è un dominio di integrità.*

Definizione 4.9. *Un* campo $(K, \oplus, \odot)$ *è dato da un insieme* $K \neq \emptyset$ *munito di due operazioni* $\oplus$ *e* $\odot$ *tali che*

- K *con* $\oplus$ *è un gruppo abeliano,*
- $K \setminus \{0\}$ *con* $\odot$ *è un gruppo abeliano,*
- $\odot$ *è distributiva (a destra e a sinistra) rispetto a* $\oplus$*.*

Quindi K è un campo se e solo se K è un anello commutativo unitario in cui ogni elemento diverso da zero ammette inverso rispetto a $\odot$.

Si dimostra facilmente che ogni campo è un dominio di integrità.

Esempio 4.10. $\mathbb{Q}$*,* $\mathbb{R}$ *e* $\mathbb{C}$ *sono campi rispetto alle usuali operazioni di somma e moltiplicazioni tra numeri.*

Esempio 4.11. *Esistono anche campi aventi un numero finito di elementi.*

Ad esempio, denotiamo $\mathbb{Z}_2 = \{\mathbf{0}, \mathbf{1}\}$ *e definiamo su* $\mathbb{Z}_2$ *due operazioni* $\oplus$ *e* $\odot$ *come segue:*

$$\mathbf{0} \oplus \mathbf{0} = \mathbf{0}, \quad \mathbf{0} \oplus \mathbf{1} = \mathbf{1}, \quad \mathbf{1} \oplus \mathbf{0} = \mathbf{1}, \quad \mathbf{1} \oplus \mathbf{1} = \mathbf{0}.$$

$$\mathbf{0} \odot \mathbf{0} = \mathbf{0}, \quad \mathbf{0} \odot \mathbf{1} = \mathbf{0}, \quad \mathbf{1} \odot \mathbf{0} = \mathbf{0}, \quad \mathbf{1} \odot \mathbf{1} = \mathbf{1}.$$

Allora $(\mathbb{Z}_2, \mathbf{0}, \mathbf{1})$ *è un campo, detto* campo binario.

Più in generale, se $p \geq 2$ *è un numero primo, consideriamo* $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$*, l'insieme delle classi di congruenza modulo* p*, cioè delle classi di equivalenza di numeri interi rispetto alla relazione di congruenza modulo* p *:* $[a] = [b] \iff p \mid (a - b)$*.* $\mathbb{Z}_p$ *è finito e ha*

p elementi. Su $\mathbb{Z}_p$ sono ben definite le seguenti operazioni (definite tramite l'usuale somma e moltiplicazione in $\mathbb{Z}$):

$$[a] \oplus [b] = [a + b], \qquad [a] \odot [b] = [a \cdot b].$$

Poiché p è primo, si può dimostrare che $(\mathbb{Z}_p, \oplus, \odot)$ è un campo.

4.2 Elementi primi, elementi irriducibili, MCD e mcm

Definizione 4.12. *Sia $(A, \oplus, \odot)$ un dominio di integrità e siano $a, b \in A$. Si dice che a* divide *b (o che a* è un divisore di *b, o che b* è un multiplo di *a), in simboli $a \mid b$, se*

$$\exists\, c \in A \ : \ b = a \odot c.$$

Definizione 4.13. *Sia $(A, \oplus, \odot)$ un dominio di integrità e sia $a \in A$ con $a \neq 0$.*

- *a si dice* irriducibile *se ogni volta che $a = b \odot c$, con $b, c \in A$, allora b è invertibile o c è invertibile. Viceversa, a è* riducibile *se $\exists b, c \in A$ non invertibili tali che $a = b \odot c$.*
- *a si dice* primo *se non è invertibile e, ogni volta che $a \mid b \odot c$, con $b, c \in A$, allora $a \mid b$ oppure $a \mid c$.*

Teorema 4.14. *Sia $(A, \oplus, \odot)$ un dominio di integrità. Allora ogni elemento primo è irriducibile.*

Dimostrazione. Sia a elemento primo e supponiamo $a = b \odot c$. Allora in particolare $a \mid b \odot c$. Poiché a è elemento primo allora $a \mid b$ oppure $a \mid c$. Nel primo caso $b = a \odot x$ nel secondo $c = a \odot x$ per qualche $x \in A$. Nel primo caso si ha che $a = a \odot x \odot c$ e quindi $1 = x \odot c$ e c è invertibile. Nel secondo $a = b \odot a \odot x$ e $1 = x \odot b$ e b è invertibile. □

Osservazione 4.15. *Chiaramente in $\mathbb{Z}$ questi due concetti di elementi irriducibili ed elementi primi coincidono, cioè: un numero intero è irriducibile se e solo se è primo.*

Definizione 4.16. *Sia $(A, \oplus, \odot)$ un dominio di integrità e siano $a, b \in A$. Un elemento $d \in A$ si chiama un* Massimo Comun Divisore *tra a e b se soddisfa*

1. *$d \mid a$, $d \mid b$;*
2. *per ogni $d' \in A$, se $d' \mid a$ e $d' \mid b$, allora $d' \mid d$.*

Definizione 4.17. *Sia* $(A, \oplus, \odot)$ *un dominio di integrità e siano* $a, b \in A$*. Un elemento* $m \in A$ *si chiama un* minimo comune multiplo *tra* a *e* b *se soddisfa*

1. $a \mid m$, $b \mid m$;
2. *per ogni* $m' \in A$, *se* $a \mid m'$ *e* $b \mid m'$, *allora* $m \mid m'$.

Osservazione 4.18. *In generale, MCD e mcm non sono unici; se moltiplichiamo un* $MCD(a, b)$ *(o* $mcm(a, b)$*) per un elemento invertibile, otteniamo un altro* $MCD(a, b)$ *(o* $mcm(a, b)$*). Ad esempio, in* $\mathbb{Z}$ *i Massimi Comun Divisori tra* 8 *e* 12 *sono* 4 *e* -4*.*

Osservazione 4.19. *Sia* $(A, \oplus, \odot)$ *un dominio di integrità e* $a \in A \backslash \{0\}$*. Allora* $MCD(a, 0) = a$*, mentre* $MCD(0, 0)$ *non esiste. Inoltre* $mcm(a, 0) = 0$ *e* $mcm(0, 0) = 0$*.*

4.3 Esercizi

Esercizio 4.1. *Sia $(G, \cdot)$ un gruppo. Si dimostri che per ogni $a, b \in G$ esiste uno e un solo $x \in G$ tale che $ax = b$.*

Svolgimento. Supponiamo che esistano due elementi distinti x_1, x_2 tali che $ax_1 = b$ e $ax_2 = b$, cioè $ax_1 = ax_2$. Poichè G è un gruppo esisterà a^{-1} inverso di $a \in G$, moltiplichiamo quindi entrambi i membri per $\overline{a}$ ottenendo $\overline{a}(ax_1) = \overline{a}(ax_2)$. Usando la proprietà associativa, $(\overline{a}a)x_1 = (\overline{a}a)x_2$, quindi $1x_1 = 1x_2$. Allora $x_1 = x_2$ contro l'ipotesi.

Esercizio 4.2. *Si consideri l'insieme $G = \{2^k | k \in \mathbb{Z}\}$. Consideriamo su G l'ordinaria operazione di moltiplicazione: $(\cdot)$, dimostrare che $(G, \cdot)$ è un gruppo commutativo.*

Svolgimento. Sappiamo che $(\mathbb{Z}, +)$ è un gruppo commutativo. Infatti l'operazione $(+)$ è associativa e commutativa, esistono l'elemento neutro 0 e l'elemento inverso $-z$ per ogni $z \in \mathbb{Z}$.
Secondo la definizione, affinchè G sia un gruppo dobbiamo provare:
1. Associatività rispetto l'operazione di moltiplicazione:
siano $k_1, k_2, k_3 \in \mathbb{Z}$

$$2^{k_1} \cdot (2^{k_2} \cdot 2^{k_3}) = 2^{k_1} \cdot 2^{k_2+k_3} = 2^{k_1+k_2+k_3} = 2^{(k_1+k_2)+k_3} = 2^{k_1+k_2} \cdot 2^{k_3} =$$

$$= (2^{k_1} \cdot 2^{k_2}) \cdot 2^{k_3},$$

dove abbiamo sfruttato l'associatività dell'operazione $+$.
2. Esistenza elemento neutro :
per $0 \in \mathbb{Z}$ si ha $2^0 = 1$ elemento neutro di $(G, \cdot)$, infatti comunque preso un elemento $2^k \in G$ si ha

$$2^k \cdot 2^0 = 2^0 \cdot 2^k = 2^k$$

3. Esistenza elemento inverso:
comunque preso un elemento 2^k esiste l'inverso 2^{-k}, dove $-k$ indica l'inverso rispetto all'operazione somma su $\mathbb{Z}$. Si ha infatti

$$2^k \cdot 2^{-k} = 2^{-k} \cdot 2^k = 1.$$

Infine la commutatività segue dal fatto che $(\mathbb{Z}, +)$ è un gruppo commutativo, quindi

$$2^{k_1} \cdot 2^{k2} = 2^{k_1+k_2} = 2^{k_2+k_1} = 2^{k_2} \cdot 2^{k_1}.$$

Esercizio 4.3. *Sia $(G, \cdot)$ un gruppo commutativo, dimostrare che presi $a, b \in G$ si ha $a^n b^n = (ab)^n$ per ogni $n \in \mathbb{N}$.*

Svolgimento. presi $a, b \in G$ si ha

$$a^n b^n = a^1 a^2 \cdots a^n b^1 b^2 \cdots b^n =$$

$$a^1 a^2 \cdots b^1 a^n b^2 \cdots = \cdots = b^1 b^2 \cdots b^n a^1 a^2 \cdots a^n = (ab)^n.$$

Esercizio 4.4. *Dimostrare che se $c|a$ e $c|b$, allora $c|(ka + mb)$ per ogni scelta di $k, m \in \mathbb{Z}$.*

Svolgimento. Poichè $c|a$ e $c|b$ esistono $x, y \in \mathbb{Z}$ tali che $a = cx$ e $b = cy$. Allora $ka + mb = kcx + mcy = c(kx + my)$, quindi $c|(ka + mb)$.

Capitolo 5

L'anello $\mathbb{Z}$ dei numeri interi

5.1 Teorema fondamentale dell'aritmetica

I numeri interi, con l'usuale somma " $+$ " e prodotto " $\cdot$ " di numeri interi, costituiscono un dominio di integrità:

- la somma di interi è associativa, commutativa, ammette neutro 0, e ogni intero a ha il suo opposto $-a$;
- il prodotto di interi è associativo, commutativo, distributivo rispetto alla somma, ammette neutro 1, e il prodotto di due interi diversi da zero dà un intero diverso da zero.

Specializziamo ora al caso di $\mathbb{Z}$ i concetti introdotti nel precedente capitolo per un generico dominio di integrità.

- Si dice che a divide b (a è un divisore di b, b è un multiplo di a), in simboli $a \mid b$, se

$$\exists\, c \in \mathbb{Z} \ : \ b = ac.$$

- Un elemento $d \in \mathbb{Z}$ si dice un *massimo comun divisore* tra a e b, se $d \mid a$, $d \mid b$, e per ogni $d' \in \mathbb{Z}$ tale che $d' \mid a$ e $d' \mid b$, si ha $d' \mid d$.
- Un elemento $m \in \mathbb{Z}$ si dice un *minimo comune multiplo* tra a e b, se $a \mid m$, $b \mid m$, e per ogni $m' \in \mathbb{Z}$ tale che $a \mid m'$ e $b \mid m'$, si ha $m \mid m'$.

- Indichiamo con $MCD(a,b)$ un massimo comun divisore tra a e b, con $mcm(a,b)$ un minimo comune multiplo tra a e b.
- Se a e b sono interi positivi, $MCD(a,b)$ indica l'unico loro MCD positivo, e $mcm(a,b)$ indica l'unico loro mcm positivo.
- Se $a \neq 0$, allora $MCD(a,0) = a$ mentre $MCD(0,0)$ non esiste. Inoltre, $mcm(a,0) = mcm(0,0) = 0$.
- I numeri interi invertibili in $\mathbb{Z}$ sono 1 e -1.
- Un intero p si dice *primo* se $p \neq 0, 1, -1$ e, ogni volta che $p \mid ab$ con $a, b \in \mathbb{Z}$, allora $p \mid a$ oppure $p \mid b$.
- Un intero $p \neq 0$ si dice *irriducibile* se, ogni volta che $p = ab$ con $a, b \in \mathbb{Z}$, allora uno tra a e b è uguale a 1 o a -1.
- Sia $p \neq 0$ un intero. Se p è primo, allora p è irriducibile. Se p è irriducibile e $p \neq \pm 1$, allora p è primo.
- Il prodotto tra un numero primo e un numero invertibile è un numero primo. Perciò, i numeri interi primi sono esattamente gli interi della forma $+p$ o $-p$, dove p è un primo positivo.

Esercizio 5.1. *Trovare tutti i numeri primi p tali che $4p+1$ è un quadrato perfetto.*

Soluzione: sia p un primo tale che $4p+1$ è un quadrato perfetto. Allora $4p+1 = n^2$ per qualche intero n. Supponiamo inizialmente che n sia pari, dunque $n = 2m$ per qualche intero m; da $4p+1 = n^2$ segue $4p+1 = 4m^2$ e dunque $1 = 4(m^2 - p)$, da cui 4 divide 1, contraddizione. Supponiamo ora che n sia dispari, diciamo $n = 2k+1$ con k intero. Allora $4p+1 = n^2$ diventa $4p+1 = 4k^2+4k+1$, cioè $p = k^2+k$ e dunque $p = k(k+1)$. Poiché p è positivo, allora sia k che $k+1$ sono positivi. Poiché p è primo e quindi irriducibile, abbiamo che $k = 1$ oppure $k+1 = 1$. Il secondo caso è da escludere (altrimenti $k = 0$), ne segue che $k = 1$, che corrisponde al primo $p = 2$.

Dimostriamo l'unicità della fattorizzazione in numeri primi positivi dei numeri naturali.

Proposizione 5.1. *Sia $n > 1$ un intero. Allora esistono $p_1 > 1, \ldots, p_r > 1$ ($r \geq 1$) primi distinti e interi $h_1 > 0, \ldots, h_r > 0$ tali che*

$$n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}.$$

Inoltre tale fattorizzazione è unica, cioè: se esiste un'altra scrittura

$$n = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$$

con $q_i > 1, \ldots, q_s > 1$ *(*$s \geq 1$*) primi distinti e* $k_1 > 0, \ldots, k_s > 0$*, allora* $r = s$ *e, a meno dell'ordine,* $p_i = q_i$ *per ogni* i*.*

Dimostrazione. Dimostriamo l'esistenza della fattorizzazione per induzione su n. Se $n = 2$ allora il numero è già scomposto, dato che 2 è un numero primo. Supponiamo che ogni intero positivo $k \leq n$ possieda una fattorizzazione e consideriamo $n+1$. Se $n+1$ è un numero primo allora non dobbiamo provare nulla. Supponiamo invece che $n+1$ non sia primo, e quindi sia riducibile. Allora esistono $a, b \in [2, \ldots, n]$ tali che $n + 1 = a \cdot b$. Poiché i due interi a, b sono minori o uguali di n allora per l'ipotesi induttiva esiste una loro fattorizzazione. Potremo quindi scrivere $a = p_1^{h_1} \cdots p_r^{h_r}$, $b = q_1^{k_1} \cdots q_s^{k_r}$. Allora $n + 1 = a \cdot b = p_1^{h_1} \cdots p_r^{h_r} \cdot q_1^{k_1} \cdots q_s^{k_r}$ e salvo modificare tale scrittura in modo tale utilizzare ciascun primo una volta sola, questa è la fattorizzazione di $n + 1$.

Proviamo ora l'unicità della fattorizzazione per induzione sul numero $m = h_1 + \cdots + h_r$. Se $m = 1$ allora $n = p_1^1$. Supponiamo che $n = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$ allora

$$p_1 \mid q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}.$$

Poiché p_1 è un numero primo che divide un prodotto, dovrà dividere uno dei fattori q_i. Possiamo supporre senza perdere generalità che sia il primo q_1. Dato che anche q_1 è primo allora $p_1 = q_1$. Quindi

$$1 = q_1^{k_1 - 1} q_2^{k_2} \cdots q_s^{k_s}.$$

I numeri a destra dell'uguale devono essere per forza tutti 1, in quanto il loro prodotto è pari a 1. Pertanto $k_1 - 1 = k_2 = \cdots = k_s = 0$ e le due scritture coincidono. Supponiamo ora che ogni numero che ammetta una fattorizzazione $n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$ con $h_1 + \cdots + h_r = m$ abbia solo questa come fattorizzazione (a meno dell'ordine dei primi p_i). Sia $n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$ con $h_1 + \cdots + h_r = m + 1$ e supponiamo che $n = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$. Allora

$$p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r} = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}.$$

Il primo p_1 divide il prodotto $q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$ e pertanto dovrà dividere uno dei primi q_i, supponiamo che sia q_1. Pertanto avremo

$$p_1^{h_1 - 1} p_2^{h_2} \cdots p_r^{h_r} = q_1^{k_1 - 1} q_2^{k_2} \cdots q_s^{k_s}.$$

Queste sono fattorizzazioni di un numero intero n' con $h_1 - 1 + \cdots + h_r = m + 1 - 1 = m$. Pertanto le due scomposizioni dovranno coincidere. Salvo riordinare i primi si ha che $p_i = q_i$ e $h_1 - 1 = k_1 - 1$, $h_2 = k_2$, $\ldots$, $h_r = k_r$. Quindi anche le due fattorizzazioni del numero n coincidono. □

Osservazione 5.2. *Sia $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Se $a > 1$ allora, per la proposizione precedente, esiste una fattorizzazione di a in numeri primi positivi p_i. Se $a < -1$ allora $-a > 1$ e quindi possiamo scomporre $-a$ in fattori primi positivi. Pertanto ogni intero diverso da $0, 1, -1$ si fattorizza in modo unico, a meno dell'ordine e del segno, in numeri primi positivi:*

$$\pm 1 p_1^{h_1} \cdots p_r^{h_r}.$$

Si può anche dire che, se $a \neq 0, 1, -1$, la sua fattorizzazione in numeri interi primi (positivi o negativi) è unica, a meno dell'ordine e a meno di moltiplicarli per ± 1:

$$(\pm p_1)^{h_1} \cdots (\pm p_r)^{h_r}.$$

Proposizione 5.3. *Siano $a, b \neq 0$ due numeri interi. Allora $a \mid b$ se e solo se ogni fattore primo di a compare nella fattorizzazione di b con esponente minore o uguale al corrispondente esponente in b.*

Dimostrazione. Lasciata per esercizio. □

Proposizione 5.4. *Siano $a, b \neq 0$ due numeri interi tali che*

$$a = \pm 1 p_1^{h_1} \cdots p_r^{h_r}, \qquad b = \pm 1 p_1^{k_1} \cdots p_r^{k_r},$$

con $h_i, k_i \geq 0$. Allora

$$MCD(a, b) = p_1^{\min\{h_1, k_1\}} \cdots p_r^{\min\{h_r, k_r\}}$$

$$mcm(a, b) = p_1^{\max\{h_1, k_1\}} \cdots p_r^{\max\{h_r, k_r\}}.$$

Dimostrazione. È facile notare che $d = p_1^{\min\{h_1, k_1\}} \cdots p_r^{\min\{h_r, k_r\}}$ è un divisore sia di a che di b. Se d' è un altro divisore comune di a e b allora nella scomposizione di d' compaiono al più i primi $p_1, \ldots, p_r$ e gli esponenti devono essere ordinatamente minori o uguali di h_i e k_i. Ma allora tali esponenti sono minori o uguali anche di $\min\{h_i, k_i\}$ e quindi $d' \mid d$. Pertanto d è il massimo comun divisore di a e b.

La dimostrazione per il minimo comune multiplo è analoga ed è lasciata per esercizio. □

5.2 Alcuni criteri di divisibilità

In questa sezione presentiamo alcuni criteri di divisibilità, dipendenti dalla scrittura decimale di un numero intero.

Ricordiamo che la scrittura posizionale decimale (in base 10) di un numero intero positivo n è una giustapposizione di cifre del tipo "$a_m a_{m-1} \dots a_1 a_0$", dove $a_0, a_1, \dots, a_m$ sono cifre decimali che rappresentano i numeri interi da 0 a 9, e la cifra più significativa a_m è diversa da zero. Tale scrittura significa:

$$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0.$$

a_0 è detta la cifra delle unità, a_1 quella delle decine, eccetera.

Più in generale, dato un intero $b \geq 2$, la scrittura posizionale in base b di un numero intero positivo n è una stringa del tipo "$b_m b_{m-1} \dots b_1 b_0$", dove $b_0, b_1, \dots, b_m$ sono cifre (simboli) che rappresentano i numeri interi da 0 a $b-1$, $b_m \neq 0$, e

$$n = b_m \cdot b^m + b_{m-1} \cdot b^{m-1} + \cdots + b_1 \cdot b + b_0.$$

Ad esempio, il sistema binario è quello con $b = 2$, in cui le cifre che rappresentato i numeri zero e uno sono 0 e 1. Ancora, il sistema esadecimale è quello con $b = 16$, in cui le cifre che rappresentano i numeri da zero a quindici sono $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$; quindi, ad esempio, il numero in notazione esadecimale $A2C$ è il numero uguale, in notazione decimale, a $10 \cdot 16^2 + 2 \cdot 16 + 12 = 2604$.

Proposizione 5.5. *Un intero positivo è divisibile per* 2 *se e solo se l'ultima cifra decimale è divisibile per* 2 *(quindi è una tra* $0, 2, 4, 6, 8$*).*

Dimostrazione. Sia n con notazione decimale $a_m a_{m-1} \dots a_1, a_0$, cioè $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$. Allora $n - a_0 = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10$ è somma di numeri divisibili per 2 e quindi è divisibile per 2. Perciò n è divisibile per 2 se e solo se a_0 è divisibile per 2. □

Proposizione 5.6. *Un intero positivo è divisibile per* 5 *se e solo se l'ultima cifra decimale è divisibile per* 5 *(quindi è* 0 *o* 5*).*

Dimostrazione. La dimostrazione è analoga al criterio del 2, perché 10 è divisibile per 5. □

Proposizione 5.7. *Un intero positivo è divisibile per* 10 *se e solo se l'ultima cifra decimale è zero.*

Dimostrazione. La dimostrazione è analoga al criterio del 2. □

Proposizione 5.8. *Un intero positivo è divisibile per* 4 *se e solo se il numero constituito dalle ultime due cifre decimali è divisibile per* 4*.*

Dimostrazione. Se $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$, dove $a_0, \ldots, a_m$ sono le cifre decimali, allora $n - (a_1 \cdot 10 + a_0) = 100(a_m \cdot 10^{m-2} + a_{m-1} \cdot 10^{m-3} + \cdots + a_2)$ è divisibile per $100 = 4 \cdot 25$ e quindi per 4. Allora n è divisibile per 4 se e solo se il numero $a_1 \cdot 10 + a_0$ è divisibile per 4. □

Proposizione 5.9. *Un intero positivo è divisibile per* 8 *se e solo se il numero constituito dalle ultime tre cifre decimali è divisibile per* 8*.*

Dimostrazione. Se $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$, dove $a_0, \ldots, a_m$ sono le cifre decimali, allora $n - (a_2 \cdot 100 + a_1 \cdot 10 + a_0) = 1000(a_m \cdot 10^{m-3} + a_{m-1} \cdot 10^{m-4} + \cdots + a_3)$ è divisibile per $1000 = 8 \cdot 125$ e quindi per 8. Allora n è divisibile per 8 se e solo se il numero $a_2 \cdot 100 + a_1 \cdot 10 + a_0$ è divisibile per 8. □

Proposizione 5.10. *Un intero positivo è divisibile per* 3 *se e solo se la somma delle sue cifre decimali è divisibile per* 3*.*

Dimostrazione. Sia $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$, dove $a_0, \ldots, a_m$ sono le cifre decimali. Allora

$$n = a_m \cdot (10^m - 1) + a_{m-1} \cdot (10^{m-1} - 1) + \cdots + a_1 \cdot (10 - 1) + (a_m + a_{m-1} + \cdots + a_1 + a_0)\,.$$

I numeri $10^m - 1, 10^{m-1} - 1, \ldots, 10 - 1$ sono tutti divisibili per 3 (infatti, 10^i con $i \in \mathbb{N}$ soddisfa $10^i \equiv 1 \pmod 3$ e dunque $10^i - 1 \equiv 0 \pmod 3$). Perciò n è divisibile per 3 se e solo se $a_m + a_{m-1} + \cdots + a_1 + a_0$ è divisibile per 3. □

Proposizione 5.11. *Un intero positivo è divisibile per* 9 *se e solo se la somma delle sue cifre decimali è divisibile per* 9*.*

Dimostrazione. La dimostrazione è analoga al criterio del 3 dimostrato qui sopra, perché gli interi della forma $10^i - 1$ sono divisibili per 9. □

Proposizione 5.12. *Un intero positivo è divisibile per* 11 *se e solo se è divisibile per* 11 *il numero ottenuto sommando le cifre in posto dispari e sottraendo le cifre in posto pari.*

Dimostrazione. Sia $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$, dove $a_0, \ldots, a_m$ sono le cifre decimali. Contiamo i posti pari e dispari a partire dalla cifrà delle unità (non cambierebbe se iniziassimo dalla cifra più significativa). Se una cifra a_i è in posto pari, significa che i è dispari, quindi $a_i \cdot 10^i = a_i \cdot (10^i + 1) - a_i$; in questo caso, $10^i + 1$ è divisibile per 11 (perché $10^i \equiv -1 \pmod{11}$ e dunque $10^i + 1 \equiv 0 \pmod{11}$). Se una cifra a_i è in posto dispari, significa che i è pari, quindi $a_i \cdot 10^i = a_i \cdot (10^i - 1) + a_i$; in questo caso, $10^i - 1$ è divisibile per 11 (perché $10^i \equiv 1 \pmod{11}$ e dunque $10^i - 1 \equiv 0 \pmod{11}$). Allora

$$n = a_1 \cdot (10 + 1) + a_2 \cdot (10^2 - 1) + a_3 \cdot (10^3 + 1) + \cdots + (a_0 - a_1 + a_2 - a_3 + \cdots),$$

e dunque n è divisibile per 11 se e solo se $a_0 - a_1 + a_2 - a_3 + \cdots$ è divisibile per 11. □

5.3 Algoritmo euclideo e massimo comun divisore

Il calcolo del massimo comun divisore mediante la fattorizzazione dei due numeri è lungo computazionalmente. Vediamo come calcolarlo in modo più efficiente.

Teorema 5.13. *Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Allora esistono $q, r \in \mathbb{Z}$ con $0 \leq r < |b|$ tali che*

$$a = bq + r.$$

Tali q e r sono unici. q è detto quoziente *e r è detto* resto *della divisione euclidea di a per b.*

Dimostrazione. Consideriamo il seguente insieme

$$T = \{a - b\alpha \mid \alpha \in \mathbb{Z}, a - b\alpha \geq 0\}.$$

Si ha che $T \subseteq \mathbb{N}$, e inoltre $T \neq \emptyset$ (basta prendere $\alpha \leq a/b$). Perciò T ammette minimo $r := \min T$, perché $(\mathbb{N}, \leq)$ è un insieme ben ordinato. Indicato con q il valore di α per cui $a - b\alpha = r$, si ha chiaramente $a = bq + r$ e $r \geq 0$. Mostriamo che $r < |b|$. Supponiamo per assurdo che $r \geq |b|$, e sia $r_0 = r - |b| \geq 0$. Allora

$$0 \leq r_0 = r - |b| = a - bq - |b| = \begin{cases} a - (q+1)b & \text{se } b > 0, \\ a - (q-1)b & \text{se } b < 0. \end{cases}$$

Perciò $r_0 \in T$. Poiché $r_0 < r$, questo è assurdo perché contraddice $r = \min T$.

Mostriamo infine che quoziente e resto sono unici. Sia $qb + r = a = q'b + r'$, con $q, r, q', r' \in \mathbb{Z}$, $0 \leq r, r' < |b|$. Allora $(q - q')b = r' - r$. Poiché $|r' - r| < |b|$, ne segue $|q - q'| \cdot |b| < |b|$, da cui $q - q' = 0$, cioè $q = q'$. Da ciò si conclude anche $r = r'$. □

Illustriamo ora l'lalgoritmo euclideo, detto anche algoritmo delle divisioni successive.

Teorema 5.14. *Siano $a, b \in \mathbb{Z}$ con $a \geq b > 0$. Si ponga $r_{-1} := a$, $r_0 := b$, e si effettui ripetutamente la divisione euclidea tra r_i e r_{i+1} ($i \geq -1$) fino a ottenere resto zero:*

$$\begin{array}{ll} r_{-1} = r_0 q_1 + r_1 & 0 < r_1 < r_0, \\ r_0 = r_1 q_2 + r_2 & 0 < r_2 < r_1, \\ r_1 = r_2 q_3 + r_3 & 0 < r_3 < r_2, \\ \vdots & \vdots \\ r_{n-2} = r_{n-1} q_n + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_n q_n. & \end{array}$$

Allora $MCD(a, b) = r_n$.

Dimostrazione. Osserviamo per prima cosa che il procedimento è effettivamente un algoritmo, cioè termina in un numero finito di passi, perché il resto inizia minore di b e decresce a ogni passo: dopo al più b divisioni diventa zero.

Si consideri r_n. Dall'ultima equazione si ha che $r_n \mid r_{n-1}$; dalla penultima equazione si ha che r_n divide anche $r_{n-2} = r_{n-1} q_n + r_n$. Procedendo in questo modo, si ha che r_n divide r_0 e r_{-1}, cioè b e a.

Supponiamo che d sia un altro divisore comune di a e b. Da $a = bq_1 + r_1$ si ha che d divide anche r_1, da $b = r_1 q_2 + r_2$ si ha che d divide anche r_2, e così via. Procedendo in questa maniera si ottiene che $d \mid r_n$. Pertanto $r_n = MCD(a, b)$. □

Il valore assoluto $|n| \in \mathbb{N}$ di un intero $n \neq 0$ è detto anche *grado euclideo*. L'anello $\mathbb{Z}$ è detto un *anello euclideo* perché è un dominio di integrità munito di una "funzione grado" $\deg(\cdot) = |\cdot| : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ che soddisfa le seguenti due proprietà:

- $\deg(a) \leq \deg(a \cdot b)$ per ogni $a, b \in \mathbb{Z} \setminus \{0\}$;
- per ogni $a, b \in \mathbb{Z}$ con $b \neq 0$, esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$, e $r = 0$ oppure $\deg(r) < \deg(b)$.

Il seguente teorema esprime la cosiddetta *identità di Bézout*.

Teorema 5.15. *Siano a e b due interi positivi. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che*

$$MCD(a, b) = \alpha a + \beta b.$$

Dimostrazione. Supponiamo senza perdere generalità che $a \geq b$. Dal Teorema 5.14 si ha che $r_n = MCD(a,b) = r_{n-2} - r_{n-1}q_n$. Inoltre per ogni $i = 1, \ldots, n-1$ si ha che $r_i = r_{i-2} - q_i r_{i-1}$. Pertanto, tramite sostituzioni successive, per ogni $i = 1, \ldots, n-1$ è possibile scrivere $r_n = \alpha_i r_i + \beta_i r_{i-1}$ con $\alpha_i, \beta_i \in \mathbb{Z}$. Quindi $r_n = \alpha_2 r_2 + \beta_2 r_1$. Utilizzando che $r_2 = b - q_2 r_1$ e $r_1 = a - q_1 b$ otteniamo che $r_n = \alpha a + \beta b$ per qualche $\alpha, \beta \in \mathbb{Z}$. □

Vogliamo mostrare nel Teorema 5.17 una limitazione superiore sul costo computazionale del calcolo del massimo comun divisore tramite l'algoritmo euclideo. A tal fine, premettiamo un lemma tecnico.

Lemma 5.16. *Sia $(f_n)_n$ la successione di Fibonacci definita da $f_1 = 1$, $f_2 = 1$ e $f_n = f_{n-1} + f_{n-2}$ per ogni $n > 2$. Allora*

$$\forall\, n > 2 \in \mathbb{N} \Longrightarrow f_n > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2}.$$

Dimostrazione. Per $n = 3$ si ha che $f_3 = 2 > \frac{1+\sqrt{5}}{2}$ e quindi il passo base è verificato. Supponiamo che la proprietà valga al passo n e dimostriamola al passo $n+1$. Si ha che

$$f_{n+1} = f_n + f_{n-1} > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1+\sqrt{5}}{2}\right)^{n-3}$$

$$= \left(\frac{1+\sqrt{5}}{2}\right)^{n-3}\left(\frac{1+\sqrt{5}}{2}+1\right) = \left(\frac{1+\sqrt{5}}{2}\right)^{n-3}\left(\frac{3+\sqrt{5}}{2}\right)$$

$$= \left(\frac{1+\sqrt{5}}{2}\right)^{n-3}\left(\frac{1+\sqrt{5}}{2}\right)^{2} = \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}.$$

□

Teorema 5.17. *Siano a e b due interi positivi con $a \geq b$. Allora il numero di divisioni da effettuare per trovare $MCD(a,b)$ utilizzando l'algoritmo euclideo è minore o uguale a $5k$, dove k è il numero di cifre decimali di b.*

Dimostrazione. Supponiamo che il numero di divisioni da effettuare sia $n+1$. Allora per ogni $i = 0, \ldots, n-1$ si ha che $q_i \geq 1$, mentre $q_n \geq 2$, poiché $r_n < r_{n-1}$. Allora

$$\begin{array}{lcl} r_n & \geq & 1 = f_2 \\ r_{n-1} & \geq & 2r_n = 2 = f_3 \\ r_{n-2} & \geq & r_{n-1} + r_n \geq f_2 + f_3 = f_4 \\ \vdots & \vdots & \vdots \\ r_i & \geq & r_{i+1} + r_{i+2} \geq f_{n-i+1} + f_{n-i} = f_{n-i+2} \\ \vdots & \vdots & \vdots \\ r_1 & \geq & r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1} \\ b & \geq & r_1 + r_2 \geq f_{n+1} + f_n = f_{n+2} \end{array} .$$

Dunque $b \geq f_{n+2}$, l'$(n+2)$-esimo numero della successione di Fibonacci. Poiché

$$f_n > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2}$$

per ogni $n > 2$, allora $b > \left(\frac{1+\sqrt{5}}{2}\right)^n$ e

$$\log_{10} b > n \log_{10} \left(\frac{1+\sqrt{5}}{2}\right) > \frac{n}{5}.$$

Poiché $b < 10^k$, questo implica $n < 5 \log_{10} b = 5k$,e dunque $n + 1 \leq 5k$. □

5.4 Esercizi

Esercizio 5.2. *Determinare il massimo comun divisore d tra i numeri* 120 *e* 31 *utilizzando l'algoritmo Euclideo. Determinare inoltre due numeri α e β tali che $d = 120\alpha + 31\beta$.*

Soluzione. I passaggi dell'algoritmo sono riportati di seguito.

$$\begin{array}{lcl} 120 & = & 3 \cdot 31 + 27 \\ 31 & = & 1 \cdot 27 + 4 \\ 27 & = & 6 \cdot 4 + 3 \\ 4 & = & 1 \cdot 3 + 1 \\ 3 & = & 3 \cdot 1 + 0 \end{array}$$

Pertanto il massimo comun divisore tra i due numeri è 1. Inoltre si ha

$$\begin{array}{lcl} \mathbf{1} & = & -1 \cdot \mathbf{3} + \mathbf{4} \\ \mathbf{3} & = & -6 \cdot \mathbf{4} + \mathbf{27} \\ \mathbf{4} & = & -1 \cdot \mathbf{27} + \mathbf{31} \\ \mathbf{27} & = & -3 \cdot \mathbf{31} + \mathbf{120} \end{array}$$

Da cui segue

$$\begin{aligned}
\mathbf{1} &= -1 \cdot \mathbf{3} + \mathbf{4} \\
\mathbf{1} &= -1 \cdot (-6 \cdot \mathbf{4} + \mathbf{27}) + \mathbf{4} = 7 \cdot \mathbf{4} - 1 \cdot \mathbf{27} \\
\mathbf{1} &= 7 \cdot (-1 \cdot \mathbf{27} + \mathbf{31}) - 1 \cdot \mathbf{27} = -8 \cdot \mathbf{27} + 7 \cdot \mathbf{31} \\
\mathbf{1} &= -8 \cdot (-3 \cdot \mathbf{31} + \mathbf{120}) + 7 \cdot \mathbf{31} = 31 \cdot \mathbf{31} - 8 \cdot \mathbf{120}
\end{aligned}$$

Esercizio 5.3. *Determinare il massimo comun divisore d tra i numeri* 3522 *e* 321 *utilizzando l'algoritmo Euclideo. Determinare inoltre due numeri* α *e* β *tali che* $d = 3522\alpha + 321\beta$.

Soluzione I passaggi dell'algoritmo sono riportati di seguito.

$$\begin{aligned}
3522 &= 10 \cdot 321 + 312 \\
321 &= 1 \cdot 312 + 9 \\
312 &= 34 \cdot 9 + 6 \\
9 &= 1 \cdot 6 + 3 \\
6 &= 2 \cdot 2 + 0
\end{aligned}$$

L'ultimo resto non nullo è il MDC e quindi $d = 3$. Per ottenere l'identità di Bézout cominciamo riscrivendo queste identità (tranne l'ultima) isolando i resti. Otteniamo

$$\begin{aligned}
312 &= 3522 - 10 \cdot 321 \\
9 &= 321 - 1 \cdot 312 \\
6 &= 312 - 34 \cdot 9 \\
3 &= 9 - 1 \cdot 6
\end{aligned}$$

Cominciando dall'ultima riga adesso sostituiamo di volta in volta le precedenti

$$\begin{aligned}
3 &= 9 - 1 \cdot 6 \\
&= 9 - 1 \cdot (312 - 34 \cdot 9) \\
&= -1 \cdot 312 + 35 \cdot 9 \\
&= -1 \cdot 312 + 35 \cdot (321 - 1 \cdot 312) \\
&= 35 \cdot 321 - 36 \cdot 312 \\
&= 35 \cdot 321 - 36 \cdot (3522 - 10 \cdot 321) \\
&= -36 \cdot 3522 + 395 \cdot 321
\end{aligned}$$

Quindi $\alpha = -36$ 3 $\beta = 395$.

Esercizio 5.4. *Determinare il massimo comun divisore d tra i numeri* 220 *e* 121 *utilizzando l'algoritmo Euclideo. Determinare inoltre due numeri* α *e* β *tali che* $d = 220\alpha + 121\beta$.

Svolgimento. Utilizzando l'algoritmo di Euclide si ha:

$$\begin{aligned}
220 &= 121 \cdot 1 + 99 \\
121 &= 99 \cdot 1 + 22 \\
99 &= 22 \cdot 4 + 11 \\
22 &= 11 \cdot 22 + 0
\end{aligned}$$

L'ultimo resto non nullo è il MDC e quindi $d = 11$. Esplicitando i resti nei passaggi dell'algoritmo si ricava:

$$\begin{aligned} 99 &= 220 - 121 \\ 22 &= 121 - 99 = 121 - 220 + 121 = 2 \cdot 121 - 220 \\ 11 &= 99 - 22 \cdot 4 = (220 - 121) - (2 \cdot 121 - 220) \cdot 4 \\ 11 &= 220 - 121 - 8 \cdot 121 + 4 \cdot 220 \\ 11 &= 5 \cdot 220 - 9 \cdot 121 \end{aligned}$$

da cui deduciamo $\alpha = 5$ e $\beta = -9$.

Esercizio 5.5. *Trovare il massimo comun divisore di* 444 *e* 100.

Svolgimento. Utilizzando l'algoritmo di Euclide si ha:

$$\begin{aligned} 444 &= 100 \cdot 4 + 44 \\ 100 &= 44 \cdot 2 + 12 \\ 44 &= 12 \cdot 3 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$$

quindi $d = 4$.

Esercizio 5.6. *Trovare il massimo comun divisore di* 1547 *e* 560.

Svolgimento.

$$\begin{aligned} 1547 &= 560 \cdot 2 + 427 \\ 560 &= 427 \cdot 1 + 133 \\ 427 &= 133 \cdot 3 + 28 \\ 133 &= 28 \cdot 4 + 21 \\ 28 &= 21 \cdot 1 + 7 \\ 21 &= 7 \cdot 4 + 0 \end{aligned}$$

quindi $d = 7$.

Esercizio 5.7. *Sia n un intero che si scrive in modo unico (a meno dell'ordine dei fattori e del segno) come prodotto di numeri primi:*

$$n = p_1 p_2 \cdots p_r,$$

dimostrare che se q è un numero primo che divide n allora $q = p_i$ per qualche i.

Svolgimento. Dato che q divide n esisterà m tale che $n = qm$. Sappiamo che m si scrive come un prodotto di numeri primi, quindi $m = q_1 q_2 \cdots q_t$. Poichè sappiamo che la fattorizzazione è unica deve essere $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_t q$, quindi $q = p_i$, per qualche i.

Capitolo 6

Polinomi univariati

Definizione 6.1. *Sia* $\mathbb{K}$ *un campo. Un* polinomio $f(x)$ *a coefficienti in* $\mathbb{K}$ *in una indeterminata* x *è una somma formale di monomi, del tipo*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \quad = \quad \sum_{i=0}^{n} a_i x^i,$$

con $a_1, \ldots, a_n \in \mathbb{K}$ *e* $n \in \mathbb{N}$*. Gli elementi* a_i *sono i* coefficienti *del polinomio* $f(x)$*.*

Esempio 6.2. *Sia* $\mathbb{Q}$ *il campo dei numeri razionali. Allora* $p(x) = 3x + \frac{5}{4}x^2 - 3x^3$ *è un polinomio a coefficienti in* $\mathbb{Q}$*, mentre* $3x^{-2} + x - 3x^4$ *non è un polinomio.*

L'insieme di tutti i polinomi a coefficienti in $\mathbb{K}$ nell'indeterminata x si indica con $\mathbb{K}[x]$.

Osservazione 6.3. *Un polinomio è univocamente determinato dai suoi coefficienti. Quindi due polinomi* $f(x), g(x) \in \mathbb{K}[x]$ *del tipo*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$$

sono uguali se e solo se $a_i = b_i$ *per ogni* $i \geq 0$*.*

Siano $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$ due polinomi in $\mathbb{K}[x]$. Allora possiamo definire la somma $f(x) + g(x)$ e il prodotto $f(x) \cdot g(x)$ nel seguente modo:

$$f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i,$$

$$f(x) \cdot g(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j \cdot b_{i-j} \right) x^i,$$

dove $a_i = 0$ se $i > n$ e $b_i = 0$ se $i > m$.

Esempio 6.4. *Consideriamo in* $\mathbb{R}[x]$ *i polinomi* $f(x) = 4x^2 + 3x$ *e* $g(x) = x^4 + 3x^2 + 2x + 2$. *La loro somma è* $h(x) = x^4 + 7x^2 + 5x + 2$. *Il loro prodotto è* $k(x) = 4x^6 + 3x^5 + 12x^4 + 17x^3 + 14x^2 + 6x$.

Il *polinomio nullo* 0 è quello con tutti i coefficienti uguali a zero.

Teorema 6.5. $(\mathbb{K}[x], +, \cdot)$ *è un dominio di integrità.*

Dimostrazione. Omettiamo la verifica che $(\mathbb{K}[x], +, \cdot)$ è un anello commutativo unitario; ciò dipende essenzialmente dalle proprietà di campo di $\mathbb{K}$. Lo zero di questo anello è il polinomio nullo, l'unità è il polinomio costante uguale a 1.

Se $f(x), g(x) \in \mathbb{K}[x]$ sono due polinomi non nulli, con monomi di grado massimo rispettivamente $a_n x^n$ e $b_m x^m$, allora il monomio di grado massimo in $f(x) \cdot g(x)$ è $a_n b_m x^{n+m}$. In particolare, $f(x) \cdot g(x)$ non è il polinomio nullo. Quindi $(\mathbb{K}[x], +, \cdot)$ è un dominio di integrità. □

Definizione 6.6. *Sia* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{K}[x]$ *un polinomio non nullo. Allora il* grado *di* $f(x)$ *è*

$$\deg f(x) = \max\{i \ : \ a_i \neq 0\}.$$

Per convenzione, il grado del polinomio nullo è posto uguale a $-\infty$, per il quale assumimo le seguenti regole di calcolo: $\max\{-\infty, d\} = d$ e $-\infty + d = -\infty$, per ogni $d \in \mathbb{N}$.

Esempio 6.7. *Il polinomio* $h(x) = 2 + 5x + x^4 \in \mathbb{C}[x]$ *ha grado* 4.

Il grado di un polinomio gode delle seguenti proprietà:

- per ogni $f(x), g(x) \in \mathbb{K}[x]$, vale $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.
- se $\deg f(x) \neq \deg g(x)$, allora $\deg(f(x) + g(x)) = \max\{\deg f(x), \deg g(x)\}$.
- per ogni $f(x), g(x)$ non nulli, vale $\deg f(x) \leq \deg(f(x) \cdot g(x))$.
- $\deg f(x) = 0$ se e solo se $f(x)$ è un polinomio costante k, per qualche $k \in \mathbb{K} \setminus \{0\}$.

Valgono inoltre le seguenti proprietà:

- $f(x)$ è un elemento invertibile di $\mathbb{K}[x]$ se e solo se $f(x)$ è un polinomio costante non nullo.
- In $\mathbb{K}[x]$ gli elementi primi e gli elementi irriducibili coincidono.

Mostriamo che in $\mathbb{K}[x]$ si può fare la divisione euclidea.

Proposizione 6.8. *Siano $f(x), g(x) \in \mathbb{K}[x]$ due polinomi con $g(x) \neq 0$. Allora esistono e sono unici due polinomi $q(x), r(x) \in \mathbb{K}[x]$, tali che $r(x) = 0$ oppure $\deg r(x) < \deg g(x)$, e*

$$f(x) = g(x)q(x) + r(x).$$

Dimostrazione. Se $\deg g(x) > \deg f(x)$ allora possiamo scrivere

$$f(x) = 0 \cdot g(x) + f(x)$$

e l'asserto è verificato. Possiamo quindi supporre che $\deg g(x) \leq \deg f(x)$ e $f(x) \neq 0$. Procediamo per induzione su $n = \deg f(x)$. Se $n = 0$ allora $f(x) = a_0$ e $g(x) = b_0 \neq 0$. Allora

$$a_0 = \frac{a_0}{b_0} \cdot b_0 + 0$$

e quindi il passo base è verificato. Supponiamo ora che l'asserto sia vero quando $\deg f(x) \leq n$. Consideriamo un generico polinomio $f(x) = a_{n+1}x^{n+1} + \cdots + a_0 \in \mathbb{K}[x]$ di grado $n+1$. Scriviamo $g(x) = b_m x^m + \cdots + b_0$, dove $m = \deg g(x) \leq n+1$. Il polinomio

$$f(x) - \frac{a_{n+1}}{b_m} x^{n+1-m} g(x)$$

ha grado al più n e pertanto, usando l'ipotesi induttiva, possiamo affermare che esistono $q(x), r(x) \in \mathbb{K}[x]$, con $r = 0$ oppure $\deg r(x) < \deg g(x)$, tali che

$$f(x) - \frac{a_{n+1}}{b_m} x^{n+1-m} g(x) = q(x)g(x) + r(x).$$

Questo implica

$$f(x) = \left(\frac{a_{n+1}}{b_m} x^{n+1-m} + q(x) \right) g(x) + r(x).$$

Perciò la tesi è dimostrata. □

Quindi $\mathbb{K}[x]$ munito del grado è un anello euclideo. Pertanto è possibile calcolare un massimo comun divisore tra due polinomi tramite l'algoritmo euclideo delle divisioni successive.

Il procedimento è esattamente lo stesso di quello visto per i numeri interi; invece che il valore assoluto di numeri interi, il grado euclideo qui considerato è il grado dei polinomi.

Teorema 6.9. *Sia $\mathbb{K}$ un campo e siano $f(x), g(x) \in \mathbb{K}[x]$ con $g(x) \neq 0$ e $\deg f(x) \geq \deg g(x)$. Si ponga $r_{-1}(x) := f(x)$, $r_0(x) := g(x)$, e si effettui ripetutamente la divisione euclidea tra $r_i(x)$ e $r_{i+1}(x)$ ($i \geq -1$) fino a ottenere resto zero:*

$$\begin{array}{ll} r_{-1}(x) = r_0(x)q_1(x) + r_1(x) & 0 < \deg r_1(x) < \deg r_0(x), \\ r_0(x) = r_1(x)q_2(x) + r_2(x) & 0 < \deg r_2(x) < \deg r_1(x), \\ r_1(x) = r_2(x)q_3(x) + r_3(x) & 0 < \deg r_3(x) < \deg r_2(x), \\ \vdots & \vdots \\ r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x) & 0 < \deg r_n(x) < \deg r_{n-1}(x), \\ r_{n-1}(x) = r_n(x)q_n(x) & \end{array}.$$

Allora $r_n(x)$ è un MCD tra $f(x)$ e $g(x)$.

Dimostrazione. Osserviamo per prima cosa che il procedimento è effettivamente un algoritmo, cioè termina in un numero finito di passi, perché il grado del resto inizia minore del grado di $g(x)$ e decresce a ogni passo: dopo al più $\deg g(x)$ divisioni diventa nullo oppure di grado zero; in questo secondo caso, abbiamo ottenuto una costante non nulla, che divide ogni possibile polinomio, e l'algoritmo termina al passo successivo.

Si consideri $r_n(x)$. Dall'ultima equazione si ha che $r_n(x) \mid r_{n-1}(x)$; dalla penultima equazione si ha che $r_n(x)$ divide anche $r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$. Procedendo in questo modo, si ha che $r_n(x)$ divide $r_0(x)$ e $r_{-1}(x)$, cioè $g(x)$ e $f(x)$.

Supponiamo che $d(x)$ sia un altro divisore comune di $f(x)$ e $g(x)$. Da $f(x) = g(x)q_1(x) + r_1(x)$ si ha che $d(x)$ divide anche $r_1(x)$, da $g(x) = r_1(x)q_2(x) + r_2(x)$ si ha che $d(x)$ divide anche $r_2(x)$, e così via. Procedendo in questa maniera si ottiene che $d(x) \mid r_n(x)$. Pertanto $r_n(x) = MCD(f(x), g(x))$. □

Poiché i polinomi invertibili in $\mathbb{K}[x]$ sono le costanti non nulle, allora ogni volta che moltiplichiamo un $MCD(f(x), g(x))$ per una costante diversa da zero, otteniamo un altro $MCD(f(x), g(x))$. Un modo per fissarne uno solo è scegliere quello *monico*, cioè che ha 1 come coefficiente del monomio di grado massimo.

Definizione 6.10. *Sia $f(x) \in \mathbb{K}[x]$. Un elemento $\alpha \in \mathbb{K}$ si dice* radice *di $f(x)$ (o* zero *di $f(x)$) se $f(\alpha) = 0$.*

Teorema 6.11. (Teorema di Ruffini) *Sia $f(x) \in \mathbb{K}[x]$ e sia $\alpha \in \mathbb{K}$. Allora α è una radice di $f(x)$ se e solo se $(x - \alpha) \mid f(x)$.*

Dimostrazione. Se $(x - \alpha) \mid f(x)$, allora per qualche $g(x)$ si ha $f(x) = (x - \alpha)g(x)$; dunque $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$ cioè α è una radice di $f(x)$.

Viceversa, sia α una radice di $f(x)$. Dividendo $f(x)$ per $(x-\alpha)$, otteniamo

$$f(x) = (x-\alpha)q(x) + r(x),$$

con $q(x), r(x) \in \mathbb{K}[x]$, dove $\deg r(x) = 0$ oppure $r(x)$ è il polinomio nullo. In ogni caso, $r(x) = k$ per qualche costante $k \in \mathbb{K}$. Poiché α è una radice di $f(x)$ allora

$$0 = f(\alpha) = (\alpha-\alpha)q(\alpha) + k = 0 \cdot q(\alpha) + k = k.$$

Pertanto $k = 0$ e dunque $f(x) = (x-\alpha) \cdot q(x)$ per qualche $q(x) \in \mathbb{K}[x]$, cioè $(x-\alpha)$ divide $f(x)$. □

Definizione 6.12. *Sia $f(x) \in \mathbb{K}[x]$ e sia $\alpha \in \mathbb{K}$ una radice di $f(x)$. La* molteplicità *di α come radice di $f(x)$ è l'intero positivo m tale che*

$$(x-\alpha)^m | f(x) \qquad e \qquad (x-\alpha)^{m+1} \nmid f(x).$$

Osservazione 6.13. *Evidentemente, un polinomio non nullo $f(x) \in \mathbb{K}[x]$ di grado n ammette al più n radici in $\mathbb{K}$, contate con molteplicità.*

Un campo $\mathbb{K}$ si dice algebricamente chiuso *se tutti i polinomi non nulli di grado n in $\mathbb{K}[x]$ ammettono esattamente n radici in $\mathbb{K}$, contando con molteplicità. Si dimostra che il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso, mentre $\mathbb{Q}$, $\mathbb{R}$ e i campi con un numero finito di elementi non sono algebricamente chiusi.*

Richiamiamo il concetto di elemento irriducibile nel contesto di $\mathbb{K}[x]$, dove gli elementi invertibili sono le costanti non nulle.

Definizione 6.14. *Un Polinomio non nullo $f(x) \in \mathbb{K}[x]$ si dice* riducibile *se esistono $g(x), h(x) \in \mathbb{K}[x]$ di grado positivo tali che $f(x) = g(x) \cdot h(x)$. Il polinomio f si dice* irriducibile *se non è riducibile.*

Proposizione 6.15. *Ogni polinomio di primo grado è irriducibile.*

Un polinomio in $\mathbb{K}[x]$ di grado 2 o 3 è irriducibile se e solo se non ha radici in $\mathbb{K}$.

Dimostrazione. Usiamo che $\deg(g(x) \cdot h(x)) = (\deg g(x)) \cdot (\deg h(x))$. Da ciò segue immediatamente che ogni polinomio di grado 1 è irriducibile.

Supponiamo ora che $f(x)$ abbia grado 2 o 3. Se $f(x)$ ha una radice $\alpha \in \mathbb{K}$, allora per il teorema di Ruffini $f(x) = (x-\alpha) \cdot h(x)$ con $\deg(x-\alpha) = 1$ e $\deg h(x) = \deg f(x) - 1 \geq 1$, quindi $f(x)$ è riducibile. Viceversa, se $f(x)$ e riducibile, allora $f(x) = g(x) \cdot h(x)$, con

$\deg g(x) \geq 1$, $\deg h(x) \geq 1$ e $\deg g(x) + \deg h(x) \in \{2, 3\}$. Allora almeno uno tra $g(x)$ e $h(x)$ ha grado 1, e quindi ha una radice in $\mathbb{K}$, che è anche una radice di $f(x)$. □

Osserviamo che un polinomio di grado ≥ 4 può essere riducibile ma non avere radici. Ad esempio, il polinomio $f(x) = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ è riducibile perché $f(x) = (x^2+1)\cdot(x^2+1)$, ma non ha radici in $\mathbb{R}$.

6.1 Esercizi

Esercizio 6.1. *Descrivere quali sono i polinomi irriducibili della forma* $f(x) = ax^2+bx+c \in \mathbb{R}[x]$*, con* $a, b, c \in \mathbb{R}$ *e* $a \neq 0$

Soluzione. Poiché $f(x)$ ha grado 2, allora $f(x)$ è irriducibile se e solo se non ha radici in $\mathbb{R}$. Dalla ben nota formula risolutiva per le equazioni di secondo grado, questo equivale a chiedere che $b^2 - 4ac < 0$.

Esercizio 6.2. *Trovare tutti i polinomi irriducibili di grado* 2 *e* 3 *in* $\mathbb{Z}_2[x]$.

Soluzione Dobbiamo trovare i polinomi di grado 2 e 3 in $\mathbb{Z}_2[x]$ che non hanno radici in $\mathbb{Z}_2$. Ricordiamo che su $\mathbb{Z}_2 = \{0, 1\}$ le operazioni sono definite come segue:

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0, \qquad 0\cdot 0=0, \quad 0\cdot 1=0, \quad 1\cdot 0=0, \quad 1\cdot 1=1.$$

Il coefficiente del monomio di grado massimo deve essere diverso da zero, e quindi è 1. L'unico polinomio della forma $x^2 + ax + b \in \mathbb{Z}_2[x]$ che non ha radici in $\mathbb{Z}_2[x]$ è $x^2 + x + 1$. Gli unici polinomi della forma $x^3 + ax^2 + bx + c$ che non hanno radici in $\mathbb{Z}_2$ sono $x^3 + x^2 + 1$ e $x^3 + x + 1$.

Si noti in generale che un polinomio irriducibile di grado positivo deve avere termine noto diverso da zero (se no ammette il fattore x). Se i coefficienti sono in $\mathbb{Z}_2$, l'unico valore che resta è 1. Un polinomio della forma $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1 \in \mathbb{Z}_2[x]$ ammette radici in $\mathbb{Z}_2$ se e solo se ammette la radice 1, e questo accade se e solo se il numero di monomi che appaiono nel polinomio è pari.

Esercizio 6.3. *Trovare tutti i polinomi irriducibili del tipo* $x^5 + ax^2 + b \in \mathbb{Z}_2[x]$.

Soluzione. Per calcolo diretto, l'unico polinomio di questo tipo che non ha radici in $\mathbb{Z}_2$ è $x^5 + x^2 + 1$. Se $x^5 + x^2 + 1$ non fosse irriducibile sarebbe il prodotto di un polinomio irriducibile di grado 2 e uno di grado 3. L'unico polinomio irriducibile di grado due su $\mathbb{Z}_2$ è $x^2 + x + 1$. Pertanto $x^5 + x^2 + 1$ dovrebbe essere divisibile per $x^2 + x + 1$. Questo non succede, perché la divisione euclidea in $\mathbb{Z}_2[x]$ dà $x^5 + x^2 + 1 = (x^2 + x + 1)(x^3 + x^2) + 1$. Quindi $x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$ è irriducibile.

Esercizio 6.4. *Si consideri il polinomio* $f(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$.

- *Determinare le radici del polinomio* f *in* $\mathbb{Z}_2$.
- *Determinare la scomposizione del polinomio* f *in fattori irriducibili sopra* $\mathbb{Z}_2$.

Soluzione. Si verifica subito che $f(x)$ non ha radici in $\mathbb{Z}_2$. In particolare, questo significa che non ha fattori di grado 1. Perciò, se $f(x)$ è riducibile, allora deve avere un fattore irriducibile di grado 2 e uno di grado 3. L'unico polinomio irriducibile di grado 2 su $\mathbb{Z}_2$ è $x^2 + x + 1$. Effettivamente, effettuando la divisione tra questi due polinomi si ha che $f(x) = (x^2 + x + 1)(x^3 + x + 1)$. Questa è la scomposizione di $f(x)$ in fattori irriducibili in $\mathbb{Z}_2[x]$.

Esercizio 6.5. *Si consideri il polinomio $f(x) = x^5 + 1 \in \mathbb{Z}_2[x]$.*

- *Determinare le radici del polinomio f in $\mathbb{Z}_2$.*
- *Determinare la scomposizione del polinomio f in fattori irriducibili sopra $\mathbb{Z}_2$.*

Soluzione. Si vede facilmente che 1 è una radice del polinomio $f(x)$. Quindi il polinomio si scompone in $(x+1)(x^4+x^3+x^2+x+1)$. Il fattore di quarto grado $x^4+x^3+x^2+x+1$ non ha radici in $\mathbb{Z}_2$. Se fosse scomponibile avrebbe due fattori di grado due irriducibili. L'unico polinomio di grado 2 che è irriducibile su $\mathbb{Z}_2$ è $x^2 + x + 1$. Pertanto l'unica possibilità è che $x^4+x^3+x^2+x+1$ fosse uguale a $(x^2+x+1)^2$. non essendo questo il caso, la decomposizione di $x^5 + 1$ è proprio $(x + 1)(x^4 + x^3 + x^2 + x + 1)$.

Esercizio 6.6. *Si consideri il polinomio $f(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x \in \mathbb{Q}[x]$, e si effettui la scomposizione di $f(x)$ in fattori irriducibili sopra $\mathbb{Q}$.*

Soluzione. Si vede facilmente che 0 e 1 sono radici di $f(x)$, quindi $f(x)$ è divisibile per x e per $x - 1$. Raccogliendo x, si ha $f(x) = x(x^5 - x^4 + x^3 - x^2 + x - 1)$. Effettuando la divisione tra $x^5 - x^4 + x^3 - x^2 + x - 1$ e $x - 1$ si ha $f(x) = x(x - 1)(x^4 + x^2 + 1)$. Dobbiamo ora provare a scomporre il fattore $g(x) = x^4 + x^2 + 1 \in \mathbb{Q}[x]$.

$g(x)$ ha un fattore di primo grado in $\mathbb{Q}[x]$ se e solo se ha una radice in $\mathbb{Q}$. Ma, per ogni numero $\alpha \in \mathbb{Q}$, $g(\alpha) = \alpha^4 + \alpha^2 + 1$ è una somma di addendi non negativi e $g(\alpha) > 0$, quindi $g(\alpha) \neq 0$. Perchiò $g(x)$ non ha radici in $\mathbb{Q}$ e non ha fattori di primo grado in $\mathbb{Q}[x]$.

Supponiamo che $g(x)$ abbia fattori di secondo grado su $\mathbb{Q}$. In tal caso, a meno di moltiplicare i fattori di $g(x)$ per costanti diverse da zero, la sua fattorizzazione è

$$g(x) = (x^2 + ax + b) \cdot (x^2 + cx + d),$$

per qualche $a, b, c, d \in \mathbb{Q}$. Svolgendo i calcoli, questo significa

$$x^4 + x^2 + 1 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.$$

Uguagliando i coefficienti dei monomi dello stesso grado, si ha il sistema

$$\begin{cases} a+c=0 \\ b+d+ac=1 \\ ad+bc=0 \\ bd=1 \end{cases}$$

Ricavando $a=-c$ dalla prima equazione, la terza equazione diventa $c(b-d)=0$. Perciò $c=0$ oppure $b-d=0$. Nel primo caso $c=0$ il sistema dà le equazioni: $a=c=0$, $b+d=1$ e $bd=1$. Dalle ultime due si ricava per sostituzione $b^2-b+1=0$, che non ha soluzione in $\mathbb{Q}$ (perché $\Delta=-3<0$). Quindi questo caso non succede e vale $b-d=0$. Il sistema diventa

$$\begin{cases} a=-c \\ d=b \\ b=\frac{c^2+1}{2} \\ b^2=1 \end{cases}$$

La quarta equazione dà $b=-1$ (che però è incompatibile con la terza equazione) oppure $b=1$. Con $b=1$ si ottiene $b=1$, $d=1$; in più, $c=1$ e $a=1$, oppure $c=-1$ e $a=1$.

La scelta di a e c non è importante (cambia solo l'ordine dei due fattori di $g(x)$), abbiamo ottenuto che $g(x)=(x^2+x+1)(x^2-x+1)$. Perciò la fattorizzazione di $f(x)$ in fattori irriducibili su $\mathbb{Q}$ è

$$f(x)=x(x-1)(x^2+x+1)(x^2-x+1).$$

Esercizio 6.7. *Si determini un massimo comun divisore in $\mathbb{Q}[x]$ tra i polinomi $5x^5-2x-3$ e x^3-1.*

Soluzione. Con l'algoritmo euclideo delle divisioni successive otteniamo

$$5x^5-2x-3=(x^3-1)(5x^2)+(3x^2-3)$$

$$x^3-1=(3x^2-3)(\frac{1}{3}x)+(x-1)$$

$$3x^2-3=(x-1)\cdot(3).$$

Quindi un massimo comun divisore in $\mathbb{Q}[x]$ tra $5x^2-2x-3$ e x^3-1 è $x-1$.

Esercizio 6.8. *Determinare, se esistono, i polinomi $P(x),Q(x)\in\mathbb{Q}[x]$ tali che*

$$P(x)(x^2+1)+Q(x)(x^3-3)=20$$

Soluzione. I polinomi $P(x)$ e $Q(x)$ sono entrambi irriducibili su $\mathbb{Q}[x]$ in quanto -1 non è un quadrato e 3 non è un cubo. Quindi non hanno fattori comuni di grado positivo, e perciò un loro MCD è 1, o anche qualsiasi altra costante non nulla, come 20. Perciò per l'identità di Bézout possiamo ricavare i polinomi $P(x)$ e $Q(x)$ richiesti. Per prima cosa, applichiamo l'algoritmo euclideo:

$$x^3 - 3 = (x^2 + 1)x + (-x - 3)$$

$$x^2 + 1 = (-x - 3)(-x + 3) + 10.$$

Ora ricaviamo 10 "all'indietro":

$$10 \;=\; (x^2+1) - (-x-3)(-x+3) \;=\; x^2 + 1 - \left(x^3 - 3 - (x^2+1)x\right)(-x+3)$$

$$\Rightarrow 10 \;=\; (1 + x(-x+3))\,(x^2{+}1) - (-x+3)\,(x^3{-}3) \;=\; (-x^2{+}3x{+}1)(x^2{+}1) + (x{-}3)(x^3{-}3).$$

Moltiplicando per 2 l'ultima identità si ha

$$20 \quad = \quad (-2x^2 + 6x + 2)(x^2 + 1) + (2x - 6)(x^3 - 3),$$

da cui $P(x) = -2x^2 + 6x + 2$ e $Q(x) = 2x - 6$.

Capitolo 7

Spazi vettoriali $\mathbb{K}^n$

7.1 Lo spazio $\mathbb{K}^n$ e i suoi sottospazi vettoriali

Nel seguito $\mathbb{K}$ denoterà sempre un campo. Ricordiamo che un campo $\mathbb{K}$ è un insieme non vuoto munito di due operazioni di somma "+" e prodotto "$\cdot$" con le seguenti proprietà:

- $(\mathbb{K}, +)$ è un gruppo abeliano, cioè: la somma è commutativa; è associativa; ammette elemento neutro (lo zero 0); ogni elemento $a \in \mathbb{K}$ ammette l'elemento opposto $-a$.

- $(\mathbb{K} \setminus \{0\}, \cdot)$ è un gruppo abeliano, cioè: il prodotto è commutativo; è associativo; ammette elemento neutro (l'uno 1); ogni elemento $a \in \mathbb{K}$ diverso da zero ammette l'elemento inverso a^{-1}.

- Il prodotto è distributivo (a destra e sinistra) rispetto alla somma.

Esempi di campi sono: $\mathbb{Q}$ (numeri razionali); $\mathbb{R}$ (numeri reali); $\mathbb{C}$ (numeri complessi); $\mathbb{Z}_2$ (campo binario).

Fissato un intero positivo n, consideriamo

$$\mathbb{K}^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{K}\}.$$

Gli elementi di $\mathbb{K}^n$ sono detti *vettori*, e vengono spesso indicati con $u, v, \underline{u}, \underline{v}, \ldots$. Gli elementi di $\mathbb{K}$ sono detti *scalari*, e vengono spesso indicati con lettere greche $\alpha, \beta, \gamma \ldots$.

Definiamo un'operazione di *somma vettoriale*:

$$\begin{aligned} \mathbb{K}^n \times \mathbb{K}^n &\to \mathbb{K}^n \\ (a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n), \end{aligned}$$

e un'operazione di *prodotto esterno*:

$$\begin{aligned} \mathbb{K} \times \mathbb{K}^n &\to \mathbb{K}^n \\ \alpha \cdot (a_1, \ldots, a_n) &= (\alpha \cdot a_1, \ldots, \alpha \cdot a_n). \end{aligned}$$

Il seguente teorema, di facile verifica, enuncia le proprietà vettoriali di $\mathbb{K}^n$. Si noti che il simbolo "+" denota sia la somma in $\mathbb{K}$ che la somma vettoriale in $\mathbb{K}^n$, e che il simbolo "$\cdot$" denota sia il prodotto in $\mathbb{K}$ che il prodotto esterno di $\mathbb{K}^n$. Il significato è chiaro dal contesto.

Teorema 7.1. $\mathbb{K}^n$*, con le operazioni di somma vettoriale e di prodotto esterno, è uno* spazio vettoriale*, cioè:*

- $(\mathbb{K}^n, +)$ *è un gruppo abeliano:*
  - *prop. commutativa:* $u + v = v + u \quad \forall u, v \in \mathbb{K}^n$,
  - *prop. associativa:* $(u + v) + w = u + (v + w) \quad \forall u, v, w \in \mathbb{K}^n$,
  - $\underline{0} := (0, \ldots, 0)$ *è elemento neutro:* $v + \underline{0} = \underline{0} + v = v \quad \forall v \in \mathbb{K}^n$,
  - *ogni* $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{K}^n$ *ammette opposto* $-\underline{a} := (-a_1, \ldots, -a_n)$*, cioè:* $\underline{a} + (-\underline{a}) = (-\underline{a}) + \underline{a} = \underline{0}$;
- $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v, \quad \forall \alpha \in \mathbb{K}, \forall u, v \in \mathbb{K}^n$;
- $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v, \quad \forall \alpha, \beta \in \mathbb{K}, \forall v \in \mathbb{K}^n$;
- $(\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v), \quad \forall \alpha, \beta \in \mathbb{K}, \forall v \in \mathbb{K}^n$;
- $1 \cdot v = v, \quad \forall v \in \mathbb{K}^n$.

Come usuale, anche il simbolo "$\cdot$" del prodotto esterno verrà omesso. Le seguenti proprietà sono di facile verifica.

Proposizione 7.2. *Per ogni* $\lambda \in \mathbb{K}$ *e* $v \in \mathbb{K}^n$ *valgono le seguenti proprietà:*

- $\lambda v = \underline{0}$ *se e solo se* $\lambda = 0$ *oppure* $v = \underline{0}$.
- $(-\lambda)v = \lambda(-v) = -(\lambda v)$.

Definizione 7.3. *Un sottoinsieme* $U \subseteq \mathbb{K}^n$ *si dice un* sottospazio vettoriale *di* $\mathbb{K}^n$ *se valgono le seguenti proprietà:*

- $U \neq \emptyset$,
- *per ogni* $u, v \in U$ *si ha* $u + v \in U$,
- *per ogni* $\lambda \in \mathbb{K}$ *e* $u \in U$ *si ha* $\lambda u \in U$.

Si dice anche che $U \neq \emptyset$ è un sottospazio vettoriale di $\mathbb{K}^n$ quando è *linearmente chiuso*, cioè chiuso rispetto alle operazioni di somma vettoriale e di prodotto esterno.

Osservazione 7.4. *Un sottospazio vettoriale* U *di* $\mathbb{K}^n$ *è esso stesso uno* spazio vettoriale, *cioè valgono tutte le proprietà enunciate nel Teorema 7.1, in cui* $\mathbb{K}^n$ *è sostituito da* U.

Si osservi anche che ogni sottospazio vettoriale contiene il vettore nullo $\underline{0}$ di $\mathbb{K}^n$.

Definizione 7.5. *Diremo* spazio vettoriale *su campo* $\mathbb{K}$ *gli spazi* $\mathbb{K}^n$ *e i loro sottospazi vettoriali.*

Esempio 7.6.
- $\{\underline{0}\}$ *è un sottospazio vettoriale di* $\mathbb{K}^n$, *detto* sottospazio banale.
- $\mathbb{K}^n$ *è un sottospazio vettoriale di* $\mathbb{K}^n$.

Esempio 7.7. *Si consideri il sottoinsieme* $U = \{(x, y) \in \mathbb{R}^2 \colon x + 2y = 0\}$ *di* $\mathbb{R}^2$. *Allora* U *è un sottospazio vettoriale di* $\mathbb{R}^2$. *Infatti:*

- $(0, 0) \in U$;
- *se* $(x_1, y_1), (x_2, y_2) \in U$, *allora* $(x_1+x_2)+2(y_1+y_2) = (x_1+2y_1)+(x_2+2y_2) = 0+0 = 0$, *e quindi* $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ *sta in* U;
- *se* $\lambda \in \mathbb{R}$ *e* $(x_1, y_1) \in U$, *allora* $\lambda x_1 + 2(\lambda y_1) = \lambda(x_1 + 2y_1) = \lambda \cdot 0 = 0$, *e quindi* $\lambda(x_1, y_1) = (\lambda x_1, \lambda y_1)$ *sta in* U.

Il sottoinsieme $V = \{(x, y) \in \mathbb{R}^2 \colon x + 2y = 1\}$ *non è un sottospazio vettoriale di* $\mathbb{R}^2$: *basta osservare che* $(0, 0) \notin V$.

Il sottoinsieme $W = \{(x, y) \in \mathbb{R}^2 \colon x^2 - y^2 = 0\}$ *non è un sottospazio vettoriale di* $\mathbb{R}^2$: *infatti* $(1, 1), (1, -1) \in W$, *ma* $(1, 1) + (1, -1) = (2, 0) \notin W$.

Il sottoinsieme $Z = \{(x, y) \in \mathbb{R}^2 \colon x^2 - y = 0\}$ *non è un sottospazio vettoriale di* $\mathbb{R}^2$*: infatti* $(1, 1) \in Z$ *ma* $2(1, 1) = (2, 2) \notin Z$*.*

Enunciamo il seguente teorema, di cui omettiamo la dimostrazione.

Teorema 7.8. *Siano* U *e* W *due sottospazi vettoriali di* $\mathbb{K}^n$*. Allora*

$$U \cap W := \{v \in \mathbb{K}^n \mid v \in U,\ v \in W\}, \qquad U + W := \{u + w \in \mathbb{K}^n \mid u \in U, w \in W\}$$

sono due sottospazi vettoriali di $\mathbb{K}^n$*, detti rispettivamente il* sottospazio intersezione *e il* sottospazio somma *di* U *e* W*.*

Inoltre, $U + W$ *è il più piccolo sottospazio vettoriale di* $\mathbb{K}^n$ *che contiene l'unione* $U \cup W$*.*

Osservazione 7.9. *In generale, l'unione insiemistica* $U \cup W$ *di due sottospazi vettoriali non è un sottospazio vettoriale.*

Un controesempio è il seguente: $U = \{(x, 0) \mid x \in \mathbb{R}\}$ *e* $W = \{(0, y) \mid y \in \mathbb{R}\}$ *sono due sottospazi vettoriali di* $\mathbb{R}^2$*, ma la loro unione* $U \cup W = \{(x, y) \in \mathbb{R}^2 \mid x = 0 \vee y = 0\}$ *non è un sottospazio vettoriale. Se un sottospazio vettoriale di* $\mathbb{R}^2$ *contiene* $U \cup W$*, allora in particolare contiene* $(1, 0) \in U$ *e* $(0, 1) \in W$*, e quindi contiene* $\lambda(1, 0) = (\lambda, 0)$ *e* $(0, \mu)$ *per ogni* $\lambda, \mu \in \mathbb{R}$*, e quindi contiene* (λ, μ) *per ogni* $\lambda, \mu \in \mathbb{R}$*; quindi contiene tutto* $\mathbb{R}^2$*. Perciò,* $U + W = \mathbb{R}^2$*.*

7.2 Sistemi di generatori, lineare indipendenza, basi

Definizione 7.10. *Siano* $v_1, \dots, v_m \in \mathbb{K}^n$ m *vettori. Una* combinazione lineare *di* $v_1, \dots, v_m$ *è un vettore* $v \in \mathbb{K}^n$ *della forma* $v = \alpha_1 v_1 + \cdots + \alpha_m v_m$*, per qualche* $\alpha_1, \dots, \alpha_m \in \mathbb{K}$*.*

Esempio 7.11. *In* $\mathbb{R}^4$*, il vettore* $(7, 1, -3, 5)$ *è combinazione lineare dei tre vettori* $(1, 0, 1, 1)$*,* $(1, 2, -1, 0)$*,* $(2, 1, -2, 1)$*. Infatti:*

$$2(1, 0, 1, 1) + (-1)(1, 2, -1, 0) + 3(2, 1, -2, 1) = (7, 1, -3, 5).$$

Teorema 7.12. *Dati* m *vettori* $v_1, \dots, v_m \in \mathbb{K}^n$*, l'insieme*

$$\{\alpha_1 v_1 + \cdots + \alpha_m v_m \in \mathbb{K}^n \mid \alpha_1, \dots, \alpha_m \in \mathbb{K}\}$$

è un sottospazio vettoriale di $\mathbb{K}^n$*. Viene detto il* sottospazio generato *da* $v_1, \dots, v_m$*, e viene indicato con* $L(v_1, \dots, v_m)$*, o con* $\mathrm{Span}(v_1, \dots, v_m)$*.*

Dimostrazione. Scegliendo $\alpha_1 = \cdots = \alpha_m = 0$, si vede che $\underline{0} \in L(v_1, \ldots, v_m)$. Ora, sia $\alpha \in \mathbb{K}$, e siano $v, w \in L(v_1, \ldots, v_m)$. Scriviamo $v = \lambda_1 v_1 + \cdots + \lambda_m v_m$ e $w = \mu_1 + \cdots + \mu_m v_m$ con $\lambda_i, \mu_i \in \mathbb{K}$. Allora $v + w = (\lambda_1 + \mu_1)v_1 + \cdots + (\lambda_m + \mu_m)v_m \in L(v_1, \ldots, v_m)$. Inoltre, $\alpha v = (\alpha\lambda_1)v_1 + \cdots + (\alpha\lambda_m)v_m \in \langle v_1, \ldots, v_m \rangle$. Quindi $L(v_1, \ldots, v_m)$ è un sottospazio vettoriale di $\mathbb{K}^n$. □

Per convenzione, si pone $L(\emptyset) = \{\underline{0}\}$; cioè, il sottospazio generato da zero vettori è il sottospazio banale.

Esempio 7.13. *Il sottospazio generato da un singolo vettore $v \in \mathbb{K}^n$ è $\{\alpha v \mid \alpha \in \mathbb{K}\}$.*

Esempio 7.14. *In $\mathbb{R}^3$, si consideri i vettori $v_1 = (1, 1, 0)$ e $v_2 = (0, 3, 1)$. Allora*

$$L(v_1, v_2) = \{\lambda(1, 1, 0) + \mu(0, 3, 1) \ : \ \lambda, \mu \in \mathbb{R}\} = \{(\lambda, \lambda + 3\mu, \mu) \ : \ \lambda, \mu \in \mathbb{R}\}.$$

Osservazione 7.15. *Siano $v_1, \ldots, v_m \in \mathbb{K}^n$. Poiché i sottospazi vettoriali sono chiusi rispetto alle combinazioni lineari, allora $L(v_1, \ldots, v_m)$ è il più piccolo sottospazio vettoriale di $\mathbb{K}^n$ che contiene $v_1, \ldots, v_m$. Cioè, se U è un sottospazio di $\mathbb{K}^n$ e $v_1, \ldots, v_m \in U$, allora $L(v_1, \ldots, v_m) \subseteq U$.*

Definizione 7.16. *Sia $V \subseteq \mathbb{K}^n$ uno spazio vettoriale, e siano $v_1, \ldots, v_m \in V$. L'insieme $\{v_1, \ldots, v_m\}$ è detto un* sistema di generatori *per V (e V è* generato *da $v_1, \ldots, v_m$) se $V = L(v_1, \ldots, v_m)$; cioè se*

$$\forall v \in V \ \exists\, \alpha_1, \ldots, \alpha_m \in \mathbb{K} \ : \ \alpha_1 v_1 + \cdots + \alpha_m v_m = v.$$

Esempio 7.17. *In $\mathbb{R}^2$, siano $v_1 = (1, 1)$, $v_2 = (0, 2)$, $v_3 = (1, 0)$. Allora $\{v_1, v_2, v_3\}$ è un sistema di generatori per $\mathbb{R}^2$. Infatti, per ogni vettore $(x, y) \in \mathbb{R}^2$, esistono $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $(x, y) = \alpha(1, 1) + \beta(0, 2) + \gamma(1, 0)$. Ad esempio, basta scegliere $\alpha = y$, $\beta = 0$, $\gamma = x - y$. Un'altra possibile scelta è $\alpha = -y$, $\beta = y$ e $\gamma = x + y$; quindi in questo caso la scelta dei coefficienti α, β, γ non è unica.*

Omettiamo la dimostrazione della seguente proposizione.

Proposizione 7.18. *Siano $v_1, \ldots, v_m$ vettori di uno spazio vettoriale $V \subseteq \mathbb{K}^n$, e sia $w \in V$. Allora $L(v_1, \ldots, v_m) = L(v_1, \ldots, v_m, w)$ se e solo se $w = \lambda_1 v_1 + \cdots + \lambda_m v_m$ per qualche $\lambda_1, \ldots, \lambda_m \in \mathbb{K}$.*

Definizione 7.19. *Siano* $v_1, \dots, v_m \in \mathbb{K}^n$.

I vettori $v_1, \dots, v_m$ *si dicono* linearmente dipendenti *se esistono* $\alpha_1, \dots, \alpha_m \in \mathbb{K}$ *non tutti uguali a zero tale che* $\alpha_1 v_1 + \cdots + \alpha_m v_m = \underline{0}$.

I vettori $v_1, \dots, v_m$ *si dicono* linearmente indipendenti *in caso contrario, cioè quando l'unica scelta di* $\alpha_1, \dots, \alpha_m \in \mathbb{K}$ *per cui vale* $\alpha_1 v_1 + \cdots + \alpha_m v_m = \underline{0}$ *è* $\alpha_1 = \cdots = \alpha_m = 0$.

Si dice anche che l'insieme $\{v_1, \dots, v_m\}$ è linearmente dipendente o indipendente. Per convenzione, si assume che l'insieme vuoto $\emptyset$ è linearmente indipendente.

Esempio 7.20. *In* $\mathbb{R}^3$, *i tre vettori* $v_1 = (1, 2, 3)$, $v_2 = (2, 0, -1)$ *e* $v_3 = (0, -4, -7)$ *sono linearmente dipendenti, perché* $2v_1 - v_2 + v_3 = \underline{0}$.

I due vettori $w_1 = (1, 1, 3)$ *e* $w_2 = (2, 0, 1)$ *sono linearmente indipendenti. Infatti, se* $\alpha, \beta \in \mathbb{R}$ *sono tali che* $\alpha w_1 + \beta w_2 = \underline{0}$, *allora* $(\alpha + 2\beta, \alpha, 3\alpha + \beta) = (0, 0, 0)$, *cioè*

$$\begin{cases} \alpha + 2\beta = 0 \\ \alpha = 0 \\ 3\alpha + \beta = 0, \end{cases}$$

da cui segue $\alpha = 0$ *e* $\beta = 0$.

Proposizione 7.21. *I vettori* $v_1, \dots, v_m \in \mathbb{K}^n$ *sono linearmente dipendenti se e solo se almeno uno di essi è combinazione lineare degli altri.*

Dimostrazione. Supponiamo che uno dei vettori sia combinazione degli altri. Ad esempio, sia v_1 combinazione lineare di $v_2, \dots, v_m$, cioè $v_1 = \alpha_2 v_2 + \cdots + \alpha_m v_m$ con $\alpha_i \in \mathbb{K}$. Allora $1 \cdot v_1 - \alpha_2 v_2 - \cdots - \alpha_m v_m = \underline{0}$, e almeno uno dei coefficienti non è zero (quello di v_1), quindi $v_1, \dots, v_m$ sono linearmente dipendenti.

Viceversa, siano $v_1, \dots, v_m$ linearmente dipendenti, e quindi $\beta_1 v_1 + \cdots + \beta_m v_m = \underline{0}$, con scalari $\beta, , \dots, \beta_m$ non tutti uguali a zero. Assumiamo senza restrizione che sia $\beta_1 \neq 0$. Allora $v_1 = -\frac{\beta_2}{\beta_1} v_2 - \cdots - \frac{\beta_m}{\beta_1} v_m$, e quindi v_1 è combinazione lineare di $v_2, \dots, v_m$. □

Se $w \in L(v_1, \dots, v_m)$, si dice che w è *linearmente dipendente da* $v_1, \dots, v_m$.

Osservazione 7.22. *Un singolo vettore* v *è linearmente indipendente se e solo se* $v \neq \underline{0}$.

Due vettori v, w *sono linearmente indipendenti se e solo se non sono uno multiplo dell'altro.*

Un insieme di vettori che contiene il vettore nullo è linearmente dipendente.

Definizione 7.23. *Sia $V \subseteq \mathbb{K}^n$ uno spazio vettoriale, e siano $v_1, \dots, v_m \in V$. L'insieme $\{v_1, \dots, v_m\}$ si dice una* base *di V se:*

- *$\{v_1, \dots, v_m\}$ è un sistema di generatori per V;*
- *$\{v_1, \dots, v_m\}$ è linearmente indipendente.*

Per convenzione, una base del sottospazio banale $\{\underline{0}\}$ è l'insieme vuoto $\emptyset$.

Osservazione 7.24. *Sia $V = \mathbb{K}^n$. Per ogni $i = 1, \dots, n$, sia $e_i := (0, \dots, 0, \underbrace{1}_{pos.\ i}, 0 \dots, 0)$ il vettore di $\mathbb{K}^n$ che ha un 1 in i-esima posizione e 0 altrove. Allora $\{e_1, \dots, e_n\}$ è una base di $\mathbb{K}^n$, detta* base canonica. *Ad esempio, la base canonica di $\mathbb{R}^3$ è $\{(1,0,0), (0,1,0), (0,0,1)\}$.*

Esempio 7.25. *Sia $V = \mathbb{R}^2$, e sia $B = \{v_1, v_2\}$ con $v_1 = (1,2)$, $v_2 = (-1,-1)$. Allora B è un sistema di generatori per $\mathbb{R}^2$; infatti, per ogni $(x,y) \in \mathbb{R}^2$ vale $(x,y) = (-x+y)(1,2) + (-2x+y)(-1,-1)$. Inoltre B è linearmente indipendente, essendo composto da due vettori non nulli e non proporzionali. Quindi B è una base di $\mathbb{R}^2$.*

Esempio 7.26. *Sia $V \subseteq \mathbb{R}^2$, $V = L(u,v,w)$, con $u = (1,0)$, $v = (2,1)$, $w = (0,-1)$. Allora $\{u,v,w\}$ è un sistema di generatori per V. Ora, $\{u,v,w\}$ è linearmente dipendente, perché $w = 2u - v$. Perciò $L(u,v,w) = L(u,v)$. Quindi anche $\{u,v\}$ è un sistema di generatori per V. Inoltre $\{u,v\}$ è linearmente indipendente. Quindi $\{u,v\}$ è una base di V.*

Esempio 7.27. *In $\mathbb{R}^3$, consideriamo il sottosazio vettoriale $V = \{(x,y,z) \mid x - y + 2z = 0\}$. Esplicitiamo $x = y - 2z$. Allora $V = \{(\alpha - 2\beta, \alpha, \beta) \mid \alpha, \beta \in \mathbb{R}\}$. Poichè $(\alpha - 2\beta, \alpha, \beta) = \alpha(1,1,0) + \beta(-2,0,1)$, allora $V = L((1,1,0), (-2,0,1))$. Infine, si vede immediatamente che $\{(1,1,0), (-2,0,1)\}$ è una base di V.*

Enunciamo senza dimostrazione il seguente importante risultato.

Teorema 7.28. *Tutte le basi di uno stesso spazio vettoriale hanno lo stesso numero di elementi.*

Definizione 7.29. *Sia V uno spazio vettoriale. Si dice* dimensione *di V, e si indica con $\dim V$, il numero di elementi di una qualsiasi sua base.*

Esempio 7.30. *La dimensione di $\mathbb{K}^n$ è n. Infatti la base canonica di $\mathbb{K}^n$ ha n vettori.*

Proposizione 7.31. *Sia V uno spazio vettoriale con $\dim V = n$.*

- *Sia S è un sistema di generatori per V. Allora $|S| \geq n$; inoltre, S è una base per V se e solo se $|S| = n$.*

- *Sia S un insieme di vettori di V linearmente indipendenti. Allora $|S| \leq n$; inoltre, S è una base per V se e solo se $|S| = n$.*

Teorema 7.32. (Estrazione di una base) *Sia V uno spazio vettoriale e $\{v_1, \ldots, v_m\}$ un suo sistema di generatori. Allora esiste una base di V contenuta in $\{v_1, \ldots, v_m\}$.*

Dimostrazione. Se $\{v_1, \ldots, v_m\}$ è linearmente indipendente, allora è una base di V. Altrimenti, esiste un vettore tra essi che è combinazione lineare degli altri. Supponiamo sia v_m; allora $L(v_1, \ldots, v_{m-1}) = L(v_1, \ldots, v_m) = V$. Procediamo alla stessa maniera su $\{v_1, \ldots, v_{m-1}\}$: se è linearmente indipendente, allora è una base di V, altrimenti uno di essi è combinazione lineare degli altri e possiamo scartarlo. Dopo un numero finito di passi, questo procedimento termina e abbiamo trovato una base di V. □

Teorema 7.33. (Completamento a una base) *Sia V uno spazio vettoriale di dimensione n, e $\{v_1, \ldots, v_m\} \subseteq V$ un insieme di vettori linearmente indipendenti. Allora esistono $n - m$ vettori $w_1, \ldots, w_{n-m} \in V$ tali che $\{v_1, \ldots, v_m, w_1, \ldots, w_{m-n}\}$ è una base di V.*

Inoltre, se B è una qualsiasi base di V, allora $w_1, \ldots, w_{n-m}$ posso essere presi da B.

Dimostrazione. Sia $B = \{u_1, \ldots, u_n\}$. Se $u_1 \in L(v_1, \ldots, v_m)$ allora $L(v_1, \ldots, v_m) = L(v_1, \ldots, v_m, u_1)$, altrimenti lo aggiungiamo e otteniamo un insieme $\{v_1, \ldots, v_m, u_1\}$ di vettori linearmente indipendenti. In questo modo, scorriamo tutti i vettori di B e, se non sono combinazioni lineari dei precedenti vettori, li aggiungiamo ad essi. Alla fine abbiamo costruito un insieme di vettori linearmente indipendenti la cui chiusura lineare contiene B, e quindi contiene V, e quindi genera V. In sintesi, abbiamo ottenuto una base di V. □

La dimensione dei sottospazi vettoriali soddisfa la seguente proprietà.

Proposizione 7.34. *Sia V uno spazio vettoriale di dimensione n, e sia W un sottospazio vettoriale di V. Allora* $\dim W \leq n$.

Inoltre, $\dim W = 0$ *se e solo se $W = \{\underline{0}\}$; e* $\dim W = n$ *se e solo $W = V$.*

Le basi di uno spazio vettoriale sono caratterizzate dal fatto di poter definire le *componenti* rispetto ad essa di ogni vettore dello spazio vettoriale.

Teorema 7.35. *Sia V uno spazio vettoriale e $B = \{v_1, \dots, v_n\} \subseteq V$. Allora B è una base di V se e solo se ogni vettore di V si scrive in maniera unica come combinazione lineare dei vettori di B, cioè*

$$\forall v \in V \; \exists! \, \alpha_1, \dots, \alpha_n \in \mathbb{K} : \quad v = \alpha_1 v_1 + \cdots + \alpha_n v_n.$$

Dimostrazione. L'esistenza per ogni $v \in V$ di $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ come sopra equivale a chiedere che B sia un sistema di generatori. L'unicità di tali $\alpha_1, \dots, \alpha_n$ equivale a chiedere che B sia linearmente indipendente. □

Definizione 7.36. *Se $B = \{v_1, \dots, v_n\}$ è una base di V e $v \in V$ si scrive come $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$, allora $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ è detta la n-upla delle* componenti *di v rispetto a B, e si indica con $v \equiv_B (\alpha_1, \dots, \alpha_n)$.*

Esempio 7.37. *Consideriamo la base $B = \{v_1 = (1, 2), v_2 = (2, -1)\}$ di $\mathbb{R}^2$, e troviamo le componenti di $v = (-1, 8)$ rispetto a B.*

Scriviamo $(-1, 8) = \alpha(1, 2) + \beta(2, -1)$ e svolgiamo i calcoli. Otteniamo $(-1, 8) = (\alpha + 2\beta, 2\alpha - \beta)$, cioè

$$\begin{cases} -1 = \alpha + 2\beta \\ 8 = 2\alpha - \beta \end{cases}$$

da cui l'unica soluzione $\alpha = 3$, $\beta = -2$. Quindi $v \equiv_B (3, -2)$.

7.3 Prodotto scalare standard in $\mathbb{R}^n$

In questa sezione il campo considerato è sempre $\mathbb{R}$.

Definizione 7.38. *Il* prodotto scalare *(standard) in $\mathbb{R}^n$ è la funzione $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ definita come segue: per ogni $\underline{x} = (x_1, \dots, x_n), \underline{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$,*

$$\langle \underline{x}, \underline{y} \rangle := \sum_{i=1}^{n} x_i y_i$$

La norma *(o* modulo*) è la funzione $|| \cdot || : \mathbb{R}^n \to \mathbb{R}$ definita per $\underline{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ da*

$$||\underline{x}|| := \sqrt{\langle \underline{x}, \underline{x} \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2} \geq 0.$$

Un vettore $\underline{x} \in \mathbb{R}^n$ si dice un versore *se $||\underline{x}|| = 1$.*

Due vettori $\underline{x}, \underline{y} \in \mathbb{R}^n$ si dicono ortogonali *(e si indica con $\underline{x} \perp \underline{y}$) se $\langle \underline{x}, \underline{y} \rangle = 0$.*

Esempio 7.39. *In* $\mathbb{R}^4$*, si ha* $\langle (1,0,1,2),(-1,2,0,2)\rangle = 1\cdot(-1)+0\cdot 2+1\cdot 0+2\cdot 2 = 3$*. La norma di* $(1,0,1,2)$ *è* $||(1,0,1,2)|| = \sqrt{1^2+0^2+1^2+2^2} = \sqrt{6}$*.*

Proposizione 7.40. *Il prodotto scalare in* $\mathbb{R}^n$ *gode delle seguenti proprietà.*

- ($\langle\cdot,\cdot\rangle$ è bilineare) *Per ogni* $u,v,w \in \mathbb{R}^n$ *e per ogni* $\lambda \in \mathbb{R}$*, si ha*

$$\langle u+v,w\rangle = \langle u,w\rangle + \langle v,w\rangle, \qquad \langle \lambda u, v\rangle = \lambda\langle u,v\rangle,$$

$$\langle u, v+w\rangle = \langle u,v\rangle + \langle u,w\rangle, \qquad \langle u, \lambda v\rangle = \lambda\langle u,v\rangle.$$

- ($\langle\cdot,\cdot,\rangle$ è simmetrico) *Per ogni* $u,v \in \mathbb{R}^n$*, si ha* $\langle u,v\rangle = \langle v,u\rangle$*.*

- ($\langle\cdot,\cdot\rangle$ è definito positivo) *Per ogni* $u \in \mathbb{R}^n$ *si ha* $\langle u,u\rangle \geq 0$*, e* $\langle u,u\rangle = 0 \iff u = \underline{0}$*.*

Dimostrazione. Lasciata per esercizio. □

Si noti che $\langle v, \underline{0}\rangle = \langle \underline{0}, v\rangle = 0$ per ogni $v \in \mathbb{R}^n$, cioè $\underline{0}$ è ortogonale a tutti i vettori di $\mathbb{R}^n$.

Proposizione 7.41. *Per ogni* $u,v \in \mathbb{R}^n$ *e per ogni* $\lambda \in \mathbb{R}$ *valgono le seguenti proprietà.*

- $||u|| \geq 0$*; inoltre,* $||u|| = 0 \iff u = \underline{0}$*.*

- $||\lambda u|| = |\lambda| \cdot ||u||$*.*

- $|\langle u,v\rangle| \leq ||u||\cdot||v||$ (disuguaglianza di Schwarz)*.*

- $||u+v|| \leq ||u|| + ||v||$ (disuguaglianza di Minkowski)*.*

Dimostrazione. La dimostrazione delle prime due proprietà è lasciata per esercizio.

Per la disuguaglianza di Schwarz, notiamo che la tesi è vera se $u = \underline{0}$ o $v = \underline{0}$; possiamo quindi assumere che u e v non sono nulli. Poichè $\langle u+xv,\rangle \geq 0$ per ogni $x \in \mathbb{R}$, e sviluppando il primo membro con la bilinearità e la simmetria, otteniamo $||v||^2x^2 + 2\langle u,v\rangle x + ||u||^2 \geq 0$ per ogni $x \in \mathbb{R}$. Perciò il discriminante Δ soddisfa $\Delta/4 \leq 0$, cioè $\langle u,v\rangle^2 - ||v||\cdot||u|| \leq 0$, da cui la tesi.

Per la disuguaglianza di Minkowski, osserviamo che usando Schwarz si ha

$$||u+v||^2 = ||u||^2 + ||v||^2 + 2\langle u,v\rangle \leq ||u||^2 + ||v||^2 + 2||u||\cdot||v|| = (||u|| + ||v||)^2,$$

da cui $||u+v|| \leq ||u|| + ||v||$. □

Definizione 7.42. *Gli* angoli *tra due vettori $u, v \in \mathbb{R}^n$ sono θ e $2\pi - \theta$, dove θ è l'unico numero reale in $[0, \pi]$ tale che $\langle u, v\rangle = ||u|| \cdot ||v|| \cdot \cos\theta$, cioè*

$$\theta = \arccos\left(\frac{\langle u, v\rangle}{||u|| \cdot ||v||}\right)$$

Proposizione 7.43. *Sia $U = L(\underline{v}_1, \ldots, \underline{v}_m)$ un sottospazio vettoriale di $\mathbb{R}^n$. Indichiamo con $U^\perp \subseteq \mathbb{R}^n$ l'insieme dei vettori di $\mathbb{R}^n$ che sono ortogonali a tutti i vettori di U. Allora $U^\perp$ è un sottospazio vettoriale di $\mathbb{R}^n$, detto il* complemento ortogonale *di U.*

Se $\underline{v}_1 = (\alpha_{11}, \ldots, \alpha_{1n}), \ldots, \underline{v}_m = (\alpha_{m1}, \ldots, \alpha_{mn})$, allora

$$U^\perp = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n = 0, \ldots\ldots, \alpha_{m1}x_1 + \cdots + \alpha_{mn}x_n = 0\}.$$

Inoltre, $\dim U^\perp = n - \dim U$.

Esempio 7.44. *Sia $v = (2, 1, 3) \in \mathbb{R}^3$ e $U = L(v)$.*

Allora $U^\perp = \{(x, y, z) \in \mathbb{R}^3 \mid 2x + y + 3z = 0\}$ e $\dim U^\perp = 3 - 1 = 2$.

Definizione 7.45. *Un insieme di vettori $\{v_1, \ldots, v_m\} \subseteq \mathbb{R}^n$ si dice* ortonormale *se ogni suo vettore ha norma 1 e ogni due suoi vettori distinti sono ortogonali, e quindi se:*

$$\langle v_i, v_j\rangle = \begin{cases} 0 & \text{se } i \neq j, \\ 1 & \text{se } i = j. \end{cases}$$

7.4 Esercizi

Esercizio 7.1. *Dimostrare che i vettori $v_1 = (1, 2)$ e $v_2 = (5, 1)$ formano una base di $\mathbb{R}^2$. Trovare inoltre le componenti di $v_3 = (11, 4)$ rispetto a questa base.*

Svolgimento. Supponiamo che $\lambda_1 v_1 + \lambda_2 v_2 = (0, 0)$, quindi

$$\lambda_1(1, 2) + \lambda_2(5, 1) = (0, 0),$$

$$(\lambda_1 + 5\lambda_2, 2\lambda_1 + \lambda_2) = (0, 0).$$

Si ha quindi il sistema

$$\begin{cases} \lambda_1 + 5\lambda_2 = 0 \\ 2\lambda_1 + \lambda_2 = 0 \end{cases} \longrightarrow \begin{cases} \lambda_1 = -5\lambda_2 \\ 2(-5\lambda_2) + \lambda_2 = 0 \end{cases} \longrightarrow \lambda_1 = \lambda_2 = 0.$$

Questo dimostra che i vettori sono linearmente indipendenti. Mostriamo ora che sono un sistema di generatori. Sia (x, y) un generico vettore di $\mathbb{R}^2$, vogliamo verificare che è possibile scrivere (x, y) come combinazione lineare di $v_1 = (1, 2)$ e $v_2 = (5, 1)$. Cioè

$$\lambda_1 v_1 + \lambda_2 v_2 = (x, y).$$

Quindi

$$\lambda_1(1, 2) + \lambda_2(5, 1) = (x, y),$$

risolvendo si ha che $\lambda_1 = \frac{5y-x}{9}$ e $\lambda_2 = \frac{2x-y}{9}$.
Per i trovare le componenti di v_3 rispetto alla base costituita dai vettori $v_1 = (1, 2)$ e $v_2 = (5, 1)$ basterà sostituire $x = 11$ e $y = 4$, così

$$\begin{cases} \lambda_1 = \frac{20-11}{9} = 1 \\ \lambda_2 = \frac{22-4}{9} = 2 \end{cases} \longrightarrow 1(1, 2) + 2(5, 1) = (11, 4) \longrightarrow 1v_1 + 2v_2 = v_3.$$

Le componenti sono quindi $(1, 2)$.

Esercizio 7.2. *Dopo aver verificato che i vettori $v_1 = (1, 2, 3)$ e $V_2 = (2, 0, 3)$ sono linearmente indipendenti, completare l'insieme $\{v_1, v_2\}$ in modo da ottenere una base di $\mathbb{R}^3$.*

Svolgimento. Per la lineare indipendenza possiamo osservare che i due vettori non sono proporzionali. Altrimenti si può procedere con la definizione risolvendo

$$\lambda_1 v_1 + \lambda_2 v_2 = \mathbf{0} = (0, 0, 0),$$

e mostrando che l'unica soluzione è $\lambda_1 = \lambda_2 = 0$.
Per ottenere una base mi occorre un vettore v_3 tale che $v_3 \notin L(v_1, v_2)$. Un vettore che soddisfa tale condizione è $v_3 = (0, 0, 1)$. Infatti si verifica facilmente che i tre vettori sono linearmente indipendenti.

Esercizio 7.3. *Determinare la dimensione del sottospazio di $\mathbb{R}^5$ generato dalla quaterna di vettori $v_1 = (1, 2, -1, 1, 1), v_2 = (1, 2, -1, 0, 0), v_3 = (0, 0, -1, 1, 0)$ e $v_4 = (3, 6, -3, 3, 3)$.*

Svolgimento. Se i vettori fossero linearmente indipendenti costituirebbero una base del sottospazio (dato che sono dei generatori per ipotesi), e il sottospazio avrebbe quindi dimensione 4. Osservando i vettori possiamo però notare che $v_4 = 3v_1$, quindi inziamo

escludendo v_4 e cerchiamo di capire se i restanti vettori sono linearmente indipendenti. Supponiamo che $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \mathbf{0} = (0,0,0,0,0)$, cioè

$$\lambda_1 \begin{pmatrix} 1 \\ 2 \\ -1 \\ 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Si ha quindi il sistema

$$\begin{cases} \lambda_1 + \lambda_2 = 0 \\ 2\lambda_1 + 2\lambda_2 = 0 \\ -\lambda_1 - \lambda_2 - \lambda_3 = 0 \\ \lambda_1 + \lambda_3 = 0 \\ \lambda_1 = 0 \end{cases} \longrightarrow \lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = 0.$$

Poichè i vettori v_1, v_2, v_3 sono quindi linearmente indipendenti e il sottospazio ha dimensione 3.

Esercizio 7.4. *Stabilire se* $\{W = (x,y) \in \mathbb{R}^2 | x \leq 0, y \geq 0\}$ *è un sottospazio vettoriale di* $\mathbb{R}^2$.

Svolgimento. Osserviamo dapprima che $(0,0) \in W$ in quanto verifica le condizioni richieste dall'insieme. Siano $v = (x,y)$ e $v' = (x',y') \in W$. Quindi $x \leq 0, x' \leq 0$ e $y \geq 0, y' \geq 0$. Sia $\lambda \geq 0$. Il vettore $v + \lambda v' = (x + x', \lambda(y + y'))$ è ancora in W visto che $x + x' \leq 0$ e $\lambda(y+y') \geq 0$. Ma se $\lambda \leq 0$ il vettore $v + \lambda v' = (x + x', \lambda(y + y')) \notin W$ visto che $\lambda(y + y') \leq 0$. Quindi W non è un sottospazio vettoriale pochè non è vero che $\forall \lambda \in \mathbb{R} : v + \lambda v' \in W$.

Esercizio 7.5. *Stabilire quali dei seguenti sottoinsiemi sono sottospazi vettoriali e, in caso affermativo, determinarne una base e la dimensione:*

- $W_1 = \{(1,0,-1,-1), (1,0,1,1), (0,1,1,0), (2,0,0,1)\} \subseteq \mathbb{R}^4$;
- $W_2 = L((5,0,-3,1), (0,2,3,1), (4,1,0,0)) \subseteq \mathbb{R}^4$;
- $W_3 = L((0,0,0), (1,1,1), (2,2,2)) \subseteq \mathbb{R}^3$;
- $W_4 = L((0,0), (-1,1), (5,-5)) \subseteq \mathbb{R}^2$;
- $W_5 = \{(x_1,x_2,x_3,x_4,x_5) : x_1 - x_2 - x_3 = x_5 = 0\} \subseteq \mathbb{R}^5$;
- $W_6 = \{(x_1,x_2,x_3,x_4) : x_1^2 - x_3 = 0\} \subseteq \mathbb{R}^4$;

- $W_7 = \{(x_1, x_2, x_3, x_4, x_5) : x_1 + x_2 - x_3 = x_4 - 3x_5 = 0\} \subseteq \mathbb{R}^5$;
- $W_8 = \{(x_1, x_2, x_3, x_4) : x_1 - x_2 = 0;\ x_3 + x_4 = -1\} \subseteq \mathbb{R}^4$;
- $W_9 = \{(x_1, x_2, x_3, x_4) : x_1 = 2x_2 - x_3; x_4 = x_5 = 0\} \subseteq \mathbb{R}^4$;
- $W_{10} = \{(x_1, x_2, x_3, x_4) : x_1^2 = x_2; x_3 + x_4 = 0\} \subseteq \mathbb{R}^4$.

Esercizio 7.6. *In $\mathbb{R}^3$, per ciascuno dei seguenti sistemi di vettori:*
(a) $S_1 = \{(1,0,1), (0,-1,0), (0,1,1), (0,2,-2)\}$;
(b) $S_2 = \{(1,0,2), (0,1,-1), (0,1,-1)\}$,
(c) $S_3 = \{(0,1,1), (-1,1,1)\}$;
(d) $S_4 = \{(2,2,2), (1,1,1)\}$,
(e) $S_5 = \{(2,-2,1), (4,4,1), (0,0,1), (1,1,-1)\}$.
stabilire, giustificando le risposte,

i) se è linearmente dipendente o indipendente;

ii) se è un sistema di generatori di $\mathbb{R}^3$;

iii) se è una base di $\mathbb{R}^3$;

iv) se è possibile completarlo ad una base di $\mathbb{R}^3$ e, in caso affermativo, esibirne una.

Esercizio 7.7. *Determinare la dimensione e una base dei seguenti sottospazi vettoriali di $\mathbb{R}^4$:*

(1) $W_1 = \{(x, y, z, t) : t = 2x + y, z = 2x, x, y \in \mathbb{R}\}$

(2) $W_2 = \{(0, -y, y + t, t) : y, t \in \mathbb{R}\}$

(3) $W_3 = \{(a - b, b, a - b, 0) : a, b \in \mathbb{R}\}$.

(4) $W_4 = \{(a + c, b - c, 3a + 2b + c, 0) : a, b, c \in \mathbb{R}\}$.

Esercizio 7.8. *Completare, se possibile, ad una base di tutto lo spazio $\mathbb{K}^n$ i seguenti sottoinsiemi:*

$$X_1 = \{(3,1,0), (0,2,1)\} \subseteq \mathbb{R}^3$$
$$X_2 = \{(-1,0,1,0), (0,1,0,2), (0,1,1,-1)\} \subseteq \mathbb{R}^4$$
$$X_3 = \{(1,0,-1,0,0), (0,1,0,2,0), (1,0,0,0,3)\} \subset \mathbb{R}^5$$

Esercizio 7.9. *Dati i vettori* $\underline{x} = (1, a, 1)$ *e* $\underline{y} = (a, 1, 1)$ *di* $\mathbb{R}^3$ *dipendenti dal parametro reale* a*, stabilire per quali valori di* $a \in \mathbb{R}$ $\underline{x}$ *e* $\underline{y}$ *sono linearmente dipendenti, e per quali valori di* $a \in \mathbb{R}$ $\underline{x}$ *e* $\underline{y}$ *sono linearmente indipendenti.*

Esercizio 7.10. *Sia* $k \in \mathbb{R}$ *e siano* $\underline{x} = (1, -1, k), \underline{y} = (1, 0, -1) \in \mathbb{R}^3$*. Calcolare* $\langle \underline{x}, \underline{y} \rangle$*,* $||\underline{x}||$*,* $||\underline{y}||$*. Stabilire per quali valori di* $k \in \mathbb{R}$ $\underline{x}$ *è un versore, e per quali* $k \in \mathbb{R}$ *i vettori* $\underline{x}$ *e* $\underline{y}$ *sono ortogonali.*

Esercizio 7.11. *In* $\mathbb{R}^4$*, considerare i vettori* $u = (0, 1, 1, 2)$*,* $v = (2, 0, 0, 1)$*,* $w = (0, 1, 0, -1)$*,* $z = (2, 1, 1, 3)$*.*

- *Determinare un vettore linearmente dipendente da* u, v *e non proporzionale a nessuno dei due.*
- *Determinare un vettore non nullo ortogonale a* u *e* w*.*
- *Determinare un vettore linearmente indipendente da* u, v, w*.*
- *Deeterminare un vettore linearmente dipendente da* u, v*, e indipendente da* z*.*

Capitolo 8

Matrici

8.1 Matrici e operazioni

Definizione 8.1. *Una matrice A di tipo $m \times n$ a elementi in un campo $\mathbb{K}$ è una tabella con m righe ed n colonne di scalari in $\mathbb{K}$ del tipo*

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

L'elemento nella riga i e colonna j è detto elemento (o entrata) di posto (i, j)*, ed è indicato con a_{ij}, o con a^i_j, o con $(A)^i_j$. Indichiamo brevemente A con $A = (a_{ij})$.*

Indichiamo con A^i la riga i-esima di A ($i = 1, \ldots, m$), e con A_j la colonna j-esima di A ($j = 1, \ldots, n$). Identifichiamo A^i con il vettore $(a_{i1}, \ldots, a_{in})$ di $\mathbb{K}^n$, e A_j con il vettore $(a_{1j}, \ldots, a_{mj})$ di $\mathbb{K}^m$.

L'insieme di tutte le matrici $m \times n$ a entrate in $\mathbb{K}$ è indicato con $\mathbb{K}^{m \times n}$, o con $\mathcal{M}_{m \times n}(\mathbb{K})$.

Una matrice in $\mathbb{K}^{m \times n}$ si dice quadrata *se $n = m$.*

Esempio 8.2. *Le seguenti matrici sono matrici reali, cioè sul campo $\mathbb{K} = \mathbb{R}$.*

$$\begin{pmatrix} 2 & -1 & 0 & 3 \\ -1 & 0 & 1 & -1 \\ 4 & 10 & 0 & 0 \end{pmatrix} \in \mathcal{M}_{3\times 4}(\mathbb{R}), \begin{pmatrix} \sqrt{2} & -1 & e \\ 5^{\sqrt{2}} & 0 & \pi \\ 4^3 & 10 & \sin 3 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{R}).$$

Esempio 8.3. *Le seguenti matrici sono matrici complesse, cioè sul campo* $\mathbb{K} = \mathbb{C}$.

$$\begin{pmatrix} \sqrt{-1} & 0 & 3 \\ 0 & 1 & -1 \end{pmatrix} \in \mathcal{M}_{2\times 3}(\mathbb{C}), \quad \begin{pmatrix} 2+3i & -1 & 0 \\ 7 & 1 & 4 \\ 0 & 10 & \tan(\pi/3) \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{C}).$$

Definizione 8.4. *Siano* $A, B \in \mathbb{K}^{m\times n}$ *due matrici. La* somma $A + B$ *è definita da*

$$C = A + B \in \mathbb{K}^{m\times n}, \qquad C = (c_{ij}), \quad c_{ij} = a_{ij} + b_{ij}.$$

Esempio 8.5. *Si ha che*

$$\begin{pmatrix} 2 & -1 & 0 & 3 \\ -1 & 0 & 1 & -1 \\ 4 & 10 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & -3 \\ 1 & 1 & 4 & 2 \\ 3 & -2 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 5 & 1 \\ 7 & 8 & 1 & 1 \end{pmatrix}.$$

La somma di due matrici è definita solamente se tali matrici hanno le stesse dimensioni.

Proposizione 8.6. *La somma in* $\mathcal{M}_{m\times n}(\mathbb{K})$ *è una operazione binaria interna tra matrici che gode delle seguenti proprietà*

1. $A + B = B + A \qquad \forall A, B \in \mathcal{M}_{m\times n}(\mathbb{K})$.
2. $A + (B + C) = (A + B) + C \qquad \forall A, B, C \in \mathcal{M}_{m\times n}(\mathbb{K})$.
3. $\exists \underline{0}_{m\times n} \in \mathcal{M}_{m\times n}(\mathbb{K})$ *tale che* $A + \underline{0}_{m\times n} = \underline{0}_{m\times n} + A = A \qquad \forall A \in \mathcal{M}_{m\times n}(\mathbb{K})$.
4. $\forall A \in \mathcal{M}_{m\times n}(\mathbb{K})\ \exists (-A) \in \mathcal{M}_{m\times n}(\mathbb{K})$ *tale che* $A + (-A) = (-A) + A = \underline{0}_{m\times n}$.

Pertanto $(\mathcal{M}_{m\times n}(\mathbb{K}), +)$ *è un gruppo commutativo.*

Dimostrazione.

1. La componente di posto (i, j) è $a_{ij} + b_{ij}$ in $A + B$, ed è $b_{ij} + a_{ij}$ in $B + A$. Questi due valori coincidono perché la somma in $\mathbb{K}$ è commutativa.
2. La componente di posto (i, j) in $A + (B + C)$ è $a_{ij} + (b_{ij} + c_{ij})$, in $(A + B) + C$ è $(a_{ij} + b_{ij}) + c_{ij}$. Questi due valori coincidono perché la somma in $\mathbb{K}$ è associativa.
3. Sia $\overline{0}_{m\times n}$ la matrice nulla, con tutti gli elementi uguali a zero. Allora $\overline{0}_{m\times n}$ è l'elemento neutro rispetto alla somma, dato che la componente di posto (i, j) in $A + \underline{0}_{m\times n} = \underline{0}_{m\times n} + A$ è $a_{ij} + 0 = 0 + a_{ij} = a_{ij}$ ed è uguale alla componente di posto (i, j) in A.
4. La matrice $-A$ che ha per componente di posto (i, j) il valore $-a_{ij}$ è la matrice inversa di A rispetto alla somma.

□

Definizione 8.7. *Sia $A \in \mathbb{K}^{m\times n}$ e $\lambda \in \mathbb{K}$. Il* prodotto per uno scalare λA *è definito da*

$$C = \lambda A \in \mathcal{M}_{m\times n}(\mathbb{K}), \qquad C = (c_{ij}), \quad c_{ij} = \lambda a_{ij}.$$

Esempio 8.8. *Si ha che*

$$7\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 5 & 1 \\ 7 & 8 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 14 & 0 & 0 & 0 \\ 0 & 7 & 35 & 7 \\ 49 & 56 & 7 & 7 \end{pmatrix}.$$

Proposizione 8.9. *Il prodotto per uno scalare gode delle seguenti proprietà.*

1. $\lambda(A+B) = \lambda A + \lambda B \qquad \forall A, B \in \mathbb{K}^{m\times n}, \forall \lambda \in \mathbb{K}.$
2. $(\lambda+\mu)A = \lambda A + \mu A \qquad \forall A \in \mathbb{K}^{m\times n}, \forall \lambda, \mu \in \mathbb{K}.$
3. $\lambda(\mu A) = (\lambda\mu)A \qquad \forall A \in \mathbb{K}^{m\times n}, \forall \lambda, \mu \in \mathbb{K}.$
4. $1A = A \qquad \forall A \in \mathbb{K}^{m\times n}.$
5. *Se* $\lambda A = \underline{0}_{m\times n}$ *allora* $\lambda = 0$ *oppure* $A = \underline{0}_{m\times n}$.

Dimostrazione.

1. La componente di posto (i,j) è $\lambda(a_{ij}+b_{ij})$ in $\lambda(A+B)$, è $\lambda a_{ij} + \lambda b_{ij}$ in $\lambda A + \lambda B$. I due valori coincidono per la proprietà distributiva in $\mathbb{K}$.
2. La componente di posto (i,j) è $(\lambda+\mu)a_{ij}$ in $(\lambda+\mu)A$, è $\lambda a_{ij} + \mu a_{ij}$ in $\lambda A + \mu A$. I due valori coincidono per la proprietà distributiva in $\mathbb{K}$.
3. La componente $\lambda(\mu a_{ij})$ di posto (i,j) in $\lambda(\mu A)$ e la componente $(\lambda\mu)a_{ij}$ di posto (i,j) $(\lambda\mu)A$ coincidono per la proprietà associativa della moltiplicazione in $\mathbb{K}$.
4. La componente di posto (i,j) della matrice $1A$ è $1a_{ij} = a_{ij}$.
5. Se $\lambda A = \underline{0}_{m\times n}$ allora per ogni posto (i,j) si ha che $\lambda a_{ij} = 0$. Dunque se $\lambda \neq 0$ si ha $a_{ij} = 0$ per ogni (i,j), per la legge di annullamento del prodotto in $\mathbb{K}$.

□

Definizione 8.10. *Sia $A \in \mathcal{M}_{m\times n}(\mathbb{R})$ una matrice. La* matrice trasposta *di A è*

$$A^T \in \mathcal{M}_{m\times n}(\mathbb{K}), \qquad A^T = (a_{ij}^T), \quad a_{ij}^T = a_{ji}.$$

Esempio 8.11. *Si ha che*

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 5 & 1 \\ 7 & 8 & 1 & 1 \end{pmatrix}^T = \begin{pmatrix} 2 & 0 & 7 \\ 0 & 1 & 8 \\ 0 & 5 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{4\times 3}(\mathbb{R}).$$

Proposizione 8.12. *La trasposta di una matrice gode delle seguenti proprietà.*

1. $(A^T)^T = A \qquad \forall A \in \mathcal{M}_{m\times n}(\mathbb{K})$.
2. $(\lambda A)^T = \lambda A^T \qquad \forall A \in \mathcal{M}_{m\times n}(\mathbb{K}),\ \forall \lambda \in \mathbb{K}$.
3. $(A+B)^T = A^T + B^T \qquad \forall A, B \in \mathcal{M}_{m\times n}(\mathbb{K})$.

Dimostrazione.

1. La componente di posto (i,j) della matrice $(A^T)^T$ è chiaramente a_{ij}.
2. La componente di posto (i,j) è λa_{ji} sia in $(\lambda A)^T$ che in λA^T.
3. La componente di posto (i,j) è $a_{ji} + b_{ji}$ sia in $(A+B)^T$ che in $A^T + B^T$.

□

Le matrici simmetriche sono una particolare sottoclasse delle matrici quadrate.

Definizione 8.13. *Una matrice $A \in \mathcal{M}_{n\times n}(\mathbb{K})$ si dice* simmetrica *se $A^T = A$.*

Esempio 8.14. *Le seguenti sono matrici simmetriche.*

$$\begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 3 & 5 & 1 & 1 \\ 0 & 8 & 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} -2 & 1 & 3 \\ 1 & 4 & 7 \\ 3 & 7 & -5 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 3 \\ 3 & -1 \end{pmatrix}.$$

Definizione 8.15. *Siano $A \in \mathbb{K}^{m\times n}$ e $B \in \mathbb{K}^{n\times r}$. Il* prodotto *$A \cdot B$ è definito da*

$$C = A \cdot B \in \mathbb{K}^{m\times r}, \qquad C = (c_{ij}), \quad c_{ij} = \sum_{h=1}^{n} a_{ih} b_{hj}.$$

Esempio 8.16. *Date le seguenti matrici A e B*

$$A = \begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 3 & 5 & 1 & 1 \end{pmatrix} \in \mathbb{R}^{3\times 4}, \qquad B = \begin{pmatrix} -2 & 1 & 3 \\ 0 & 4 & 7 \\ 3 & -3 & 1 \\ 2 & 1 & 4 \end{pmatrix} \in \mathbb{R}^{4\times 3},$$

si ha

$$A \cdot B = \begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 3 & 5 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 & 3 \\ 0 & 4 & 7 \\ 3 & -3 & 1 \\ 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & -7 & 9 \\ 31 & -3 & 44 \\ -1 & 21 & 49 \end{pmatrix} \in \mathbb{R}^{3\times 3},$$

$$B \cdot A = \begin{pmatrix} -2 & 1 & 3 \\ 0 & 4 & 7 \\ 3 & -3 & 1 \\ 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 3 & 5 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 16 & 2 & 11 \\ 21 & 39 & 27 & 39 \\ 9 & 2 & -5 & -23 \\ 16 & 21 & 15 & 12 \end{pmatrix} \in \mathbb{R}^{4\times 4}.$$

Si noti come in generale se è possibile moltiplicare due matrici AB non è detto che sia possibile calcolare BA; anche quando questo sia possibile, e A e B siano matrici quadrate della stessa dimensione, non è detto che $AB = BA$.

Esempio 8.17.

$$\begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 & 0 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ 13 & 2 \end{pmatrix} \neq \begin{pmatrix} 8 & -4 \\ 8 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix}.$$

Definizione 8.18. *Sia $A = (a_{ij}) \in \mathbb{K}^{n\times n}$ una matrice quadrata.*

- *Gli elementi sulla* diagonale principale *di A sono gli elementi $a_{11}, \ldots, a_{nn}$ con uguale indice di riga e colonna.*
- *A si dice* triangolare superiore *se $a_{ij} = 0$ quando $i > j$, cioè se tutti gli elementi sotto la diagonale principale sono uguali a zero.*
- *A si dice* triangolare inferiore *se $a_{ij} = 0$ quando $i < j$, cioè se tutti gli elementi sopra la diagonale principale sono uguale a zero.*
- *A si dice* triangolare *se è triangolare superiore o triangolare inferiore.*
- *A si dice* diagonale *se $a_{ij} = 0$ quando $i \neq j$, cioè se tutti gli elementi fuori dalla diagonale principale sono uguali a zero.*
- *A si dice* matrice scalare *se è una matrice diagonale e tutti gli elementi sulla diagonale principale sono uguali tra loro.*

Definizione 8.19. *La* matrice identità *di ordine n è la matrice $I_n = (\delta_{ij}) \in \mathbb{K}^{n\times n}$ dove* $\delta_{ij} = \begin{cases} 1 & \text{se } i = j, \\ 0 & \text{altrimenti.} \end{cases}$ *Quindi I_n è la matrice scalare con tutti* 1 *sulla diagonale principale.*

Proposizione 8.20. *Il prodotto tra matrici gode delle seguenti proprietà.*

1. $I_m A = A,\ AI_n = A \qquad \forall A \in \mathbb{K}^{m\times n}$.
2. $A(BC) = (AB)C \qquad \forall A \in \mathbb{K}^{m\times n},\ \mathbb{K}^{n\times r},\ \forall C \in \mathbb{K}^{r\times s}$.
3. $A(B+C) = AB + AC \qquad \forall A \in \mathbb{K}^{m\times n},\ \forall B, C \in \mathbb{K}^{n\times r}$.
4. $(B+C)A = BA + CA \qquad \forall A \in \mathbb{K}^{m\times n},\ \forall B, C \in \mathbb{K}^{r\times m}$.
5. $\lambda(AB) = (\lambda A)B = A(\lambda B) \qquad \forall A \in \mathbb{K}^{m\times n},\ \forall B \in \mathbb{K}^{n\times r},\ \forall \lambda \in \mathbb{K}$
6. $(AB)^T = B^T A^T \qquad \forall A \in \mathbb{K}^{m\times n},\ \forall B \in \mathbb{K}^{n\times r}$

Dimostrazione. 1. La componente (i,j) nella matrice $I_m A$ è $\sum_{h=1}^{m} \delta_h^i a_j^h = \delta_i^i a_j^i = a_j^i$, come in A. Allo stesso modo la componente (i,j) in AI_n è $\sum_{h=1}^{n} a_h^i \delta_j^h = a_j^i \delta_j^j = a_j^i$.

2. Si ha

$$(A(BC))_j^i = \sum_{k=1}^{n} a_k^i \left(\sum_{\ell=1}^{r} b_\ell^k c_j^\ell \right) = \sum_{k=1}^{n} \sum_{\ell=1}^{r} a_k^i b_\ell^k c_j^\ell = \sum_{\ell=1}^{r} \left(\sum_{k=1}^{n} a_k^i b_\ell^k \right) c_j^\ell = ((AB)C)_j^i \,.$$

3. Si ha

$$(A(B+C))_j^i = \sum_{k=1}^{n} a_k^i (b_j^k + c_j^k) = \sum_{k=1}^{n} (a_k^i b_j^k + a_k^i c_j^k) = \sum_{k=1}^{n} a_k^i b_j^k + \sum_{k=1}^{n} a_k^i c_j^k = (AB + AC)_j^i \,.$$

4. Si ha

$$((B+C)A)_j^i = \sum_{k=1}^{m} (b_k^i + c_k^i) a_j^k = \sum_{k=1}^{m} b_k^i a_j^k + \sum_{k=1}^{m} c_k^i a_j^k = (BA + CA)_j^i \,.$$

5. Sono uguali le seguenti componenti (i,j):

$$(\lambda(AB))_j^i = \lambda \sum_{k=1}^{n} a_k^i b_j^k, \qquad ((\lambda A)B)_j^i = \sum_{k=1}^{n} (\lambda a_k^i) b_j^k, \qquad (A(\lambda B))_j^i = \sum_{k=1}^{n} a_k^i (\lambda b_j^k).$$

6. Si ha

$$\left((A \cdot B)^T\right)_j^i = (AB)_i^j = \sum_{k=1}^{n} a_k^j b_i^k = \sum_{k=1}^{n} b_i^k a_k^j = \sum_{k=1}^{n} \left(B^T\right)_k^i \left(A^T\right)_j^k = \left(B^T \cdot A^T\right)_j^i \,.$$

□

Alcune operazioni sulle matrici sono più veloci se le matrici stesse hanno delle particolari strutture o forme. Tutte le matrici possono essere trasformate in modo tale da avere tali particolari forme, attraverso opportune operazioni.

Definizione 8.21. *Una matrice si dice* a scala (o a gradini) per righe *se:*

- *le righe nulle della matrice si trovano in basso.*
- *Il primo elemento non nullo di una riga non nulla, detto* pivot *di quella riga, si trova più a destra dei pivot delle righe precedenti.*

Si dice completamente ridotta *se ogni pivot è uguale a* 1 *ed è l'unico elemento non nullo della sua colonna.*

Si noti che "più in alto / più in basso" significa "con un indice di riga minore/maggiore", così come "più a sinistra / più a destra" significa "con un indice di colonna minore/maggiore". Si noti anche che una matrice quadrata a gradini per righe è triangolare superiore.

Esempio 8.22. *Esempi di matrici a gradini per righe sono le seguenti:*

$$\begin{pmatrix} 1 & -1 & 1 & 3 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 & 5 \\ 0 & 1 & 7 \\ 0 & 0 & 0 \end{pmatrix}.$$

Esempi di matrici completamente ridotte a gradini sono le seguenti:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 7 \\ 0 & 0 & 0 \end{pmatrix}.$$

Una matrice $A \in \mathbb{K}^{m\times n}$ può essere trasformata tramite le seguenti *operazioni elementari di riga* (le operazioni elementari di colonna si definiscono in modo analogo):

1. scambiare di posto due righe di A: $A^i \leftrightarrow A^j$;
2. moltiplicare tutti gli elementi di una riga di A per un fissato scalare $\lambda \neq 0$: $A^i \to \lambda A^i$;
3. sommare a una riga di A un multiplo di un'altra riga: $A^i \to A^i + \lambda A^j$.

Il seguente algoritmo, detto *algoritmo di Gauss*, trasforma una qualsiasi matrice in una matrice a gradini (o in una matrice completamente ridotta a gradini), tramite operazioni elementari di riga.

Definizione 8.23 (Algoritmo di Gauss)**.** *Sia $A \in \mathbb{K}^{m\times n}$.*

1. *Se A è la matrice è nulla, allora A è già completamente ridotta a gradini.*
2. *Se A non è nulla, si cerca la prima colonna da sinistra che ha almeno un elemento non zero. Si scambia la prima riga con la prima riga contenente un elemento $\mu \neq 0$ in quella colonna; μ diventa il pivot della prima riga.*
3. *Si trasformano in zeri tutti gli elementi sotto al primo pivot nella colonna del primo pivot, sottraendo ad ogni riga sotto il primo pivot multipli opportuni della prima riga.*
4. *Si considera la sottomatrice che si ottiene senza considerare la prima riga e si ripetono tutti i passi precedenti.*

In questo modo si ottiene una matrice a gradini. Se si vuole una matrice a gradini completamente ridotta, si procede ancora come segue.

1. *Per ogni pivot a partire dall'ultimo, si trasformano in zeri tutti gli elementi sopra al pivot nella colonna del pivot, sottraendo alle righe sopra al pivot opportuni multipli della riga del pivot.*
2. *Per ogni pivot μ, si divide tutta la sua riga per μ.*

In realtà al punto (2) la scelta della riga può essere fatta in maniera arbitraria: se esistono più righe che hanno elementi non nulli nella colonna selezionata, la scelta può ricadere su ognuna di esse. In generale si preferisce scegliere (se possibile) una riga che contiene già un 1 in tale posizione.

Usando in modi diversi le tre operazioni elementari di riga, si possono ottenere matrici a gradini differenti. Resta comunque invariato il numero di pivot ottenuti.

Esempio 8.24. *Mostriamo attraverso un esempio i passaggi da effettuare mediante l'algoritmo di Gauss su una matrice per renderla a gradini. Partiamo dalla seguente matrice:*

$$A = \begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 3 & 5 & 1 & 1 \end{pmatrix} \in \mathbb{R}^{3\times 4}.$$

La prima riga ha al primo posto l'elemento $2 \neq 0$. Rendiamo uguali a zero tutti gli elementi sotto al pivot 2 della prima riga. Basta sottrarre alla terza riga $\frac{3}{2}$ per la prima riga. Si ottiene

$$\begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 0 & 5 & -7/2 & 1 \end{pmatrix}.$$

Ora consideriamo la seconda colonna, dalla seconda riga in giù: nella seconda colonna e seconda riga abbiamo un 1*; teniamo quell'*1 *come pivot, e annullare gli elementi sotto di lui. Basta sottrarre alla terza riga* 5 *volte la seconda riga:*

$$\begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 0 & 0 & -57/2 & -39 \end{pmatrix}.$$

Ora la matrici è ridotta a gradini. Se la vogliamo completamente ridotta, dobbiamo trasformare in zero tutti gli elementi delle colonne dei pivot (tranne in pivot), e dividere ogni riga per il suo pivot:

$$\xrightarrow[R_1 \to \frac{1}{2} R_1]{} \begin{pmatrix} 1 & 0 & 3/2 & 0 \\ 0 & 1 & 5 & 8 \\ 0 & 0 & -57/2 & -39 \end{pmatrix} \xrightarrow[R_1 + \frac{1}{19} R_3]{} \begin{pmatrix} 1 & 0 & 0 & -39/19 \\ 0 & 1 & 5 & 8 \\ 0 & 0 & -57/2 & -39 \end{pmatrix}$$

$$\xrightarrow[R_2 + \frac{10}{57} R_3]{} \begin{pmatrix} 1 & 0 & 0 & -39/19 \\ 0 & 1 & 0 & 22/19 \\ 0 & 0 & -57/2 & -39 \end{pmatrix} \xrightarrow[R_3 \to -\frac{2}{57} R_3]{} \begin{pmatrix} 1 & 0 & 0 & -39/19 \\ 0 & 1 & 0 & 22/19 \\ 0 & 0 & 1 & 26/19 \end{pmatrix}$$

8.2 Matrici invertibili

Definizione 8.25. *Una matrice quadrata $M \in \mathbb{K}^{n \times n}$ si dice* invertibile *se esiste una matrice $N \in \mathbb{K}^{n \times n}$ tale che $MN = NM = I_n$. La matrice N si chiama* inversa *di M e si indica con M^{-1}.*

Esempio 8.26. *È di facile verifica che le due matrici*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 0 & 1 \\ 3 & 2 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1/2 & -1 & -1/2 \\ -5/4 & 2 & 7/4 \\ 1 & -1 & -1 \end{pmatrix}$$

sono l'una l'inversa dell'altra.

La matrice inversa gode delle seguenti proprietà.

Proposizione 8.27.

- *Se $A \in \mathbb{K}^{n \times n}$ è invertibile, allora la sua inversa A^{-1} è unica.*
- *Se $A \in \mathbb{K}^{n \times n}$ è invertibile, allora A^{-1} è invertibile, con inversa $(A^{-1})^{-1} = A$.*
- *Se $A, B \in \mathbb{K}^{n \times n}$ sono invertibili, allora AB è invertibile, e $(AB)^{-1} = B^{-1}A^{-1}$.*
- *Se $A \in \mathbb{K}^{n \times n}$ è invertibile, allora A^T è invertibile con inversa $(A^T)^{-1} = (A^{-1})^T$.*

- *Se $A \in \mathbb{K}^{n\times n}$ è invertibile e $\alpha \in \mathbb{K}\setminus\{0\}$, allora αA è invertibile e $(\alpha A)^{-1} = \alpha^{-1}A^{-1}$.*

Dimostrazione. Se $B, C \in \mathbb{K}^{n\times n}$ sono due inverse di A, allora

$$B = BI_n = B(AC) = (BA)C = I_nC = C.$$

Se $A \in \mathbb{K}^{n\times n}$ è invertibile, allora $A^{-1}A = AA^{-1} = I_n$ e A^{-1} è invertibile con inversa A.

Se $A, B \in \mathbb{K}^{n\times n}$ sono invertibili, allora

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$$

e analogamente $(AB)(B^{-1}A^{-1}) = I_n$, quindi AB è invertibile con inversa $B^{-1}A^{-1}$.

Se $A \in \mathbb{K}^{n\times n}$ è invertibile, allora $(A^{-1})^TA^T = (AA^{-1})^T = I_n^T = I_n$; analogamente, $A^T(A^{-1})^T = I_n$. Quindi A^T è invertibile con inversa $(A^{-1})^T$.

Se $A \in \mathbb{K}^{n\times n}$ è invertibile e $\alpha \in \mathbb{K}$ con $\alpha \neq 0$, allora $(\alpha^{-1}A^{-1})(\alpha A) = (\alpha^{-1}\alpha)(A^{-1}A) = 1\cdot I_n = I_n$; analogamente, $(\alpha A)(\alpha^{-1}A^{-1}) = I_n$. Quindi αA è invertibile con inversa $\alpha^{-1}A^{-1}$. □

Definizione 8.28. *Una matrice $A \in \mathbb{K}^{n\times n}$ si dice* ortogonale *se A è invertibile con inversa $A^{-1} = A^T$; cioè, se $AA^T = A^TA = I_n$.*

Esempio 8.29. *Si può controllare facilmente che le seguenti matrici sono ortogonali.*

$$\begin{pmatrix} 1/3 & 2/3 & 2/3 \\ 2/3 & 1/3 & -2/3 \\ 2/3 & -2/3 & 1/3 \end{pmatrix}, \begin{pmatrix} 1/3 & 2/3 & 2/3 \\ 2/3 & 1/3 & -2/3 \\ -2/3 & 2/3 & -1/3 \end{pmatrix}.$$

Osservazione 8.30. *Sia $\mathbb{K} = \mathbb{R}$. L'elemento di posto (i, j) in AA^T è il prodotto tra la i-esima riga di A e la j-esima colonna di A^T, quindi tra la i-esima e la j-esima riga di A (visti come vettori di $\mathbb{R}^n$); analogamente, l'elemento (i, j) di A^TA è il prodotto tra la i-esima e la j-esima colonna di A (visti come vettori di $\mathbb{R}^n$).*

Perciò, una matrice $A \in \mathbb{R}^{n\times n}$ è ortogonale se e solo se l'insieme delle sue righe e l'insieme delle sue colonne formano due basi ortogonali di $\mathbb{R}^{n\times n}$ (rispetto al prodotto scalare standard).

Per calcolare la matrice inversa (qualora esista) di $A \in \mathbb{K}^{n\times n}$ si può procedere nel seguente modo. Si scrive la matrice $n \times 2n$ B ottenuta accostando alla destra di A la matrice identica I_n, e si trasforma B in una matrice a gradini tramite operazioni elementari di riga. Se nelle prime n colonne troviamo meno di n pivot, allora A non è invertibile.

Altrimenti proseguiamo fino a ottenere una matrice completamente ridotta a gradini C. In questo caso, le prime n colonne di C formano ma matrice identità I_n, e le ultime n colonne di C formano l'inversa A^{-1}. Esponiamo questo metodo mediante qualche esempio.

Esempio 8.31. *Controlliamo se la matrice*

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

è invertibile e determiniamone eventualmente l'inversa.

Riduciamo a gradini la matrice

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

$$\xrightarrow[R_2+2R_1]{} \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 4 & 7 & 2 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[R_3-3R_1]{} \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 4 & 7 & 2 & 1 & 0 \\ 0 & -4 & -8 & -3 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow[R_3+R_2]{} \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 4 & 7 & 2 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix} \xrightarrow[R_1-\frac{1}{2}R_2]{} \begin{pmatrix} 1 & 0 & -1/2 & 0 & -1/2 & 0 \\ 0 & 4 & 7 & 2 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow[R_1-\frac{1}{2}R_3]{} \begin{pmatrix} 1 & 0 & 0 & 1/2 & -1 & -1/2 \\ 0 & 4 & 7 & 2 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix} \xrightarrow[R_2+7R_3]{} \begin{pmatrix} 1 & 0 & 0 & 1/2 & -1 & -1/2 \\ 0 & 4 & 0 & -5 & 8 & 7 \\ 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow[R_2\to\frac{1}{4}R_2]{} \begin{pmatrix} 1 & 0 & 0 & 1/2 & -1 & -1/2 \\ 0 & 1 & 0 & -5/4 & 2 & 7/4 \\ 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix} \xrightarrow[R_3\to -R_3]{} \begin{pmatrix} 1 & 0 & 0 & 1/2 & -1 & -1/2 \\ 0 & 1 & 0 & -5/4 & 2 & 7/4 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{pmatrix}$$

Poichè le prime tre colonne della matrice ottenuta formano la matrice identità I_3, allora A è invertibile e

$$A^{-1} = \begin{pmatrix} 1/2 & -1 & -1/2 \\ -5/4 & 2 & 7/4 \\ 1 & -1 & -1 \end{pmatrix}.$$

Esempio 8.32. *Controlliamo se la matrice*

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

è invertibile e determiniamone eventualmente l'inversa.

Riduciamo a gradini la matrice

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 1 & 2 & -2 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \underset{R_2-R_1}{\longrightarrow} \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 2 & -4 & -1 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\underset{R_3-2R_1}{\longrightarrow} \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 2 & -4 & -1 & 1 & 0 \\ 0 & 2 & -4 & -2 & 0 & 1 \end{pmatrix} \underset{R_3-R_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 2 & -4 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \end{pmatrix}.$$

Le prime tre colonne contengono solo due pivot. Perciò A non è invertibile.

8.3 Determinante di una matrice

Introduciamo il determinante di una matrice quadrata tramite il seguente teorema.

Teorema 8.33. *Esiste una e una sola funzione* $\det : \mathbb{K}^{n\times n} \to \mathbb{K}$ *che gode delle seguenti proprietà:*

- $\det(I_n) = 1$*;*
- *se* $A \in \mathbb{K}^{n\times n}$ *e* B *è ottenuta da* A *scambiando due righe o due colonne, allora* $\det(B) = -\det(A)$*;*
- *se* $A \in \mathbb{K}^{n\times n}$ *e* B *è ottenuta da* A *moltiplicando una riga o una colonna per* $\alpha \in \mathbb{K}$*, allora* $\det(B) = \alpha \cdot \det(A)$*;*
- *se* $A \in \mathbb{K}^{n\times n}$ *e* B *è ottenuta da* A *sommanda ad una riga (o ad una colonna) un multiplo di un'altra riga (o di un'altra colonna), allora* $\det(B) = \det(A)$.

La funzione $\det : \mathbb{K}^{n\times n} \to \mathbb{K}$ sopra descritta è detta *determinante*, e il valore $\det(A) \in \mathbb{K}$ è detto determinante della matrice A. Il determinante di una matrice scritta in forma estesa è indicato anche con due barre dritte al posto delle parentesi tonde.

Esempio 8.34. *Cambiando tra loro due righe (o due colonne) di una matrice il determinante cambia di segno.*

$$\det \begin{pmatrix} 1 & -2 & 3 & 4 \\ 6 & 5 & 9 & -1 \\ 3 & 1 & 2 & 5 \\ -1 & 3 & 0 & 1 \end{pmatrix} = -\det \begin{pmatrix} 1 & -2 & 3 & 4 \\ 6 & 5 & 9 & -1 \\ -1 & 3 & 0 & 1 \\ 3 & 1 & 2 & 5 \end{pmatrix}.$$

Esempio 8.35. *Sommando ad una riga di A un multiplo di una sua altra riga il determinante non cambia.*

$$\det\begin{pmatrix} 1 & -2 & 3 & 4 \\ 6 & 5 & 9 & -1 \\ 3 & 1 & 2 & 5 \\ -1 & 3 & 0 & 1 \end{pmatrix} = \det\begin{pmatrix} 1 & -2 & 3 & 4 \\ 6 & 5 & 9 & -1 \\ 5 & -3 & 8 & 13 \\ -1 & 3 & 0 & 1 \end{pmatrix}.$$

Esempio 8.36. *Moltiplicando una riga per uno scalare λ, il determinante della matrice risulta essere moltiplicato per lo stesso scalare λ.*

$$\det\begin{pmatrix} 1 & -2 & 3 & 4 \\ 18 & 15 & 27 & -3 \\ 3 & 1 & 2 & 5 \\ -1 & 3 & 0 & 1 \end{pmatrix} = 3\det\begin{pmatrix} 1 & -2 & 3 & 4 \\ 6 & 5 & 9 & -1 \\ 3 & 1 & 2 & 5 \\ -1 & 3 & 0 & 1 \end{pmatrix}.$$

Definizione 8.37. *Data una matrice quadrata $A = (a^i_j) \in \mathbb{K}^{n\times n}$, si dice* complemento algebrico *dell'elemento di posto (i,j), e si indica con $A^i_j \in \mathbb{K}$, il numero $(-1)^{i+j}$ moltiplicato per il determinante della matrice $(n-1)\times(n-1)$ ottenuta da A eliminando la i-esima riga e la j-esima colonna.*

Si noti che, se $n = 1$ e $A = (a^1_1) \in \mathbb{K}^{1\times 1}$, allora $\det(A) = a^1_1$. Se $n > 1$, allora il determinante può essere calcolato tramite il seguente *teorema di Laplace*, che riconduce il calcolo del determinante di una matrice $n \times n$ al calcolo del determinante di matrici $(n-1)\times(n-1)$.

Teorema 8.38. *Sia $A = (a^i_j) \in \mathbb{K}^{n\times n}$ con $n > 1$. Sia h un intero con $1 \le h \le n$. Allora*

$$\det(A) = \sum_{j=1}^{n} a^h_j A^h_j \qquad \textit{(“sviluppo di Laplace sulla h-esima riga”)},$$

$$\det(A) = \sum_{i=1}^{n} a^i_h A^i_h \qquad \textit{(“sviluppo di Laplace sulla h-esima colonna”)}.$$

Per $n \le 3$, il teorema di Laplace fornisce le seguenti per il calcolo del determinante.

- $n = 1$: se $A = (a^1_1) \in \mathbb{K}^{1\times 1}$, allora $\det(A) = a^1_1$.
- $n = 2$: se $A = \begin{pmatrix} a^1_1 & a^1_2 \\ a^2_1 & a^2_2 \end{pmatrix} \in \mathbb{K}^{2\times 2}$, allora $\det(A) = a^1_1 a^2_2 - a^2_1 a^2_2$.

- $n = 3$: se $A = \begin{pmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^3 & a_2^3 & a_3^3 \end{pmatrix} \in \mathbb{K}^{3\times 3}$, allora

$$\det(A) = a_1^1 a_2^2 a_3^3 + a_2^1 a_3^2 a_1^3 + a_3^1 a_1^2 a_2^3 - a_1^3 a_2^2 a_3^1 - a_2^3 a_3^2 a_1^1 - a_3^3 a_1^2 a_2^1$$

e $\det(A)$ può essere calcolato ricordando la regola mnemonica detta *regola di Sarrus*: ricopiamo a destra di A le prime due colonne di A, poi prendiamo col segno positivo i tre prodotti degli elementi che stanno su una diagonale "parallela" alla diagonale principale di A, e col segno negativo i tre proodotti degli elementi che stanno su una delle tre diagonali parallele alla daigonale secondaria.

Esempio 8.39. *Calcoliamo il determinante della matrice dell'esempio precedente*

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{pmatrix}$$

utilizzando direttamente il metodo di Sarrus. Si ha che il determinante di A è pari a

$$\begin{aligned} & 1\cdot 1\cdot 1 + 2\cdot(-2)\cdot 2 + 2\cdot 2\cdot(-2) \\ -2\cdot 1\cdot 2 - (-2)\cdot(-2)\cdot 1 - 1\cdot 2\cdot 2 &= \\ & 1 - 8 - 8 - 4 - 4 - 4 \quad = \quad -27. \end{aligned}$$

Esempio 8.40. *Calcoliamo il determinante della seguente matrice*

$$A = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 4 & 2 & 1 & -2 \\ 0 & 2 & 3 & 1 \\ 1 & 1 & 3 & -2 \end{pmatrix}$$

sviluppando rispetto alla prima riga. Quindi $\det(A)$ *è uguale a*

$$\begin{aligned} & 1\cdot\det\begin{pmatrix} 2 & 1 & -2 \\ 2 & 3 & 1 \\ 1 & 3 & -2 \end{pmatrix} 0\cdot(-1)\cdot\det\begin{pmatrix} 4 & 1 & -2 \\ 0 & 3 & 1 \\ 1 & 3 & -2 \end{pmatrix} + \\ & 2\cdot\det\begin{pmatrix} 4 & 2 & -2 \\ 0 & 2 & 1 \\ 1 & 1 & -2 \end{pmatrix} + (-1)\cdot(-1)\cdot\det\begin{pmatrix} 4 & 2 & 1 \\ 0 & 2 & 3 \\ 1 & 1 & 3 \end{pmatrix} \end{aligned}$$

Osservazione 8.41. *Per le proprietà del determinante viste a inizio sezione, sappiamo che il determinante non cambia se sommiamo a una riga (o colonna) un multiplo di un'altra riga (o colonna).*

Possiamo allora usare queste trasformazioni per semplificare il calcolo del determinante tramite Laplace: se riesco ad avere "tanti" zeri in una riga o colonna (idealmente, tutti gli elementi tranne al più uno), posso poi sviluppare il determinante su quella riga o colonna avendo meno conti da fare (perchè non occorre calcolare i determinanti che andrebbero poi moltiplicati per zero).

Esempio 8.42. *Calcoliamo il determinante della matrice A dell'esempio precedente, applicando prima delle trasformazioni che non cambiano il determinante:*

$$\det(A) = \det\begin{pmatrix} 1 & 0 & 2 & -1 \\ 4 & 2 & 1 & -2 \\ 0 & 2 & 3 & 1 \\ 1 & 1 & 3 & -2 \end{pmatrix} \underset{C_3-2C_1}{=} \det\begin{pmatrix} 1 & 0 & 0 & -1 \\ 4 & 2 & -7 & -2 \\ 0 & 2 & 3 & 1 \\ 1 & 1 & 1 & -2 \end{pmatrix} \underset{C_4+C_1}{=} \det\begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & 2 & -7 & 2 \\ 0 & 2 & 3 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

$$\underset{Laplace\ R_1}{=} \det\begin{pmatrix} 2 & -7 & 2 \\ 2 & 3 & 1 \\ 1 & 1 & -1 \end{pmatrix} \underset{Sarrus}{=} -6 - 7 + 4 - 6 - 2 - 14 = -31.$$

Elenchiamo alcune importanti proprietà del determinante.

Teorema 8.43. *Siano $A, B \in \mathbb{K}^{n\times n}$ e $\lambda \in \mathbb{K}$.*

1. *Se A ha due righe o colonne uguali, allora* $\det(A) = 0$.
2. *Più in generale, se una riga (o colonna) di A è combinazione lineare delle altre righe (o colonne) di A, allora* $\det(A) = 0$.
3. $\det(\lambda A) = \lambda^n \det(A)$.
4. *Se A è triangolare, allora* $\det(A)$ *è il prodotto degli elementi sulla diagonale principale di A.*
5. $\det(A^T) = \det(A)$.
6. (Teorema di Binet) $\det(A \cdot B) = \det(A) \cdot \det(B)$.
7. *Se A è invertibile, allora* $\det(A) \neq 0$ *e* $\det(A^{-1}) = \frac{1}{\det(A)}$.

Esempio 8.44. *Le seguenti matrici hanno determinante pari a* 0

$$\begin{pmatrix} 1 & 2 & 2 & 3 \\ 2 & 1 & -2 & -2 \\ 1 & 2 & 2 & 3 \\ -1 & 2 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 4 \\ 2 & 1 & 2 & -2 \\ 1 & 2 & 1 & 0 \\ -1 & 2 & -1 & 3 \end{pmatrix}.$$

Esempio 8.45. *Si ha che*

$$\det\begin{pmatrix} 4 & 8 & 8 & 12 \\ 12 & -4 & 0 & -8 \\ 4 & -4 & 0 & 4 \\ 4 & 8 & -12 & 16 \end{pmatrix} = 256 \times \det\begin{pmatrix} 1 & 2 & 2 & 3 \\ 3 & -1 & 0 & -2 \\ 1 & -1 & 0 & 1 \\ 1 & 2 & -3 & 4 \end{pmatrix}.$$

Esempio 8.46. *Si ha che*

$$\det\begin{pmatrix} 1 & -2 & 3 & 4 \\ 0 & 5 & 0 & -1 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & -2 \end{pmatrix} = 1 \times 5 \times 2 \times (-2) = -20.$$

Esempio 8.47. *Utilizzando la proprietà (5) del Teorema 8.43 si ha che*

$$\det\begin{pmatrix} 1 & -2 & 3 & 4 \\ 6 & 5 & 9 & -1 \\ 3 & 1 & 2 & 5 \\ -1 & 3 & 0 & 1 \end{pmatrix} = \det\begin{pmatrix} 1 & 6 & 3 & -1 \\ -2 & 5 & 1 & 3 \\ 3 & 9 & 2 & 0 \\ 4 & -1 & 5 & 1 \end{pmatrix}.$$

Definizione 8.48. *Data una matrice $A \in \mathbb{K}^{n\times n}$, si dice* matrice aggiunta *di A, e si indica con $A^{\#} \in \mathbb{K}^{n\times n}$, la matrice dei complementi algebrici di A; cioè, l'elemento di posto (i,j) in $A^{\#}$ è il complemento algebrico A^i_j dell'elemento a^i_j di A.*

Il seguente teorema mostra che il non annullarsi di $\det(A)$ caratterizza l'invertibilità di A, e che un altro metodo per calcolare l'inversa è tramite la matrice aggiunta.

Teorema 8.49. *Sia $A \in \mathbb{K}^{n\times n}$.*

- *A è invertibile se e solo se* $\det(A) \neq 0$.
- *Se A è invertibile, allora*
$$A^{-1} = \frac{1}{\det(A)} \left(A^{\#}\right)^T.$$

Esempio 8.50. *Calcoliamo (se possibile) l'inversa della matrice*

$$A = \begin{pmatrix} 4 & -2 & 6 \\ 1 & 3 & -2 \\ -1 & 2 & -1 \end{pmatrix} \in \mathbb{R}^{3\times 3}.$$

Poichè $\det(A) = 28 \neq 0$*, A è invertibile. I suoi complementi algebrici sono*

$$A^1_1 = +\det\begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix} = 1,\ A^1_2 = -\det\begin{pmatrix} 1 & -2 \\ -1 & -1 \end{pmatrix} = 3,\ A^1_3 = +\det\begin{pmatrix} 1 & 3 \\ -1 & 2 \end{pmatrix} = 5,$$

$$A_1^2 = -\det\begin{pmatrix} -2 & 6 \\ 2 & -1 \end{pmatrix} = 4,\ A_2^2 = +\det\begin{pmatrix} 4 & 6 \\ -1 & -1 \end{pmatrix} = 2,\ A_3^2 = -\det\begin{pmatrix} 4 & -2 \\ -1 & 2 \end{pmatrix} = -6,$$
$$A_1^3 = +\det\begin{pmatrix} -2 & 6 \\ 3 & -2 \end{pmatrix} = -14,\ A_2^3 = -\det\begin{pmatrix} 4 & 6 \\ 1 & -2 \end{pmatrix} = 14,\ A_3^3 = +\det\begin{pmatrix} 4 & -2 \\ 1 & 3 \end{pmatrix} = 14.$$

Pertanto la matrice inversa è

$$\mathbf{A}^{-1} = \frac{1}{28}\begin{pmatrix} 1 & 3 & 5 \\ 10 & 2 & -6 \\ -14 & 14 & 14 \end{pmatrix}^T = \frac{1}{28}\begin{pmatrix} 1 & 10 & -14 \\ 3 & 2 & 14 \\ 5 & -6 & 14 \end{pmatrix}.$$

8.4 Rango di una matrice

Sia A una matrice in $\mathbb{K}^{m\times n}$. Le sue righe $A^1, \dots, A^m$ possono essere viste come vettori di $\mathbb{K}^n$, e quindi generano un sottospazio vettoriale $L(A^1, \dots, A^m)$ di $\mathbb{K}^n$. Alla stessa maniera, le colonne di A generano un sottospazio vettoriale $L(A_1, \dots, A_n)$ di $\mathbb{K}^m$. Come noto dal precedente capitolo, la dimensione $\dim(L(A^1, \dots, A^m))$ è la cardinalità di una base estratta da $\{A^1, \dots, A^m\}$, e quindi è uguale al massimo numero di righe di A linearmente indipendenti (in $\mathbb{K}^n$). Alla stessa maniera, $\dim(L(A_1, \dots, A_n))$ è il massimo numero di colonne di A linearmente indipendenti.

Proposizione 8.51. *Per ogni $A \in \mathbb{K}^{m\times n}$ si ha* $\dim(L(A^1, \dots, A^m)) = \dim(L(A_1, \dots, A_n))$.

Questa proposizione permette di dare la seguente definizione di rango.

Definizione 8.52. *Sia $A \in \mathbb{K}^{m\times n}$. Si dice* rango *di A, e si indica con* $\mathrm{rk}(A)$*, il massimo numero di righe o colonne linearmente indipendenti.*

Osservazione 8.53. *Se $A \in \mathbb{K}^{m\times n}$, allora* $0 \le \mathrm{rk}(A) \le \min\{m, n\}$.

Si osservi che le tre trasformazioni elementari di riga non modificano il sottospazio $L(A^1, \dots, A^m)$ di $\mathbb{K}^n$ generato dalle righe di A. Perciò, se B è una matrice a gradini ottenuta da A tramite trasformazioni elementari di riga, allora lo spazio generato dalle righe di A è uguale allo spazio generato dalle righe di B, e quindi $\mathrm{rk}(A) = \mathrm{rk}(B)$. Se B è una matrice a gradini, è facile verificare che le righe non nulle di B (quelle che contengono i pivot) sono tutte linearmente indipendenti. Risulta quindi dimostrata la seguente proposizione.

Proposizione 8.54. *Se $A \in \mathbb{K}^{m\times n}$ viene ridotta tramite operazioni elementari di riga in una matrice a gradini B, allora il rango di A è uguale al numero di pivot di B.*

Inoltre, le righe non nulle di B formano una base del sottospazio vettoriale di $\mathbb{K}^n$ generato dalle righe di A.

Esempio 8.55. *Abbiamo già mostrato nell'Esempio 8.24 che la matrice*

$$A = \begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 1 & 5 & 8 \\ 3 & 5 & 1 & 1 \end{pmatrix}$$

può essere ridotta mediante l'algoritmo di Gauss nella matrice completamente ridotta

$$\begin{pmatrix} 1 & 0 & 0 & -39/19 \\ 0 & 1 & 0 & 22/19 \\ 0 & 0 & 1 & 26/19 \end{pmatrix}.$$

Quindi $\mathrm{rk}(A) = 3$.

Vogliamo ora dare un altro metodo di calcolo del rango.

Definizione 8.56. *Si dice* sottomatrice *di tipo* $h \times k$ *di* A *ogni matrice* $h \times k$ *ottenuta scegliendo* h *righe di* A *e* k *colonne di* A *e considerando gli elementi di* A *che stanno in quelle righe e colonne.*

Data una sottomatrice quadrata $h \times h$ M *di* A*, si dice* orlato *di* M *ogni sottomatrice quadrata* $(h+1) \times (h+1)$ *di* A *ottenuta da* M *aggiungendo gli elementi in un'altra riga e colonna di* A*.*

Si dice minore *di ordine* h *il determinante di una sottomatrice quadrata* $h \times h$ *di* A*.*

Se ho un minore di A *associato a una sottomatrice quadrata* M *di* A*, si dice* minore orlato *di quel minore il determinante di un orlato di* M*.*

Esempio 8.57. *Data la matrice*

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & -1 & 2 & -2 \\ 2 & 1 & 2 & 4 \end{pmatrix} \in \mathbb{R}^{3\times 4},$$

una sua sottomatrice quadrata 2×2 *è*

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

un orlato di B *è*

$$C = \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 2 \\ 2 & 1 & 2 \end{pmatrix},$$

un minore di ordine 3 *di* A *è*

$$\det \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 2 & 2 & 4 \end{pmatrix}.$$

Teorema 8.58. (di Kronecker) *Sia* $A \in \mathbb{K}^{m\times n}$. *Allora* $\mathrm{rk}(A)$ *è il massimo ordine di un minore diverso da zero di* A.

Inoltre, se troviamo in A *un minore diverso da zero di ordine* h, *e tutti i suoi minori orlati sono uguali a zero, allora* $\mathrm{rk}(A) = h$.

Il teorema di Kronecker mostra che, per trovare il rango di A non c'è bisogno di controllare tutti i minori di A: basta partire da un minore non nullo e orlare quello, fino a trovare un minore non nullo di ordine uno in più, procedere orlando questo nuovo minore, finché non si arriva a un minore non nullo non più orlabile a un minore non nullo più grande. Questo è il cosiddetto *metodo degli orlati*.

Esempio 8.59. *Riprendiamo la matrice*

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & -1 & 2 & -2 \\ 2 & 1 & 2 & 4 \end{pmatrix} \in \mathbb{R}^{3\times 4},$$

e calcoliamo il suo rango con il metodo degli orlati.

Chiaramente il suo rango è almeno 1, *perché* A *non è la matrice nulla. Preso il minore* 1×1 *non nullo dato dalla prima riga e prima colonna, orliamolo con la seconda riga e la seconda colonna:*

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

Abbiamo trovato un minore 2×2 *non nullo, e quindi proseguiamo orlandolo. Orliamolo con la terza riga e la terza colonna:*

$$\det \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 2 \\ 2 & 1 & 2 \end{pmatrix} = -2 + 0 + 0 + 4 - 2 + 0 = 0.$$

Poiche questa scelta non ha dato un minore non nullo, orliamo il minore 2×2 *di prima con la terza riga e la quarta colonna:*

$$\det \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & -2 \\ 2 & 1 & 4 \end{pmatrix} = -4 + 0 + 0 + 2 + 2 + 0 = 0.$$

Quindi tutti gli orlati di quel minore non nullo 2×2 *sono nulli. Quindi* $\mathrm{rk}(A) = 2$.

Esempio 8.60. *Supponiamo di dover calcolare il rango della seguente matrice.*

$$\begin{pmatrix} 0 & 4 & 1 & -3 & 0 \\ 1 & 4 & 3 & 5 & 7 \\ 3 & 0 & 7 & -4 & 1 \\ 0 & 1 & 3 & -2 & 3 \end{pmatrix}.$$

Possiamo sottrarre alla terza riga tre volte la seconda riga, ottenendo

$$\begin{pmatrix} 0 & 4 & 1 & -3 & 0 \\ 1 & 4 & 3 & 5 & 7 \\ 0 & -12 & -2 & -19 & -20 \\ 0 & 1 & 3 & -2 & 3 \end{pmatrix}.$$

Ora utilizziamo la quarta riga: sottraiamo quattro volte questa riga alla prima e aggiungiamola dodici volte alla terza. Otteniamo quindi

$$\begin{pmatrix} 0 & 0 & -11 & 5 & -12 \\ 1 & 4 & 3 & 5 & 7 \\ 0 & 0 & 34 & -33 & 16 \\ 0 & 1 & 3 & -2 & 3 \end{pmatrix}.$$

A questo punto, invece che continuare le operazioni sulle righe, possiamo provare a calcolare il determinante della matrice formata dalle prime 4 *colonne e dalle* 4 *righe della matrice. Sviluppando il determinante rispetto alla prima colonna si ha che esso è pari a*

$$-\det\begin{pmatrix} 0 & -11 & 5 \\ 0 & 34 & -33 \\ 1 & 3 & -2 \end{pmatrix} = -\det\begin{pmatrix} -11 & 5 \\ 34 & -33 \end{pmatrix} \neq 0,$$

dove il penultimo passaggio è stato ottenuto sviluppando rispetto alla prima colonna della nuova matrice 3×3*. Il rango della matrice iniziale è pertanto pari a* 4 *in quanto abbiamo determinato un minore* 4×4 *diverso da* 0*.*

Dal teorema di Kronecker segue immediatamente la seguente caratterizzazione delle matrici quadrate di rango massimo.

Proposizione 8.61. *Una matrice quadrata* $A \in \mathbb{K}^{n\times n}$ *ha rango* n *se e solo se* $\det(A) \neq 0$*.*

8.5 Esercizi

Esercizio 8.1. *Si calcoli il rango della seguente matrice.*

$$\mathbf{A} = \begin{pmatrix} 3 & 4 & -2 & 6 \\ 1 & 3 & 4 & -2 \\ -1 & 2 & -1 & 1 \end{pmatrix}.$$

Soluzione.

La matrice A è una 3×4 quindi il suo rango è al più 3. Utilizziamo l'algoritmo di eliminazione.

$$\begin{pmatrix} 1 & 4/3 & -2/3 & 2 \\ 0 & 5/3 & 14/3 & -4 \\ 0 & 10/3 & -3 & 3 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 4/3 & -2/3 & 2 \\ 0 & 1 & 14/5 & -12/5 \\ 0 & 10/3 & -3 & 3 \end{pmatrix}$$

$$\Longrightarrow \begin{pmatrix} 1 & 4/3 & -2/3 & 2 \\ 0 & 1 & 14/5 & -12/5 \\ 0 & 0 & -34/3 & 11 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 4/3 & -2/3 & 2 \\ 0 & 1 & 14/5 & -12/5 \\ 0 & 0 & 1 & -33/34 \end{pmatrix}.$$

Quindi il rango è 3.

Esercizio 8.2. *Ridurre in matrici a scala per righe le seguenti matrici.*

$$\begin{pmatrix} 1 & 1 & 1 & -3 & 2 \\ 3 & 4 & 3 & -7 & 7 \\ 1 & 0 & 0 & -4 & -1 \\ 0 & 1 & 3 & 1 & 7 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 0 & 4 \\ 2 & 5 & 3 & 0 \\ 1 & 4 & -8 & -18 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 & -1 \\ 3 & 2 & 6 & 4 & 4 & 7 & -2 \\ 1 & -6 & 2 & -2 & -3 & 1 & -3 \\ -3 & 8 & -6 & 1 & 2 & -4 & 10 \end{pmatrix}$$

Esercizio 8.3. *Ridurre in matrici a scala per righe ridotte le matrici dell'esercizio precedente.*

Esercizio 8.4. *Determinare il rango della seguente matrice*

$$A = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 1 & 3 & 0 & 0 \\ 1 & -3 & 2 & 4 \\ 2 & 3 & 1 & 2 \end{pmatrix}$$

Indicando con r_i la $i-esima$ riga eseguiamo le seguenti sostituzioni: r_1 con $r_2 - r_1$, r_3 con $r_3 - r_1$ e r_4 con $r_4 - 2r_2$. Si ha quindi

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 3 & -1 & -2 \\ 0 & -3 & 1 & 2 \\ 0 & 3 & -1 & -2 \end{pmatrix}.$$

Osservando la matrice ottenuta appare chiaro che non conviene utilizzare la riga 1 per nuove sostituizioni, da momento che vanificherebbe la fatica fatta per avere gli 0 al primo posto nelle

righe sottostanti. Quindi procediamo con le prossime operazioni elementari, sostituiamo r_3 con $r_3 + r_2$ e r_4 con $r_4 - r_1$. Otteniamo quindi

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 3 & -1 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Si verifica facilmente che la matrice ha ragno pari a 2.

Esercizio 8.5. *Si riduca la seguente matrice a scala per riga.*

$$A = \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 2 & 4 & 0 & 4 & 4 \\ 1 & 2 & 3 & 5 & 5 \\ 2 & 4 & 0 & 4 & 7 \end{pmatrix}.$$

Svolgimento. Indicando con r_i la i-esima riga eseguiamo le seguenti sostituzioni: r_2 con $r_2 - 2r_1$, r_3 con $r_23 - r_1$ e r_4 con $r_4 - 2r_2$, quindi si ha:

$$\begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 0 & 0 & -2 & -2 & -2 \\ 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & -2 & -2 & 1 \end{pmatrix}.$$

Adesso sostituiamo r_3 con $r_3 + r_2$ e r_4 con $r_4 - r_2$ ottenendo:

$$\begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 0 & 0 & -2 & -2 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

Infine scambiamo r_3 con r_4 e sostituiamo r_2 con $\frac{-r_2}{2}$, quindi

$$\begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Esercizio 8.6. *Determinare l'inversa della seguente matrice*

$$A = \begin{pmatrix} 1 & 0 & 3 \\ 4 & 2 & -1 \\ -2 & 0 & -2 \end{pmatrix}.$$

Svolgimento. Per ottenere A^{-1} dobbiamo cercare di trasformare A nella matrice $\mathbb{I}_3$ eseguendo operazioni elementari che replichiamo contemporaneamente su I_3. Quindi abbiamo

$$\begin{pmatrix} 1 & 0 & 3 \\ 4 & 2 & -1 \\ -2 & 0 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Indicando con r_i la $i-esima$ riga eseguiamo le seguenti sostituzioni: r_2 con $r_2 - 4r_1$ e r_3 con $r_3 + 2r_1$, ottenendo:

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & -13 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

Dividiamo la seconda riga per 2 e la terza riga per 4.

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -13/2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1/2 & 0 \\ 1/2 & 0 & 1/4 \end{pmatrix}.$$

Sottraiamo alla prima riga 3 volta la terza e sommiamo alla seconda $13/2$ volte la terza

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1/2 & 0 & -3/4 \\ 5/4 & 1/2 & 13/8 \\ 1/2 & 0 & 1/4 \end{pmatrix}.$$

Quindi

$$A^{-1} = \begin{pmatrix} -1/2 & 0 & -3/4 \\ 5/4 & 1/2 & 13/8 \\ 1/2 & 0 & 1/4 \end{pmatrix}.$$

Esercizio 8.7. *Determinare il rango della seguente matrice*

$$A = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 4 & 2 & 2 \\ 3 & 6 & 3 & 4 \end{pmatrix}.$$

Svolgimento. Utilizziamo il processo di riduzione di Gauss per determinare una riduzione in forma a scala per riga. Indicando con r_i la $i-esima$ riga sostituiamo r_2 con $r_2 - 2r_1$, ottenendo

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 3 & 6 & 3 & 4 \end{pmatrix}.$$

Scambiamo la seconda e la terza riga:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 6 & 3 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Infine sostituiamo r_2 con $r_2 - 3r_1$. Si ha

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Quindi il rango di A è 2.

Esercizio 8.8. *Determnare il determinante della seguente matrice utilizzando l'algoritmo di Gauss.*

$$A = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

Svolgimento. Indicando con r_i la $i - esima$ riga scambiamo r_2 con r_3. Questa operazione elementare comporta, per il calcolo del determinante, il cambiamento di segno, ossia

$$det = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} = -det \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \\ -1 & 0 & 2 \end{pmatrix}.$$

Adesso scambiamo r_3 con $r_3 + \frac{1}{2}r_1$, quindi $detA$ sarà

$$-det \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & \frac{1}{2} & 2 \end{pmatrix}.$$

Scambiamo di nuovo r_3, questa volta con $r_3 - \frac{1}{2}r_2$, quindi $detA$ sarà

$$-det \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

La matrice è una triangolare superiore e il determinante è dato dal prodotto degli elementi sulla diagonale, $\det(A) = -(2 \cdot 1 \cdot 1) = -2$.

Capitolo 9

Sistemi Lineari

In questo capitolo trattiamo i sistemi lineari su un campo K; la discussione della loro risolubilità e del numero di soluzioni; e i metodi risolutivi per il calcolo esplicito delle soluzioni.

Definizione 9.1. *Un* sistema lineare su K di m equazioni in n incognite $x_1, \dots, x_n$ *è un'espressione S del tipo*

$$S : \begin{cases} a_1^1 x_1 + a_2^1 x_2 + \cdots + a_n^1 x_n = b_1 \\ a_1^2 x_1 + a_2^2 x_2 + \cdots + a_n^2 x_n = b_2 \\ \vdots \\ a_1^m x_1 + a_2^m x_2 + \cdots + a_n^m x_n = b_m \end{cases}$$

dove $a_j^i, b_j \in \mathbb{K}$. Una soluzione *del sistema S è una n-upla $(\bar{x}_1, \dots, \bar{x}_n) \in \mathbb{K}^n$ tale che*

$$\begin{cases} a_1^1 \bar{x}_1 + a_2^1 \bar{x}_2 + \cdots + a_n^1 \bar{x}_n = b_1 \\ a_1^2 \bar{x}_1 + a_2^2 \bar{x}_2 + \cdots + a_n^2 \bar{x}_n = b_2 \\ \vdots \\ a_1^m \bar{x}_1 + a_2^m \bar{x}_2 + \cdots + a_n^m \bar{x}_n = b_m. \end{cases}$$

$Sol(S) \subseteq \mathbb{K}^n$ indica l'insieme di tutte le soluzioni di S. Il sistema lineare S si dice:

- compatibile *(o* possibile*) se ammette soluzioni, cioè se $Sol(S) \neq \emptyset$;*
- incompatibile *(o* impossibile*) se non ammette soluzioni, cioè se $Sol(S) = \emptyset$;*
- determinato *se ammette una e una sola soluzione, cioè se $|Sol(S)| = 1$;*
- indeterminato *se ammette più soluzioni, cioè se $|Sol(S)| > 1$;*

- omogeneo *se tutti i termini noti sono zero, cioè* $b_1 = \cdots = b_m = 0$.

Dati due sistemi lineari S, S' *in* n *incognite su* K*,*

- S *e* S' *si dicono* equivalenti *se hanno le stesse soluzioni, cioè* $Sol(S) = Sol(S')$*;*
- S' *si dice un* sottosistema *di* S *se tutte le equazioni di* S' *sono anche equazioni di* S*;*
- S *si dice un sistema* minimo *se non è equivalente a nessun suo sottosistema proprio.*

Poniamo

$$A = \begin{pmatrix} a_1^1 & \cdots & a_n^1 \\ \vdots & \ddots & \vdots \\ a_n^m & \cdots & a_n^m \end{pmatrix} \in \mathbb{K}^{m\times n}, \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{K}^{m\times 1}.$$

Allora la forma matriciale *del sistema* S *sopra descritto è*

$$S: \ AX = B.$$

La matrice A *è detta* matrice dei coefficienti *o* matrice incompleta *del sistema* S*,* X *è la colonna delle incognite e* B *è la colonna dei termini noti. La matrice*

$$C = (A \mid B) = \begin{pmatrix} a_1^1 & \cdots & a_n^1 & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_1^m & \cdots & a_n^m & b_m \end{pmatrix} \in \mathbb{K}^{m\times(n+1)}$$

è detta matrice completa *del sistema* S*.*

Si osservi che, poichè C ha una colonna in più di A, allora $\mathrm{rk}(C) = \mathrm{rk}(A)$ oppure $\mathrm{rk}(C) = \mathrm{rk}(A) + 1$.

9.1 Compatibilità di un sistema lineare

Sia $S : AX = B$ un sistema lineare, con $A = (a_j^i) \in \mathbb{K}^{m\times n}$. Per studiarne la compatibilità, iniziamo osservando che, preso $\bar{X} = (\bar{x}_1, \ldots, \bar{x}_n) \in \mathbb{K}^n$ visto come colonna in $\mathbb{K}^{m\times 1}$, si ha

$$A\bar{X} = \begin{pmatrix} a_1^1\bar{x}_1 + \cdots + a_n^1\bar{x}_n \\ \vdots \\ a_1^m\bar{x}_1 + \cdots + a_n^m\bar{x}_n \end{pmatrix} = \begin{pmatrix} \bar{x}_1 a_1^1 \\ \vdots \\ \bar{x}_1 a_1^m \end{pmatrix} + \cdots + \begin{pmatrix} \bar{x}_n a_n^1 \\ \vdots \\ \bar{x}_n a_n^m \end{pmatrix} = \bar{x}_1 \cdot \begin{pmatrix} a_1^1 \\ \vdots \\ a_1^m \end{pmatrix} + \cdots + \bar{x}_n \cdot \begin{pmatrix} a_n^1 \\ \vdots \\ a_n^m \end{pmatrix}.$$

Definiamo allora la seguente *forma per colonne* del sistema S:

$$S: \quad x_1 A_{(1)} + \cdots x_n A_{(n)} = B,$$

dove $A_{(1)}, \ldots, A_{(n)}$ sono le colonne di A. In termini di algebra lineare, quanto appena osservato con $\bar{X}$ dimostra il seguente criterio.

Proposizione 9.2. *Il sistema lineare $S : AX = B$ è compatibile se e solo se B (visto come vettore di $\mathbb{K}^m$) è combinazione lineare delle colonne di A. In formula:*

$$S \text{ è compatibile} \iff B \in L(A_{(1)}, \ldots, A_{(n)}).$$

Possiamo ora dimostrare il teorema fondamentale sulla compatibilità dei sistemi lineari.

Teorema 9.3. (di Rouché-Capelli) *Un sistema lineare è compatibile se e solo se la matrice incompleta e la matrice completa hanno lo stesso rango.*

Dimostrazione. Sia $A = (A_{(1)} \cdots A_{(n)})$ la matrice incompleta e $C = (A_{(1)} \cdots A_{(n)} B)$ la matrice completa del sistema lineare S. Allora, usando la proposizione precedente, si ha che

$$S \text{ è compatibile} \iff B \in L(A_{(1)}, \ldots, A_{(n)}) \iff L(A_{(1)}, \ldots, A_{(n)}, B) = L(A_{(1)}, \ldots, A_{(n)})$$

$$\iff \dim L(A_{(1)}, \ldots, A_{(n)}, B) = \dim L(A_{(1)}, \ldots, A_{(n)}) \iff \mathrm{rk}(C) = \mathrm{rk}(A).$$

□

Se S è un sistema compatibile, chiamiamo *rango di S* il rango (uguale) delle sue matrici incompleta e completa.

L'insieme delle soluzioni di un sistema lineare omogeneo è descritto nel seguente risultato, di cui omettiamo la dimostrazione.

Proposizione 9.4. *Sia $S_0 : AX = \underline{0}$ un sistema lineare omogeneo su $\mathbb{K}$ in n variabili. Allora $Sol(S_0)$ è un sottospazio vettoriale di $\mathbb{K}^n$, di dimensione $n - \mathrm{rk}(A)$.*

Se in campo $\mathbb{K}$ ha infiniti elementi, si usa anche dire che S_0 ha "$\infty^{n-\mathrm{rk}(A)}$ soluzioni"; con la convenzione che $\infty^0 = 1$, cioè: se $\mathrm{rk}(A) = n$, allora S_0 è determinato, e l'unica soluzione è il vettore nullo.

Proposizione 9.5. *Sia $S : AX = B$ un sistema lineare compatibile, e $\bar{X} \in SOl(S)$ una sua fissata soluzione. Sia $S_0 : AX = \underline{0}$ il suo* sistema omogeneo associato. *Allora*

$$Sol(S) = \{\bar{X} + X_0 \colon X_0 \in Sol(S_0)\}.$$

Dimostrazione. Sia $\tilde{X} \in \mathbb{K}^n$. Allora $\tilde{X} \in Sol(S)$ se e solo se $A\tilde{X} = B = A\bar{X}$, cioè se e solo se $A(\tilde{X} - \bar{X}) = \underline{0}$, cioè se e solo se $\tilde{X} - \bar{X} = X_0$ per qualche $X_0 \in Sol(S_0)$. □

La precedente dimostrazione mostra che l'insieme delle soluzioni di un sistema lineare compatibile è in corrispondenza biunivoca con l'insieme delle soluzioni del suo sistema omogeneo associato.

Perciò, se S è un sistema compatibile in n incognite di rango r, allora $Sol(S)$ dipende da $n - r$ parametri indipendenti e liberi di variare in $\mathbb{K}$; se $\mathbb{K}$ è infinito, diciamo che S ha ∞^{n-r} soluzioni (se $r = n$, allora S è determinato).

Definizione 9.6. *Le* operazioni elementari *sui sistemi lineari sono:*

1. *scambiare due equazioni tra loro;*
2. *moltiplicare una equazione membro a membro per uno scalare $\lambda \in \mathbb{K}$ con $\lambda \neq 0$;*
3. *aggiungere membro a membro ad una equazione un multiplo di un'altra equazione.*

Dato un sistema lineare lineare $S : AX = B$ con matrice completa C, fare una operazione elementare su S corrisponde a fare la corrispondente trasformazione elementare di riga sulla matrice completa C.

Osservazione 9.7. *Le operazioni elementari non modificano l'insieme delle soluzioni di un sistema lineare S; cioè, trasformano S in un sistema lineare S' equivalente a S.*

Possiamo quindi parlare di *combinazione lineare* delle equazioni di un sistema, intendendo la corrispondente combinazione lineare delle righe della matrice completa.

Se una equazione del sistema S è combinazione lineare delle altre equazioni di S, allora eliminando tale equazione l'insieme delle soluzioni non cambia, cioè si ottiene un sistema equivalente a S. Perciò, se S è compatibile di rango r e identifichiamo r righe linearmente indipendenti nella matrice completa C, allora possiamo eliminare le equazioni corrispondenti alle altre $n - r$ righe di C, e ottenere un sottosistema *minimo* equivalente a S.

9.2 Rappresentazione di sottospazi vettoriali di $\mathbb{K}^n$

Diamo due modi di rappresentare un sottospazio vettoriale V di $\mathbb{K}^n$: una rappresentazione *parametrica* di V, dove i vettori di V si ottengono al variare in $\mathbb{K}$ di alcuni parametri liberi; e una rappresentazione *cartesiana* di V, dove i vettori di V sono le soluzioni di un sistema lineare omogeneo.

Sia V un sottospazio vettoriale di $\mathbb{K}^n$, sia $s = \dim(V)$, e sia $B = \{\underline{v}_1, \dots, \underline{v}_s\}$ una base di V, con

$$\underline{v}_1 = (v_1^1, v_1^2, \dots, v_1^n),\ \underline{v}_2 = (v_2^1, v_2^2, \dots, v_s^n),\ \dots,\ \underline{v}_s = (v_s^1, v_s^2, \dots, v_s^n).$$

Allora $V = L(\underline{v}_1, \dots, \underline{v}_s)$, e quindi il vettore $\underline{x} = (x_1, \dots, x_n) \in \mathbb{K}^n$ appartiene a V se e solo se $\underline{x} = \alpha_1\underline{v}_1 + \cdots + \alpha_s\underline{v}_s$ per qualche $\alpha_1, \dots, \alpha_s \in \mathbb{K}$, cioè se e solo se

$$(x_1, \dots, x_n) = \alpha_1(v_1^1, v_1^2, \dots, v_1^n) + \alpha_2(v_2^1, v_2^2, \dots, v_2^n) + \cdots + \alpha_s(v_s^1, v_s^2, \dots, v_s^n).$$

Scrivendolo in forma di sistema, questo ci dà delle *equazioni parametriche* di V :

$$\begin{cases} x_1 = \alpha_1 v_1^1 + \alpha_2 v_2^1 + \cdots + \alpha_s v_s^1 \\ x_2 = \alpha_1 v_1^2 + \alpha_2 v_2^2 + \cdots + \alpha_s v_s^2 \\ \vdots \\ x_n = \alpha_1 v_1^n + \alpha_2 v_2^n + \cdots + \alpha_s v_s^n \end{cases} \qquad \alpha_1, \dots, \alpha_s \in \mathbb{K}$$

Si noti che le equazioni cartesiane di V non sono uniche, perché dipendono dalla base B.

Ora, scriviamo una matrice $(s+1) \times n$ in cui la prima riga è un generico vettore $(x_1, \dots, x_n)$ di $\mathbb{K}^n$ e le altre righe formano una base B del sottospazio V :

$$A = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ v_1^1 & v_1^2 & \cdots & v_1^n \\ \vdots & \vdots & \ddots & \vdots \\ v_s^1 & v_s^2 & \cdots & v_s^n \end{pmatrix}$$

Le ultime s righe sono linearmente indipendenti; perciò, per il teorema di Kronecker, esiste un minore M $s \times s$ formato con le ultime s righe e con certe s colonne tale che $\det(M) \neq 0$. Inoltre $(x_1, \dots, x_n)$ appartiene a V se e solo se la prima riga di A è combinazione lineare delle altre, quindi se e solo se il rango di A è s (non cresce a $s+1$). Per il teorema di Kronecker, questo equivale a dire che tutti i minori orlati $(s+1) \times (s+1)$ di M hanno determinante zero.

Il numero di questi orlati è uguale al numero di colonne fuori da M, quindi è $n - s$. Chiamiamo $N_1(x_1, \dots, x_n), \dots, N_{n-s}(x_1, \dots, x_n)$ questi minori orlati; essi sono polinomi lineari omogenei in $x_1, \dots, x_n$. Quindi $(x_1, \dots, x_n)$ appartiene a V se e solo se

$$\begin{cases} N_1(x_1, \dots, x_n) = 0, \\ \vdots \\ N_{n-s}(x_1, \dots, x_n) = 0. \end{cases}$$

Questo sistema lineare omogeneo fornisce delle *equazioni cartesiane* di V. Si noti che la rappresentazione cartesiana di V non è unica, perché dipende dalla base B e dalla scelta del minore M.

9.3 Metodi di risoluzione per sistemi lineari

Vediamo ora due metodi per risolvere un sistema lineare compatibile.

Definizione 9.8. *Un* sistema di Cramer *è un sistema lineare $S : AX = B$ in cui la matrice incompleta $A \in \mathbb{K}^{n\times n}$ è quadrata e* $\det(A) \neq 0$.

Teorema 9.9. *Un sistema di Cramer $S : AX = B$ è determinato, e la soluzione è $\bar{X} = A^{-1}B$. Inoltre, se $\bar{X} = (\bar{x}_1, \dots, \bar{x}_n)$, allora per ogni $j = 1, \dots, n$ vale*

$$\bar{x}_j = \frac{\det(D_j)}{\det(A)},$$

dove $D_j \in \mathbb{K}^{n\times n}$ è la matrice ottenuta da A sostituendo alla j-esima colonna $A_{(j)}$ di A la colonna B dei termini noti.

Dimostrazione. Siano $A \in \mathbb{K}^{n\times n}$ e $C \in \mathbb{K}^{n\times(n+1)}$ le matrici incompleta e completa di S. Poichè $det(A) \neq 0$, allora $\mathrm{rk}(A) = n$; poichè $\mathrm{rk}(A) \leq \mathrm{rk}(C) \leq \min\{n, n+1\}$, questo implica $\mathrm{rk}(C)$. Quindi il sistema è compatibile per Rouché-Capelli, ed è determinato. Sia $\bar{X}$ la soluzione, cioè $A\bar{X} = B$. Moltiplicando entrambi i membri a sinistra per A^{-1} (che esiste perchè $\det(A) \neq 0$), si ottiene $\bar{X} = A^{-1}B$.

Ora, la j-esima componente $\bar{x}_j$ di $\bar{X}$ si ottiene come prodotto scalare tra la j-esima riga di A^{-1} e B. Quindi $\bar{x}_j$ è $\frac{1}{\det(A)}$ moltiplicato per il prodotto scalare tra la j-esima colonna dell'aggiunta $A^{\#}$ e B, e dunque

$$\bar{x}_j = \frac{1}{\det(A)} \sum_{i=1}^{n} A^i_j b_i.$$

Inoltre, la matrice D_j ha l'elemento b_i in posizione (i, j), e il suo complemento algebrico è uguale a A^i_j. Perciò $\bar{x}_j = \frac{1}{\det(A)} \cdot \det(D_j)$ per il teorema di Laplace applicato alla j-esima colonna di D_j. □

Il metodo di Cramer (cioè il calcolo della soluzione tramite le matrici D_j) permette di calcolare la soluzione in un sistema di Cramer $AX = B$ senza calcolare esplicitamente l'inversa A^{-1}.

Si noti che il teorema di Cramer si applica solo a sistemi di Cramer, e quindi determinati. Tuttavia, è possibile usare un metodo di "Cramer generalizzato" anche per risolvere sistemi compatibili e indeterminati, come segue:

- dato il sistema compatibile $S : AX = B$, se ne calcola il rango $r = \mathrm{rk}(A) = \mathrm{rk}(C)$;
- si ricava un sottosistema minimo equivalente a S tenendo solo r righe linearmente indipendenti di C;
- si identificano r colonne indipendenti nella matrice incompleta, si tengono a sinistra nel sistema le incognite corrispondenti $x_{i_1}, \dots, x_{i_r}$ e si porta a destra nel sistema le altre $n - r$ incognite, che diventano parametri indipendenti $\alpha_1, \dots, \alpha_{n-r}$, liberi di variare in $\mathbb{K}$;
- si applica il metodo di Cramer al sistema di Cramer così ottenuto nelle r incognite $x_{i_1}, \dots, x_{i_r}$; si noti che i "termini noti" di questo sistema, e quindi i determinanti delle matrici D_j, dipendono dai parametri $\alpha_1, \dots, \alpha_{n-r}$.

Descriviamo ora il secondo metodo risolutivo, detto *metodo di Gauss-Jordan*.

Esso si basa su quanto abbiamo osservato sopra: se operiamo trasformazioni elementari di riga sulla matrice completa C di un sistema lineare S, otteniamo la matrice completa C' di un sistema lineare S' equivalente a S.

Sia $S : AX = B$ un sistema lineare su $\mathbb{K}$ in n incognite, con matrice completa $C \in \mathbb{K}^{m\times(n+1)}$. Il metodo di Gauss-Jordan è il seguente.

1. Ridurre a gradini tramite operazioni elementari di riga la matrice completa C, ottenendo una matrice C'.
2. Sia r il numero di pivot di C'. Se tutti gli r pivot di C' si trovano nelle prime n colonne, allora S è compatibile, con ∞^{n-r} soluzioni; se invece C' ha un pivot nell'ultima colonna, allora S è incompatibile.
3. Supponiamo che S sia compatibile, e scriviamo il sistema S' associato a C'. Teniamo a sinistra le r "variabili pivotali" corrispondenti alle colonne dei pivot, e portiamo a destra le altre $n - r$ variabili, che diventano parametri liberi $\alpha_1, \dots, \alpha_{n-r} \in \mathbb{K}$.
4. Ricaviamo le variabili pivotali per "sostituzione all'indietro", partendo dall'ultima e sostituendone i valori nelle equazioni precedenti; oppure:

5. Riduciamo completamente a gradini la matrice C', e poi ricaviamo immediatamente il valore delle r variabili pivotali.

Esempio 9.10. *Consideriamo il sistema lineare in tre equazioni e tre incognite*

$$\begin{cases} x_1 + 2x_2 - x_3 = 1 \\ -x_1 + 4x_2 + 2x_3 = 0 \\ x_1 + 4x_3 = -1 \end{cases}.$$

La matrice completa associata a questo sistema è

$$C = \begin{pmatrix} 1 & 2 & -1 & 1 \\ -1 & 4 & 2 & 0 \\ 1 & 0 & 4 & -1 \end{pmatrix}.$$

Trasformiamo la matrice C in matrice completamente ridotta a gradini.

$$\begin{pmatrix} 1 & 2 & -1 & 1 \\ -1 & 4 & 2 & 0 \\ 1 & 0 & 4 & -1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 6 & 1 & 1 \\ 0 & -2 & 5 & -2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 1/6 & 1/6 \\ 0 & -2 & 5 & -2 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 1/6 & 1/6 \\ 0 & 0 & 16/3 & -5/3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 1/6 & 1/6 \\ 0 & 0 & 1 & -5/16 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 2 & 0 & 11/16 \\ 0 & 1 & 0 & 21/96 \\ 0 & 0 & 1 & -5/16 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 24/96 \\ 0 & 1 & 0 & 21/96 \\ 0 & 0 & 1 & -5/16 \end{pmatrix}.$$

Tutte le incognite sono pivotali, in quanto i pivot si trovano su tutte le prime tre colonne. Pertanto otteniamo un'unica soluzione data da

$$\left(\frac{1}{4}, \frac{7}{32}, -\frac{5}{16}\right).$$

Esempio 9.11. *Consideriamo adesso il sistema in tre incognite e due equazioni*

$$\begin{cases} x_1 + x_2 - x_3 = 10 \\ 2x_1 + x_2 + 4x_3 = -2 \end{cases}.$$

La matrice completa associata a questo sistema è

$$C = \begin{pmatrix} 1 & 1 & -1 & 10 \\ 2 & 1 & 4 & -2 \end{pmatrix}.$$

Trasformiamola completamente a gradini:

$$\begin{pmatrix} 1 & 1 & -1 & 10 \\ 2 & 1 & 4 & -2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & -1 & 10 \\ 0 & -1 & 6 & -22 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & -1 & 10 \\ 0 & 1 & -6 & 22 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 0 & 5 & -12 \\ 0 & 1 & -6 & 22 \end{pmatrix}.$$

In questo caso x_1 e x_2 sono incognite pivotali, mentre x_3 non lo è. Quindi x_3 sarà considerato come un parametro (diciamo λ). Le soluzioni sono dunque

$$\{(-12 - 5\lambda, 22 + 6\lambda, \lambda) \mid \lambda \in \mathbb{R}\}.$$

Esempio 9.12. *Consideriamo il sistema in tre equazioni e due incognite*

$$\begin{cases} x_1 + 4x_2 = 1 \\ -x_1 + 2x_2 = 0 \\ 2x_1 + 3x_2 = -1 \end{cases}.$$

La matrice completa associata a questo sistema è

$$C = \begin{pmatrix} 1 & 4 & 1 \\ -1 & 2 & 0 \\ 2 & 3 & -1 \end{pmatrix}.$$

La riduciamo completamente a gradini.

$$\begin{pmatrix} 1 & 4 & 1 \\ 0 & 6 & 1 \\ 0 & -5 & -3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & 1/6 \\ 0 & -5 & -3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & 1/6 \\ 0 & 0 & -13/6 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & 1/6 \\ 0 & 0 & 1 \end{pmatrix}.$$

Poiché la terza colonna (la colonna dei termini noti) contiene un pivot, il sistema non è compatibile.

9.4 Sistemi Lineari Parametrici

Definizione 9.13. *Un sistema lineare è detto* parametrico *se oltre alle incognite compaiono anche alcuni parametri che possono assumere determinati valori del campo $\mathbb{K}$.*

In generale un sistema parametrico è compatibile oppure no a seconda del valore del parametro. Pertanto va effettuata un'analisi caso per caso, al variare del parametro nell'insieme dei valori ammissibili (tipicamente, in tutto il campo $\mathbb{K}$). Il metodo di risoluzione di un sistema lineare parametrico può essere riassunto mediante il seguente schema.

- Numero equazioni: m.

- Numero incognite: n.

- Parametri: $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{K}$.

Metodo risolutivo

- $m \leq n$. In questo caso si prende una qualsiasi sottomatrice A' $m \times m$ della matrice incompleta tale che $\det(A') \neq 0$, oppure $\det(A')$ dipende in generale dai vari parametri. Sia $\det(A') = f(\lambda_1, \ldots, \lambda_r)$.

  1. I valori dei parametri tali che $f(\lambda_1, \ldots, \lambda_r) \neq 0$ sono tali che il rango della matrice dei coefficienti è m ed è massimo e quindi anche il rango della matrice completa è m. Pertanto il sistema è compatibile. Per trovare le soluzioni di questo sistema si costruisce il sistema equivalente le cui incognite e le equazioni sono quelle selezionate dalla matrice A'. Le altre incognite vengono portate dall'altra parte dell'uguale e diventeranno nuovi parametri. Il nuovo sistema è per costruzione un sistema di Cramer avendo per matrice dei coefficienti A' che ha determinante diverso da 0.

  2. I valori dei parametri tali che $f(\lambda_1, \ldots, \lambda_r) = 0$ vengono studiati a parte. Per questi valori il sistema può essere compatibile o incompatibile. Si procede prendendo altre possibili sottomatrici quadrate della matrice dei coefficienti.

- $m > n$. In questo caso si prende una qualsiasi sottomatrice C' $(n+1) \times (n+1)$ della matrice completa tale che il determinante è diverso da 0 oppure dipende in generale dai vari parametri. Sia $\det(C') = g(\lambda_1, \ldots, \lambda_r)$.

  1. I valori dei parametri tali che $g(\lambda_1, \ldots, \lambda_r) \neq 0$ sono tali che il rango della matrice completa è $n+1$, e quindi è maggiore del rango della matrice incompleta. Pertanto il sistema è incompatibile.

  2. I valori dei parametri tali che $g(\lambda_1, \ldots, \lambda_r) = 0$ vengono studiati a parte. Per questi valori il sistema può essere compatibile o incompatibile. Si procede prendendo altre possibili sottomatrici quadrate della matrice dei coefficienti.

9.5 Esercizi

Esercizio 9.1. *Risolvere mediante il metodo di eliminazione di Gauss i seguenti sistemi lineari.*

$$\begin{cases} x_1 - 4x_2 + x_3 = 2 \\ 2x_1 - 6x_2 + 5x_3 = 8 \\ x_1 - x_2 + 5x_3 = 8 \end{cases} \qquad \begin{cases} x + 2y + 3z = 6 \\ 2x - y + z = 2 \\ 3x + 8y + 10z = 20 \end{cases}$$

$$\begin{cases} x - y - z = 3 \\ 3x - 2y - 4z = 3 \\ 4x + y - 9z = 7 \end{cases} \qquad \begin{cases} x + 2y - 4z = 1 \\ 2x + 3y - 10z = 2 \\ 5x - 3y - 4z = 5 \end{cases}$$

Esercizio 9.2. *Risolvere i seguenti sistemi lineari discutendo la compatibilità del sistema utilizzando il Teorema di Rouché-Capelli.*

$$\begin{cases} x + y + 3z = 2 \\ 3x + 3y + 4z = 6 \\ x + y - z = -2 \end{cases} \qquad \begin{cases} 3x - 7y - z = -2 \\ 2x - 8y + z = -8 \\ x + y - 9z = -2 \\ x - 4y + 6z = -1 \\ 2x - 3y - 4z = 2 \end{cases}$$

$$\begin{cases} 2x - 3y - 2z = -4 \\ x + 4y - 11z = -1 \\ -5x + 9y - 11z = -3 \end{cases} \qquad \begin{cases} 3x_1 - 3x_2 + 2x_3 + x_4 - 6x_5 = -1 \\ 2x_1 - 2x_2 - 4x_3 + 6x_4 + 7x_5 = 5 \\ 5x_1 - 5x_2 - 3x_3 + 8x_4 + 4x_5 = 6 \end{cases}$$

$$\begin{cases} 3x_1 - 3x_2 + x_3 + 2x_4 - 6x_5 = -2 \\ 5x_1 - 5x_2 + 2x_3 + 3x_4 + 3x_5 = 10 \\ x_1 - x_2 + 5x_3 - 4x_4 - 4x_5 = 2 \\ x_1 - x_2 + 3x_3 - 2x_4 - 5x_5 = -1 \\ 3x_1 - 3x_2 - 5x_3 + 8x_4 + 2x_5 = 0 \end{cases}$$

Esercizio 9.3. *Stabilire se il seguente sistema lineare ammette soluzione ed eventualmente determinarle.*

$$\begin{cases} 3x + 4y - 2z + 6t = 3 \\ x + 3y + 4z - 2t = 0 \\ -x + 2y - z + t = 1 \end{cases} .$$

Soluzione. Per prima cosa è necessario scrivere la matrice dei coefficienti e quella completa, per poi andarne a calcolare i rispettivi ranghi.

$$\mathbf{A} = \begin{pmatrix} 3 & 4 & -2 & 6 \\ 1 & 3 & 4 & -2 \\ -1 & 2 & -1 & 1 \end{pmatrix} \qquad \mathbf{A}|\mathbf{b} = \begin{pmatrix} 3 & 4 & -2 & 6 & 3 \\ 1 & 3 & 4 & -2 & 0 \\ -1 & 2 & -1 & 1 & 1 \end{pmatrix}$$

L'esercizio 8.1 mostra che il rango della matrice $\mathbf{A}$ è 3. Il rango della matrice $\mathbf{A}|\mathbf{b}$ è anch'esso 3, in quanto non è possibile estrarre una matrice 4×4 da essa ed inoltre contiene la stessa

sottomatrice quadrata di $\mathbf{A}$ che ne ha determinato il rango. Quindi il sistema è compatibile. Per determinare le soluzioni, non essendo il sistema direttamente di Cramer, non possiamo applicare la formula. Tuttavia, essendo il sistema compatibile esiste una sottomatrice di $\mathbf{A}$ con determinante diverso da 0 che ne determina il rango. Questa matrice seleziona delle righe e delle colonne. Nel nostro caso, essendo la matrice $\mathbf{A_1}$ dell'esercizio 8.1 formata dalle tre righe della matrice e dalle prime tre colonne, il sistema di partenza è equivalente al seguente

$$\begin{cases} 3x + 4y - 2z = 3 - 6t \\ x + 3y + 4z = +2t \\ -x + 2y - z = 1 - t \end{cases}$$

dove l'incognita t è diventata un parametro. Ora possiamo interpretare il sistema come un sistema in 3 sole incognite e tre equazioni. Inoltre il nuovo sistema è di Cramer in quanto la matrice dei coefficienti è $\mathbf{A_1}$. Perciò, con il metodo di Cramer generalizzato, si ha

$$x = \frac{\det \begin{pmatrix} 3-6t & 4 & -2 \\ 2t & 3 & 4 \\ 1-t & 2 & -1 \end{pmatrix}}{\det(\mathbf{A_1})} \quad y = \frac{\det \begin{pmatrix} 3 & 3-6t & -2 \\ 1 & 2t & 4 \\ -1 & 1-t & -1 \end{pmatrix}}{\det(\mathbf{A_1})}$$

$$z = \frac{\det \begin{pmatrix} 3 & 4 & 3-6t \\ 1 & 3 & 2t \\ -1 & 2 & 1-t \end{pmatrix}}{\det(\mathbf{A_1})}.$$

Una volta calcolato il valore (che dipende da t) delle incognite x, y, z è possibile scrivere l'insieme delle soluzioni (x, y, z, t) del sistema lineare di partenza. Si lascia per esercizio il calcolo esplicito di queste soluzioni.

Esercizio 9.4. *Studiare, e se possibile risolvere con il metodo di Gauss-Jordan, i seguenti sistemi lineari a coefficienti reali:*

$$\begin{cases} x_1 - 2x_2 + x_3 = 0 \\ 3x_1 + 2x_2 - x_3 = 1 \\ 2x_1 + 4x_2 - 2x_3 = 1 \\ 5x_1 + 6x_2 - 3x_3 = 2 \end{cases}, \qquad \begin{cases} x_1 + 2x_2 + x_3 = 0 \\ x_2 + x_4 = 1 \\ x_1 + x_2 + x_3 - x_4 = -1 \end{cases},$$

$$\begin{cases} x_1 + x_2 - 3x_3 = 1 \\ x_1 + 3x_2 + x_3 = 4 \\ 2x_1 + 4x_2 - 2x_3 = -5 \end{cases}, \qquad \begin{cases} x_1 + 2x_4 = 2 \\ x_2 + x_3 - 6x_4 = -1 \\ x_1 + x_3 - 3x_4 = 2 \\ 2x_1 + x_2 + 2x_3 - 7x_4 = 3 \end{cases}.$$

Esercizio 9.5. *Studiare, e se possibile risolvere con il metodo di Cramer o Cramer generalizzato, i seguenti sistemi reali:*

$$\begin{cases} x_1 - x_3 + x_4 = 0 \\ x_2 + 2x_3 = 1 \\ 3x_1 + 4x_3 + 2x_4 = 0 \\ x_4 = 0 \\ 4x_1 + x_2 + 5x_3 + 4x_4 = 2 \end{cases} \qquad \begin{cases} -x_1 - x_3 = 0 \\ x_2 - x_3 = 0 \\ 2x_1 + x_2 + x_3 = -1 \\ x_1 + 2x_2 - x_3 = -1 \end{cases} \quad , \quad \begin{cases} x_1 - x_4 = -1 \\ 2x_1 + x_3 - x_4 = 1 \\ -x_1 + x_2 + x_4 = 0 \\ x_2 - x_3 + x_4 = 1 \\ x_1 + x_2 + x_3 = 1 \end{cases}$$

Esercizio 9.6. *Studiare, al variare del parametro reale h, i seguenti sistemi lineari*

$$\begin{cases} hx + 2y = 4 \\ 5x + y = 2 \end{cases} \qquad \begin{cases} x + y - z = 1 \\ 2x - y + z = 0 \\ x - 2y + 2z = h \end{cases} \qquad \begin{cases} x_1 + x_2 - hx_3 = 0 \\ x_1 - x_2 + x_3 = 1 \\ 2x_2 - 3x_3 = -1 \end{cases} \qquad \begin{cases} 2x - hy = 3 \\ 3x + y = 0 \end{cases}$$

e in caso di compatibilità, determinarne le soluzioni.

Esercizio 9.7. *Studiare, al variare $h \in \mathbb{R}$, il sistema lineare quadrato di ordine 3 a coefficienti reali $AX = B$, dove*

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

Per i valori di h per cui il sistema risulta determinato, si determini la soluzione.

Esercizio 9.8. *Studiare al variare di $h, k \in \mathbb{R}$, e quando possibile risolvere, il seguente sistema lineare reale:*

$$\begin{cases} x_1 + 2x_2 + hx_3 = 1 \\ 2x_1 + hx_2 + 8x_3 = 1 \\ 4x_1 + 7x_2 + x_3 = k \end{cases}$$

Esercizio 9.9. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} x + 3y = 0 \\ 3x - y = k - 1 \\ kx - 2ky = 1 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Soluzione.

La matrice dei coefficienti e quella completa sono

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

Poiché la matrice C è quadrata, partiamo con il calcolare il suo determinante. Si ha

$$\det(C) = (k-2)(k+1).$$

Abbiamo quindi due casi:
$\det(C) \neq 0$: corrisponde a $k \neq 2$ e $k \neq -1$. In questo caso il rango della matrice C è 3. Poiché il rango della matrice A è al massimo 2, il sistema non è compatibile, per il Teorema di Rouché-Capelli, avendo le matrici rango differente.
$\det(C) = 0$: corrisponde a $k = 2$ oppure $k = -1$.

1. Caso $k = 2$: le matrici diventano

$$A_2 = \begin{pmatrix} 1 & 3 \\ 3 & -1 \\ 2 & -4 \end{pmatrix} \qquad C_2 = \begin{pmatrix} 1 & 3 & 0 \\ 3 & -1 & 1 \\ 2 & -4 & 1 \end{pmatrix}.$$

   Si vede facilmente che il rango delle due matrici è pari a 2, poiché hanno in comune la sottomatrice $\begin{pmatrix} 1 & 3 \\ 3 & -1 \end{pmatrix}$ che ha determinante diverso da 0. Il sistema è dunque compatibile ed è equivalente al sistema

$$\begin{cases} x + 3y = 0 \\ 3x - y = 1 \end{cases}$$

   La soluzione di questo sistema è la seguente

$$x = \frac{3}{10} \quad y = -\frac{1}{10}.$$

   Quindi le soluzioni del sistema di partenza sono in questo caso

$$\mathcal{S}_2 = \left\{ \left(\frac{3}{10}, -\frac{1}{10} \right) \right\}.$$

2. Caso $k = -1$: le matrici diventano

$$A_{-1} = \begin{pmatrix} 1 & 3 \\ 3 & -1 \\ -1 & 2 \end{pmatrix} \qquad C_{-1} = \begin{pmatrix} 1 & 3 & 0 \\ 3 & -1 & -2 \\ -1 & 2 & 1 \end{pmatrix}.$$

Si vede facilmente che il rango delle due matrici è pari a 2, poiché hanno in comune la sottomatrice $\begin{pmatrix} 1 & 3 \\ 3 & -1 \end{pmatrix}$ che ha determinante diverso da 0. Il sistema è dunque compatibile ed è equivalente al sistema

$$\begin{cases} x + 3y = 0 \\ 3x - y = -2 \end{cases}$$

La soluzione di questo sistema è la seguente

$$x = -\frac{3}{5} \quad y = \frac{1}{5}.$$

Quindi le soluzioni del sistema di partenza sono in questo caso

$$\mathcal{S}_2 = \left\{ \left(-\frac{3}{5}, \frac{1}{5} \right) \right\}.$$

Esercizio 9.10. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} x + y = 3 \\ y - kx = k \\ kx + 2y = 0 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Soluzione.

La matrice dei coefficienti e quella completa sono

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

Poiché la matrice C è quadrata, partiamo con il calcolare il suo determinante. Si ha

$$\det(C) = k^2 - 6k - 3k - 2k = k^2 - 11k.$$

Abbiamo quindi due casi:
$\det(C) \neq 0$: corrisponde a $k \neq 0, 11$. In questo caso il rango della matrice C è 3. Poiché il rango della matrice A è al massimo 2, il sistema **non** è compatibile per il Teorema di Rouché-Capelli. $\det(C) = 0$: corrisponde a $k = 0$ oppure $k = 11$.

Nel primo caso ($k = 0$) le due matrici diventano:

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

Sappiamo già che il rango della matrice C non è 3. Inoltre la sottomatrice

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

ha determinante $1 \neq 0$ e quindi il rango di C è uguale a quello di A essendo entrambi 2. Dunque il sistema è compatibile. Per determinare le soluzioni basta osservare che il sistema è equivalente a

$$\begin{cases} x + y = 3 \\ y = 0 \end{cases}$$

Questo sistema è un sistema di Cramer. Anche senza utilizzare la formula risolutiva per tali sistemi è facile determinare che l'unica soluzione è $(3, 0)$. Quindi le soluzioni del sistema di partenza sono in questo caso

$$\mathcal{S}_0 = \{(3, 0)\}.$$

Nel secondo caso ($k = 11$) le due matrici diventano:

$$A = \begin{pmatrix} 1 & 1 \\ -11 & 1 \\ 11 & 2 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 1 & 3 \\ -11 & 1 & 11 \\ 11 & 2 & 0 \end{pmatrix}.$$

Sappiamo già che il rango della matrice C non è 3. Inoltre la sottomatrice

$$\begin{pmatrix} 1 & 1 \\ -11 & 1 \end{pmatrix}$$

ha determinante $12 \neq 0$ e quindi il rango di C è uguale a quello di A essendo entrambi 2. Dunque il sistema è compatibile. Per determinare le soluzioni basta applicare il Teorema di Cramer al sistema

$$\begin{cases} x + y = 3 \\ -11x + y = 11 \end{cases}$$

La soluzione è la seguente

$$x = \frac{\det \begin{pmatrix} 3 & 1 \\ 11 & 1 \end{pmatrix}}{12} \quad x = \frac{\det \begin{pmatrix} 1 & 3 \\ -11 & 11 \end{pmatrix}}{12}$$

Quindi le soluzioni del sistema di partenza sono in questo caso

$$\mathcal{S}_{11} = \left\{ \left(-\frac{2}{3}, \frac{11}{3} \right) \right\}.$$

Esercizio 9.11. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} x - y + z = 1 \\ x + ky = 0 \\ kx + y + z = k - 1 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Soluzione.

La matrice dei coefficienti e quella completa sono

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & k & 0 \\ k & 1 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & k & 0 & 0 \\ k & 1 & 1 & k-1 \end{pmatrix}.$$

Poiché la matrice A è quadrata, partiamo con il calcolare il suo determinante. Si ha

$$\det(A) = -k^2 + k + 2.$$

Abbiamo quindi due casi:

$\det(A) \neq 0$: corrisponde a $k \neq -1, 2$. In questo caso il rango della matrice A è 3. Poiché il rango della matrice C è al massimo 3, il sistema è compatibile per il Teorema di Rouché-Capelli, avendo entrambe le matrici rango pari a 3. Inoltre possiamo applicare il Teorema di Cramer. L'**unica** soluzione è pertanto

$$x = \frac{\det \begin{pmatrix} 1 & -1 & 1 \\ 0 & k & 0 \\ k-1 & 1 & 1 \end{pmatrix}}{-k^2 + k + 2} = \frac{-k^2 + 2k}{-k^2 + k + 2} = \frac{k}{k+1}$$

$$y = \frac{\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ k & k-1 & 1 \end{pmatrix}}{-k^2 + k + 2} = \frac{-1}{k+1}$$

$$z = \frac{\det \begin{pmatrix} 1 & -1 & 1 \\ 1 & k & 0 \\ k & 1 & k-1 \end{pmatrix}}{-k^2 + k + 2} = \frac{0}{-k^2 + k + 2}$$

e quindi

$$S_k = \left\{ \left(\frac{k}{k+1}, \frac{-1}{k+1}, 0 \right) \right\}.$$

$\det(A) = 0$: corrisponde a $k = -1$ oppure $k = 2$.

Nel primo caso ($k = -1$) le due matrici diventano:

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ -1 & 1 & 1 & -2 \end{pmatrix}.$$

Sappiamo già che il rango della matrice A non è 3. Inoltre la sottomatrice di A

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

ha determinante $1 \neq 0$ e quindi il rango di A è due. Inoltre la sottomatrice di C

$$\begin{pmatrix} -1 & 1 & 1 \\ -1 & 0 & 0 \\ 1 & 1 & -2 \end{pmatrix}$$

ha determinante $-3 \neq 0$ e quindi C ha rango 3. Il sistema non è dunque compatibile per il Teorema di Rouché-Capelli.

Nel secondo caso ($k = 2$) le due matrici diventano:

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 2 & 0 \\ 2 & 1 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 1 \end{pmatrix}.$$

Sappiamo già che il rango della matrice A non è 3. Inoltre la sottomatrice di A

$$\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$$

ha determinante $3 \neq 0$ e quindi il rango di A è due. È facile verificare che tutte le sottomatrici 3×3 di C hanno determinante 0, pertanto anche il rango di $\overline{A}$ è 2. Il sistema è dunque compatibile ed è equivalente al sistema

$$\begin{cases} x - y = 1 - z \\ x + 2y = 0 \end{cases}$$

La soluzione di questo sistema è la seguente

$$x = \frac{2(1-z)}{3} \quad y = \frac{z-1}{3}.$$

Quindi le soluzioni del sistema di partenza sono in questo caso

$$\mathcal{S}_2 = \left\{ \left(\frac{2(1-z)}{3}, \frac{z-1}{3}, z \right) \text{ t.c. } z \in \mathbb{R} \right\}.$$

Esercizio 9.12. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} 2x - y + z = 1 \\ kx + (k+1)z = 1 \\ y + 2z = 0 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Soluzione. La matrice dei coefficienti e quella completa sono

$$A = \begin{pmatrix} 2 & -1 & 1 \\ k & 0 & k+1 \\ 0 & 1 & 2 \end{pmatrix} \qquad C = \begin{pmatrix} 2 & -1 & 1 & 1 \\ k & 0 & k+1 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix}.$$

Poiché la matrice A è quadrata, partiamo con il calcolare il suo determinante. Si ha

$$\det(A) = k - 2.$$

Abbiamo quindi due casi:
$\det(A) \neq 0$: corrisponde a $k \neq 2$. In questo caso il rango della matrice A è 3. Poiché il rango della matrice C è al massimo 3, il sistema è compatibile per il Teorema di Rouché-Capelli, avendo entrambe le matrici rango pari a 3. Inoltre possiamo applicare il Teorema di Cramer. L'**unica** soluzione è pertanto

$$x = \frac{\det \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & k+1 \\ 0 & 1 & 2 \end{pmatrix}}{k-2} = \frac{-k+2}{k-2} = -1$$

$$y = \frac{\det \begin{pmatrix} 2 & 1 & 1 \\ k & 1 & k+1 \\ 0 & 0 & 2 \end{pmatrix}}{k-2} = \frac{-2k+4}{k-2} = -2$$

$$z = \frac{\det \begin{pmatrix} 2 & -1 & 1 \\ k & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}{-k-2} = \frac{k-2}{k-2} = 1$$

e quindi

$$S_k = \{(-1, -2, 1)\}.$$

$\det(A) = 0$: corrisponde a $k = 2$. In questo caso le due matrici diventano:

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

Sappiamo già che il rango della matrice A non è 3. Inoltre la sottomatrice di A

$$\begin{pmatrix} 2 & -1 \\ 2 & 0 \end{pmatrix}$$

ha determinante $2 \neq 0$ e quindi il rango di A è due. È facile verificare che tutte le sottomatrici 3×3 di C hanno determinante 0, pertanto anche il rango di C è 2. Il sistema è dunque compatibile ed è equivalente al sistema

$$\begin{cases} 2x - y = 1 - z \\ 2x = 1 - 3z \end{cases}$$

La soluzione di questo sistema è la seguente

$$x = \frac{1 - 3z}{2} \quad y = -2z.$$

Quindi le soluzioni del sistema di partenza sono in questo caso

$$\mathcal{S}_2 = \left\{ \left(\frac{1 - 3z}{2}, -2z, z \right) \;\middle|\; z \in \mathbb{R} \right\}.$$

Esercizio 9.13. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x + 2y = 1 \\ -x + y = k \\ 3x - 2y = 0 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.14. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x - 3y = k \\ 2x + 3y = -k \\ kx - 2y = 1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.15. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} (2\lambda + 1)x + (\lambda + 1)y + 3\lambda z = \lambda \\ (2\lambda - 1)x + (\lambda - 2)y + (2\lambda - 1)z = \lambda + 1 \\ 3\lambda x + 2\lambda y + (4\lambda - 1)z = 1 \end{cases}.$$

al variare del parametro reale λ.

Esercizio 9.16. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x - 2y = k \\ x + ky = 1 \\ 2kx + 3y = 0 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.17. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x + y + z = 0 \\ kx - y + z = 1 \\ 3x + kz = 1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.18. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x - y + 3z = 0 \\ kx - z = 1 \\ x + (k+1)z = 1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.19. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x - (k+1)y + kz = 1 \\ y + z = 1 \\ (k-2)x - 3y + 4z = 1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.20. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} 2x + 3y - z + t = k - 2 \\ (k+2)x + 2(k+1)y - 2z + kt = 0 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.21. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} 3x - y + 2z - t = 1 \\ 2kx + 2y + (k-1)z + 2t = 0 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.22. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x+3y=0 \\ 3x-y=k-1 \\ kx-2ky=1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.23. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} 2x-y+z=1 \\ kx+(k+1)z=1 \\ y+2z=0 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.24. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x-3y+2z=0 \\ x+ky+4z=1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.25. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x-3y+2z=0 \\ x+ky+4z=1 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.26. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x-y-t=1 \\ kx-3y+(k-3)z-kt=k \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.27. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x-y+z=0 \\ y+kz=1 \\ kx+3kz=2 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.28. *Discutere ed eventualmente risolvere il sistema lineare*

$$\begin{cases} x-y=1 \\ 2kx+(k-1)y=k \\ 2x+3y=0 \end{cases}.$$

al variare del parametro reale k.

Esercizio 9.29. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} x + kz = 1 \\ x + (k-1)y + (k+1)z = 1 \\ x + (k-1)y + (k^2+4k+3)z = k+3 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Soluzione. La matrice dei coefficienti è

$$A_k = \begin{pmatrix} 1 & 0 & k \\ 1 & k-1 & k+1 \\ 1 & k-1 & k^2+4k+3 \end{pmatrix}$$

ed ha determinante $(k+1)(k-1)(k+2)$. Se $k \neq 0, 1, -4$ allora il sistema è di Cramer e la sua unica soluzione è data da

$$x = \frac{\begin{vmatrix} 1 & 0 & k \\ 1 & k-1 & k+1 \\ k+3 & k-1 & k^2+4k+3 \end{vmatrix}}{k(k-1)(k+4)} = \frac{(k+2)(k-1)}{(k+1)(k-1)(k+2)} = \frac{1}{k+1},$$

$$y = \frac{\begin{vmatrix} 1 & 1 & k \\ 1 & 1 & k+1 \\ 1 & k+3 & k^2+4k+3 \end{vmatrix}}{k(k-1)(k+4)} = \frac{-(k+2)}{(k+1)(k-1)(k+2)} = \frac{-1}{(k+1)(k-1)}$$

$$z = \frac{\begin{vmatrix} 1 & 0 & 1 \\ 1 & k-1 & 1 \\ 1 & k-1 & k+3 \end{vmatrix}}{k(k-1)(k+4)} = \frac{(k+2)(k-1)}{(k+1)(k-1)(k+2)} = \frac{1}{k+1}.$$

Pertanto

$$\mathcal{S}_k = \left\{ \left(\frac{1}{k+1}, \frac{-1}{(k+1)(k-1)}, \frac{1}{k+1} \right) \right\}.$$

Consideriamo $k = 1$. Allora

$$A_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 2 \\ 1 & 0 & 8 \end{pmatrix}$$

ha rango 2 mentre

$$C_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 0 & 8 & 4 \end{pmatrix}$$

ha rango 3: il sistema non è compatibile.

Se $k = -1$, allora

$$A_{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -2 & 0 \\ 1 & -2 & 0 \end{pmatrix}, \quad C_{-1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & -2 & 0 & 1 \\ 1 & -2 & 0 & 2 \end{pmatrix}$$

hanno rango rispettivamente 2 e 3: il sistema non è compatibile. Infine consideriamo il caso $k = -2$. Le matrici

$$A_{-2} = \begin{pmatrix} 1 & 0 & -2 \\ 1 & -3 & -1 \\ 1 & -3 & 0-1 \end{pmatrix}, \quad C_{-2} = \begin{pmatrix} 1 & 0 & -2 & 1 \\ 1 & -3 & -1 & 1 \\ 1 & -3 & -1 & 1 \end{pmatrix}$$

hanno entrambe rango 2. Il sistema pertanto è compatibile. Le sue soluzioni sono $x = 2z+1$ e $y = 0$. Dunque le soluzioni del sistema iniziale in questo caso sono

$$\mathcal{S}_{-2} = \{(2z + 1, 0, z) \ : \ z \in \mathbb{R}\}.$$

Esercizio 9.30. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} x + 2w = 1 \\ x + y + 3z + 2w = 1 \\ 2x + y + (k + 2)z + 4w = 2 \\ x + y + 3z + (k^2 - k + 2)w = k \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Esercizio 9.31. *Stabilire per quali valori del parametro reale k il sistema lineare*

$$\begin{cases} x - y - t = 1 \\ kx - 3y + (k - 3)z - kt = k \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Esercizio 9.32. *Stabilire per quali valori del parametro h il seguente sistema*

$$\begin{cases} x - 2y + z = 1 \\ hx - 2y + (h + 1)z = h - 2 \\ 2x + 3z = 0 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Esercizio 9.33. *Stabilire per quali valori del parametro t il seguente sistema*

$$\begin{cases} -tx + (t-1)y + z = 1 \\ (t-1)y + tz = 1 \\ 2x + z = 5 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Esercizio 9.34. *Stabilire per quali valori del parametro k il seguente sistema*

$$\begin{cases} kx + y + z = -1 \\ 4x + 2y = -k \\ 6x + 3y + kz = -3 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Esercizio 9.35. *Stabilire per quali valori del parametro k il seguente sistema*

$$\begin{cases} x + y + kz = 2 \\ x + y + 3z = k - 1 \\ 2x + ky - z = 1 \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Esercizio 9.36. *Stabilire per quali valori del parametro a il seguente sistema*

$$\begin{cases} (2a-2)x + 2y - z = 0 \\ x + ay + z = 0 \\ 4ax + (4a+2)y + (2a+1)z = a^2 + a \end{cases}$$

ammette soluzioni ed eventualmente determinarle.

Capitolo 10

Funzioni lineari

10.1 Definizioni

Definizione 10.1. *Siano V e W due spazi vettoriali sullo stesso campo $\mathbb{K}$. Una funzione $L : V \to W$ è detta* funzione lineare *se*

- $L(u+v) = L(u) + L(v)$ *per ogni $u, v \in V$,*
- $L(\lambda u) = \lambda L(u)$ *per ogni $\lambda \in \mathbb{K}$ e per ogni $u \in V$.*

Esempio 10.2. *La seguente funzione $L : \mathbb{R}^3 \to \mathbb{R}^2$ è lineare:*

$$L((x, y, z)) = (3x + y, x - 2y).$$

Esempio 10.3. *La seguente funzione $L : \mathbb{R}^3 \to \mathbb{R}^2$ non è lineare:*

$$L((x, y, z)) = (3x + 4, x - 2y).$$

Esempio 10.4. *Data una matrice $A \in \mathbb{K}^{m \times n}$, la seguente funzione è lineare:*

$$L_A : \mathbb{K}^n \to \mathbb{K}^m, \quad L_A(X) = A \cdot X.$$

Osservazione 10.5. *Una funzione lineare $L : V \to W$ soddisfa $L(\underline{0}_V) = \underline{0}_W$.*
Infatti, scelto un vettore $u \in V$, si ha $L(\underline{0}_V) = L(0 \cdot u) = 0 \cdot L(u) = \underline{0}_W$.

Definizione 10.6. *Sia $L : V \to W$ una funzione lineare.*

- *Il* nucleo *di L è* $\mathrm{Ker}(L) := \{v \in V : L(v) = \underline{0}_W\}$.

- *L'*immagine *di* L *è* $\mathrm{Im}(L) := \{L(v) \colon v \in V\}$.

Proposizione 10.7. *Sia* $L : V \to W$ *una funzione lineare. Allora* $\mathrm{Ker}(L)$ *è un sottospazio vettoriale di* V *e* $\mathrm{Im}(L)$ *è un sottospazio vettoriale di* W.

Dimostrazione. Siano $u, v \in \mathrm{Ker}(L)$ e $\lambda \in \mathbb{K}$. Allora $L(u+v) = L(u) + L(v) = \underline{0}_W + \underline{0}_W = \underline{0}_W$, quindi $u + v \in \mathrm{Ker}(L)$; $L(\lambda v) = \lambda L(v) = \lambda \underline{0}_W = \underline{0}_W$, quindi $\lambda v \in \mathrm{Ker}(L)$.

Siano $w_1, w_2 \in \mathrm{Im}(L)$ e $\lambda \in \mathbb{K}$. Presi $v_1, v_2 \in V$ tali che $L(v_1) = w_1$ e $L_(v_2) = w_2$, si ha $L(v_1 + v_2) = L(v_1) + L(v_2) = w_1 + w_2$, quindi $w_1 + w_2 \in \mathrm{Im}(L)$; e $L(\lambda v_1) = \lambda L(v_1) = \lambda w_1$, quindi $\lambda w_1 \in \mathrm{Im}(L)$. □

Si noti che $\mathrm{Ker}(L)$ è la controimmagine di $\{\underline{0}_W\}$ $\mathrm{Ker}(L) = L^{-1}(\{\underline{0}_W\})$; mentre $\mathrm{Im}(L)$ è l'immagine di tutto V: $\mathrm{Im}(L) = L(V)$.

La precedente proposizione può essere generalizzata come segue.

Proposizione 10.8. *Sia* $L : V \to W$ *una funzione lineare.*

- *Se* U *è un sottospazio vettoriale di* V*, allora* $L(U)$ *è un sottospazio vettoriale di* W.
- *Se* Z *è un sottospazio vettoriale di* W*, allora* $L^{-1}(Z)$ *è un sottospazio vettoriale di* V.

Proposizione 10.9. *Sia* $f : V \to W$ *una funzione lineare. Se* $\{v_1, \ldots, v_n\}$ *è una base di* V*, allora* $\{f(v_1), \ldots, f(v_2)\}$ *è un sistema di generatori per* $\mathrm{Im}(f)$.

Dimostrazione. Sia $w \in \mathrm{Im}(f)$. Sia $v \in V$ una controimmagine di w, cioè tale che $f(v) = w$, e siano $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ tali che $v = \alpha_1 v_1 + \cdots \alpha_n v_n$. Allora

$$w = f(v) = f(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n) \in L(f(v_1), \ldots, f(v_n)).$$

Quindi $\mathrm{Im}(f) = L(f(v_1), \ldots, f(v_n))$ e la tesi è dimostrata. □

Per studiare l'iniettività di una funzione lineare basta studiare il suo nucleo:

Proposizione 10.10. *Sia* $f : V \to W$ *una funzione lineare. Allora* f *è iniettiva se e solo se* $\mathrm{Ker}(f) = \{\underline{0}_V\}$.

Dimostrazione. Sappiamo per quanto osservato sopra che $f(\underline{0}_V) = \underline{0}_W$, cioè $\underline{0}_V \in \mathrm{Ker}(f)$. Se f è iniettiva, allora chiaramente $\underline{0}_V$ è l'unica controimmagine di $\underline{0}_W$ e quindi $\mathrm{Ker}(f) = \{\underline{0}_V\}$. Viceversa, supponiamo che $\mathrm{Ker}(f) = \{\underline{0}_V\}$, e consideriamo due vettori $u, v \in V$ tali che $f(u) = f(v)$. Allora $f(u) - f(v) = \underline{0}_W$, da cui $f(u - v) = \underline{0}_W$, cioè $u - v \in \mathrm{Ker}(f) = \{\underline{0}_V\}$. Perciò $u - v = \underline{0}_V$ e quindi $u = v$. Allora f è iniettiva. □

Osservazione 10.11. *Più in generale, si ha che: se $f : V \to W$ è una funzione lineare e $w \in \mathrm{Im}(f)$, allora l'insieme controimmagine $f^{-1}(w) \subseteq V$ è in corrispondenza biunivoca con $\mathrm{Ker}(f)$ (e quindi $f^{-1}(w_1)$ e $f^{-1}(w_2)$ sono in corrispondenza biunivoca per ogni $w_1, w_2 \in \mathrm{Im}(f)$).*

Infatti, sia $\bar{v} \in f^{-1}(w)$ una fissata controimmagine di w. Allora, per ogni $u \in V$, si ha

$$u \in f^{-1}(w) \iff f(u) = w = f(\bar{v}) \iff f(u - \bar{v}) = \underline{0}_W$$

10.2 Teoremi fondamentali

Teorema 10.12 (Teorema della dimensione)**.** *Sia $f : V \to W$ una funzione lineare. Allora*

$$\dim V = \dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f).$$

Dimostrazione. Sia $n = \dim V$ e $h = \dim \mathrm{Ker}(f)$. Sia $\{v_1, \dots, v_h\}$ una base di $\mathrm{Ker}(f)$, e sia $\{v_1, \dots, v_h, u_1, \dots, u_{n-h}\}$ un suo completamento a una base di V. Per la proposizione precedente,

$$\mathrm{Im}(f) = L(f(v_1), \dots, f(v_h), f(u_1), \dots, f(u_{n-h}))$$

$$= L(\underline{0}_W, \dots, \underline{0}_W, f(u_1), \dots, f(u_{n-h})) = L(f(u_1), \dots, f(u_{n-h})).$$

Ci basta dimostrare che $f(u_1), \dots, f(u_{n-h})$ sono linearmente indipendenti, e così formeranno una base per $\mathrm{Im}(f)$, e la tesi sarà dimostrata.

Supponiamo per assurdo che $f(u_1), \dots, f(u_{n-h})$ siano linearmente dipendenti, e siano $\alpha_1, \dots, \alpha_{n-h} \in \mathbb{K}$ non tutti uguali a zero tali che $\alpha_1 f(u_1) + \dots + \alpha_{n-h} f(u_{n-h}) = \underline{0}_W$. Allora $f(\alpha_1 u_1 + \dots + \alpha_{n-h} u_{n-h}) = \underline{0}_V$, quindi $\alpha_1 u_1 + \dots + \alpha_{n-h} u_{n-h} \in \mathrm{Ker}(f)$ e dunque $\alpha_1 u_1 + \dots + \alpha_{n-h} u_{n-h} = \beta_1 v_1 + \dots + \beta_h v_h$ per qualche $\beta_1, \dots, \beta_h \in \mathbb{K}$. Allora abbiamo la combinazione lineare nulla $\beta_1 v_1 + \dots + \beta_h v_h - \alpha_1 u_1 - \dots - \alpha_{n-h} u_{n-h} = \underline{0}_V$ con coefficienti non tutti uguali a zero, che è assurdo perchè $\{v_1, \dots, v_h, u_1, \dots, u_{n-h}\}$ è linearmente indipendente in quanto base di V. □

Teorema 10.13 (Teorema di esistenza e unicità delle applicazioni lineari)**.** *Siano V e W due spazi vettoriali sullo stesso campo $\mathbb{K}$. Sia $\{v_1, \dots, v_n\}$ una base di V e siano $w_1, \dots, w_n$ vettori di W. Allora esiste una e una sola applicazione lineare $f : V \to W$ tale che $L(v_1) = w_1$, …, $L(v_n) = w_n$.*

Dimostrazione. Definiamo la funzione $f : V \to W$ tramite $f(u) = \alpha_1 w_1 + \dots + \alpha_n w_n$, dove $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ sono le componenti di u rispetto alla base ordinata $B = (v_1, \dots, v_n)$ di V

(cioè $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$). Osserviamo che f è una funzione ben definita, per l'esistenza e unicità delle componenti di un vettore rispetto a una base ordinata. Chiaramente si ha $f(v_1) = w_1, \ldots, f(v_n) = w_n$. Inoltre tale funzione f è lineare; infatti, presi $\lambda \in \mathbb{K}$ e $u, v \in V$ con le loro componenti $u \equiv_B (\alpha_1, \ldots, \alpha_n)$, $v \equiv_B (\beta_1, \ldots, \beta_n)$, si ha:

$$f(u+v) = f\left((\alpha_1 v_1 + \cdots + \alpha_n v_n) + (\beta_1 v_1 + \cdots + \beta_n v_n)\right)$$

$$= f((\alpha_1 + \beta_1)v_1 + \cdots + (\alpha_n + \beta_n)v_n) = (\alpha_1 + \beta_1)w_1 + \cdots (\alpha_n + \beta_n)w_n$$

$$= (\alpha_1 w_1 + \cdots \alpha_n w_n) + (\beta_1 w_1 + \cdots + \cdots \beta_n w_n) = f(u) + f(v),$$

e

$$f(\lambda u) = f(\lambda(\alpha_1 v_1 + \cdots + \alpha_n v_n)) = f((\lambda\alpha_1)v_1 + \cdots (\lambda\alpha_n)v_n)$$

$$= (\lambda\alpha_1)w_1 + \cdots + (\lambda\alpha_n)w_n = \lambda(\alpha_1 w_1 + \cdots + \alpha_n w_n) = \lambda f(u).$$

Quindi f è lineare. Per dimostrare l'unicità, supponiamo che $g : V \to W$ sia una funzione lineare tale che $g(v_1) = w_1, \ldots, g(v_n) = w_n$. Per ogni $u \in V$, se $u \equiv_B (\alpha_1, \ldots, \alpha_n)$, allora

$$g(u) = g(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \alpha_1 g(v_1) + \cdots + \alpha_n g(v_n)$$

$$= \alpha_1 w_1 + \cdots + \alpha_n w_n = \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n) = f(\alpha_1 v_1 + \cdots + \alpha_n v_n) = f(u).$$

Quindi $g(u) = f(u)$ per ogni $u \in V$, cioè $g = f$. □

Osservazione 10.14. *Ogni funzione lineare $f : \mathbb{K}^n \to \mathbb{K}^m$ è della forma $L_A : X \mapsto A \cdot X$ per qualche matrice $A \in \mathbb{K}^{m\times n}$, infatti:*

se $\{e_1, \ldots, e_n\}$ è la base canonica di $\mathbb{K}^n$ e $f(e_1) = w_1, \ldots, f(e_n) = w_n$, allora sia $A \in \mathbb{K}^{m\times n}$ la matrice che ha ordinatamente come colonne i vettori $w_1, \ldots, w_n$ di $\mathbb{K}^m$. Poichè il prodotto tra una matrice e l'i-esimo vettore della base canonica (visto come colonna) dà come risultato l'i-esima colonna della matrice, allora $L_A(e_i) = f(e_i)$ per ogni $i = 1, \ldots, n$. Quindi L_A e f coincidono sui vettori $e_1, \ldots, e_n$ della base canonica di $\mathbb{K}^n$. Per il teorema di esistenza e unicità dimostrato sopra, ciò implica $L_A = f$.

Osservazione 10.15. *Consideriamo una matrice $A \in \mathbb{K}^{m\times n}$ e la funzione lineare $L_A : \mathbb{K}^n \to \mathbb{K}^m$ definita da $L(X) = AX$. Poichè le colonne di A sono le immagini della base canonica, allora:*

- *le colonne di A sono un sistema di generatori per* $\mathrm{Im}(L_A)$*;*
- $\dim \mathrm{Im}(L_A) = \mathrm{rk}(A), \quad \dim \mathrm{Ker}(L_A) = n - \mathrm{rk}(A).$

Osservazione 10.16. *Siano V, W spazi vettoriali sullo stesso campo $\mathbb{K}$, con $\dim W \geq 1$. Siano $w_1, \ldots, w_h \in W$, e siano $v_1, \ldots, v_h \in V$. Dal teorema di esistenza e unicità segue che:*

- *se $\{v_1, \ldots, v_h\}$ è un insieme di vettori linearmente indipendenti ma non è una base di V, allora esiste ma non è unica la funzione lineare $f : V \to W$ tale che $f(v_1) = w_1, \ldots, f(v_h) = w_h$. Infatti, la funzione f è libera di assumere qualsiasi immagine sui vettori che completano $\{v_1, \ldots, v_h\}$ ad una base di V.*
- *Se $v_1, \ldots, v_h$ sono linearmente dipendenti ed esiste una funzione lineare $f : V \to W$ tale che $f(v_1) = w_1, \ldots, f(v_h) = w_h$, allora $w_1, \ldots, w_h$ devono soddisfare la stessa relazione di dipendenza lineare che soddisfano $v_1, \ldots, v_h$.*

10.3 Isomorfismi

Definizione 10.17. *Una funzione lineare $f : V \to W$ si dice:*

- *un* monomorfismo *se f è iniettiva;*
- *un* epimorfismo *se f è suriettiva;*
- *un* isomorfismo *se f è biettiva;*
- *un* endomorfismo *se $V = W$;*
- *un* automorfismo *se $V = W$ e f è biettiva.*

Esempio 10.18. *Sia V un $\mathbb{K}$-spazio vettoriale di dimensione n, e sia B una sua base ordinata. La funzione $f : V \to \mathbb{K}^n$ definita da $f(v) = (\alpha_1, \ldots, \alpha_n)$ se $v \equiv_B (\alpha_1, \ldots, \alpha_n)$, è un isomorfismo, detto* isomorfismo delle componenti *rispetto alla base ordinata B.*

Di facile dimostrazione è la seguente proposizione.

Proposizione 10.19.

- *Se $f : V \to W$ e $g : W \to Z$ sono funzioni lineari, allora la funzione composta $g \circ f : V \to Z$ è una funzione lineare.*
- *Se $f : V \to W$ è un isomorfismo, allora la funzione inversa $f^{-1} : W \to V$ è un isomorfismo.*

Teorema 10.20. *Sia $f : V \to W$ una funzione lineare tra spazi della stessa dimensione* $\dim V = \dim W$. *Allora*

$$f \text{ è biettiva} \iff f \text{ è iniettiva} \iff f \text{ è suriettiva.}$$

Dimostrazione. Per il teorema dimensionale, $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = \dim V$. Poichè sappiamo che f è iniettiva se e solo se $\dim \mathrm{Ker}(f) = 0$, allora f è iniettiva se solo se $\dim \mathrm{Im}(f) = \dim V = \dim W$. Poichè $\mathrm{Im}(f)$ è un sottospazio vettoriale di W, l'uguaglianza $\dim \mathrm{Im}(f) = \dim W$ si verifica se e solo se $\mathrm{Im}(f) = W$, cioè se e solo se f è suriettiva. Quindi f è iniettiva se e solo se è suriettiva, e quindi se e solo se è biettiva. □

Definizione 10.21. *Due $\mathbb{K}$-spazi vettoriali V, W si dicono* isomorfi *se esiste un isomorfismo $f : V \to W$.*

Teorema 10.22. *Due $\mathbb{K}$-spazi vettoriali V, W sono isomorfi se e solo se hanno la stessa dimensione.*

Dimostrazione. Se V e W sono isomorfi tramite un isomorfismo $f : V - W$, allora $\dim \mathrm{Ker}(f) = 0$ (perchè f è un monomorfismo) e $\dim \mathrm{Im}(f) = \dim W$ (perchè f è un epimorfismo); quindi dal teorema dimensionale segue $\dim V = \dim W$.

Viceversa, se V e W hanno la stessa dimensione n, prendiamo due basi ordinate B_V e B_W di V e W rispettivamente, e consideriamo gli isomorfismi delle componenti $c_{B_V} : V \to \mathbb{K}^n$ e $c_{B_W} : W \to \mathbb{K}^n$. Poichè l'inversa di un isomorfismo è un isomorfismo, e la composizione di isomorfismi è un isomorfismo, allora la funzione $(c_{B_W})^{-1} \circ c_{B_V} : V \to W$ è un isomorfismo, e quindi V e W sono isomorfi. □

10.4 Esercizi

Esercizio 10.1. *Sia $L : \mathbb{R}^3 \to \mathbb{R}^2$ data da $L(x, y, z) = (x + 2y + z, y + z)$.*

1. *Verificare che L è lineare.*
2. *Determinare una base di $Ker(L)$ e stabilire se L è iniettiva. Determinare una base di $Im(L)$.*
3. *Calcolare $w = L(2, 1, 3)$ e determinare $L^{-1}(w)$.*

Soluzione.

1. Siano (x_1, y_1, z_1), (x_2, y_2, z_2) elementi di $\mathbb{R}^3$ e $\lambda, \mu \in \mathbb{R}$. Allora

$$L\left(\lambda(x_1, y_1, z_1) + \mu(x_2, y_2, z_2)\right)$$

$$= L\left(\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2\right)$$

$$= (\lambda x_1 + \mu x_2 + 2(\lambda y_1 + \mu y_2) + \lambda z_1 + \mu z_2, \lambda y_1 + \mu y_2 + \lambda z_1 + \mu z_2)$$

$$= (\lambda x_1 + 2\lambda y_1 + \lambda z_1 + \mu x_2 + 2\mu y_2 + \mu z_2, \lambda y_1 + \lambda z_1 + \mu y_2 + \mu z_2)$$

$$= \lambda(x_1 + 2y_1 + z_1, y_1 + z_1) + \mu(x_2 + 2y_2 + z_2, y_2 + z_2)$$

$$= \lambda L\left(x_1, y_1, z_1\right) + \mu L\left(x_2, y_2, z_2\right)$$

   e pertanto L è lineare.

2. Il $Ker(L)$ è dato da

$$\{(x, y, z) \in \mathbb{R}^3 \mid x + 2y + z = y + z = 0\} = \{(\alpha, -\alpha, \alpha) \in \mathbb{R}^3 \mid \alpha \in \mathbb{R}\}$$

$$= \{\alpha(1, -1, 1) \mid \alpha \in \mathbb{R}\} = \langle(1, -1, 1)\rangle.$$

   Si vede chiaramente che $(1, -1, 1)$ è una base di $Ker(L)$. Poiché $Ker(L)$ non contiene solo $(0, 0, 0)$ allora L non è iniettiva.

   Poiché per il Teorema 10.12

$$\dim(Ker(L)) + \dim(Im(L)) = \dim(\mathbb{R}^3) = 3,$$

   allora $\dim(Im(L)) = 2$ e $Im(L) = \mathbb{R}^2$ e come base possiamo scegliere $(1, 0)$ e $(0, 1)$.

3. Si ha che $L(2, 1, 3) = (7, 4)$. Inoltre

$$L^{-1}(7, 4) = \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y + z = 7, y + z = 4\}$$

$$= \{(\alpha - 1, 4 - \alpha, \alpha) \mid \alpha \in \mathbb{R}\}.$$

Esercizio 10.2. *Siano*

$$v_1 = (0, 0, 2, -1), v_2 = (-1, 1, 2, 1), v_3 = (0, 1, 0, 2), v_4 = (0, 0, 0, 1) \in \mathbb{R}^4.$$

1. *Verificare che v_1, v_2, v_3, v_4 è base di $\mathbb{R}^4$.*

2. *Dimostrare che esiste un'unica* $L : \mathbb{R}^4 \to \mathbb{R}^4$ *tale che*

$$L(v_1) = L(v_2) = v_1 - v_3, L(v_3) = v_1, L(v_4) = \mathbf{0}.$$

Calcolare la matrice $A \in \mathbb{R}^{4\times 4}$ *tale che* $L(X) = A \cdot X$.

3. *Trovare basi di* $Ker(L)$ *e di* $Im(L)$.

Soluzione.

1. Poiché la dimensione di $\mathbb{R}^4$ è 4, basta controllare che i 4 vettori siano linearmente indipendenti, ovvero che il rango della matrice

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

sia 4. Si ha che

$$\det(A) = 1 \det \begin{pmatrix} 0 & 0 & 2 \\ -1 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix} = 1(-1) \det \begin{pmatrix} 0 & 2 \\ -1 & 2 \end{pmatrix} = 2 \neq 0.$$

2. Poiché v_1, v_2, v_3, v_4 costituisco una base di $\mathbb{R}^4$ tale applicazione lineare esiste ed è unica per il Teorema 10.13. Per costruire la matrice A dobbiamo calcolare

$$L(1,0,0,0), \quad L(0,1,0,0), \quad L(0,0,1,0), \quad L(0,0,0,1),$$

sapendo che

$$L(0,0,2,-1) = (0,-1,2,-3), \quad L(-1,1,2,1) = (0,-1,2,-3),$$

$$L(0,1,0,2) = (0,0,2,-1), \quad L(0,0,0,1) = (0,0,0,0).$$

Per ipotesi $L(0,0,0,1) = (0,0,0,0)$. Inoltre

$$\begin{aligned} L(0,1,0,0) = \quad & L(0,1,0,2) - 2L(0,0,0,1) \\ & = (0,0,2,-1) - 2(0,0,0,0) = (0,0,2,-1); \end{aligned}$$

$$\begin{aligned} L(0,0,1,0) = \quad & \tfrac{1}{2}L(0,0,2,-1) + \tfrac{1}{2}L(0,0,0,1) \\ & = \tfrac{1}{2}(0,-1,2,-3) + \tfrac{1}{2}(0,0,0,0) = \left(0,-\tfrac{1}{2},1,-\tfrac{3}{2}\right); \end{aligned}$$

$$\begin{aligned} L(1,0,0,0) = \quad & -L(-1,1,2,1) + L(0,1,0,0) \\ & +2L(0,0,1,0) + L(0,0,0,1) \\ & = (0,1,-2,3) + (0,0,2,-1) \\ & + (0,-1,2,-3) + (0,0,0,0) = (0,0,2,-1). \end{aligned}$$

Pertanto si ha

$$M_{\mathcal{C}}^{\mathcal{C}}(L) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & 0 \\ 2 & 2 & 1 & 0 \\ -1 & -1 & -\frac{3}{2} & 0 \end{pmatrix}.$$

3. Si ha che $Im(L)$ è generato da $\{(v_1), L(v_2), L(v_3), L(v_4)\}$. Quindi basta selezionare il massimo numero di vettori indipendenti tra $L(v_1), L(v_2), L(v_3), L(v_4)$ per ottenere una base di $Im(L)$. Si vede che tale numero è 2 e una base di $Im(L)$ è data da $(0,-1,2,-3), (0,0,2,-1)$. Per determinare il $Ker(L)$ si può osservare che $Ker(L) =$

$$\left\{(x,y,z,t) \in \mathbb{R}^4 \mid -\frac{1}{2}z = 0,\ 2x+2y+z = 0,\ -x-y-\frac{3}{2}z = 0\right\}$$

$$= \{(\alpha, -\alpha, 0, \beta) \mid \alpha, \beta \in \mathbb{R}\} = \langle (1,-1,0,0), (0,0,0,1) \rangle.$$

Dal Teorema 10.12 già sappiamo che la dimensione del $Ker(L)$ è 2, pertanto una base del $Ker(L)$ è data proprio da $(1,-1,0,0), (0,0,0,1)$.

Esercizio 10.3. *Sia $L : \mathbb{R}^4 \to \mathbb{R}^4$ definita da*

$$L(x,y,z,t) = (-x+z, -y+t, x-z, y-t).$$

Determinare la dimensione ed una base di $Ker(L)$ e di $Im(L)$.

Soluzione. Si ha che

$$Ker(L) = \{(x,y,z,t) \in \mathbb{R}^4 \mid -x+z = 0, y+t = 0,\ x-z = 0,\ y-t = 0\}$$

$$= \{(\alpha, \beta, \alpha, \beta) \mid \alpha, \beta \in \mathbb{R}\} = \langle (1,0,1,0), (0,1,0,1) \rangle.$$

Si vede facilmente che $(1,0,1,0), (0,1,0,1)$ sono linearmente indipendenti e pertanto costituiscono una base di $Ker(L)$. Dal Teorema 10.12 si ha che la dimensione di $Im(L)$ è anch'essa 2. Una sua base può essere selezionata tra i vettori

$$L(1,0,0,0) = (-1,0,1,0), \qquad L(0,1,0,0) = (0,-1,0,1),$$

$$L(0,0,1,0) = (1,0,-1,0), \qquad L(0,0,0,1) = (0,1,0,-1).$$

Si vede facilmente che $(-1,0,1,0)$ e $(0,-1,0,1)$ sono linearmente indipendenti e poiché sono 2 costituiscono una base di $Im(L)$.

Esercizio 10.4. *Determinare se esiste un'applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^2$, tale che*

$$L(1,1,1) = (3,0), L(0,2,-1) = (0,3),$$

$$L(2,0,0) = (0,0), L(1,0,1) = (3,1).$$

Soluzione. I vettori $(1,1,1), (0,2,-1), (2,0,0)$ costituiscono una base per $\mathbb{R}^3$, pertanto esiste un'unica applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^2$, tale che

$$L(1,1,1) = (3,0), \qquad L(0,2,-1) = (0,3), \qquad L(2,0,0) = (0,0).$$

Si ha che

$$(x,y,z) = \frac{y+2z}{3}(1,1,1) + \frac{y-z}{3}(0,2,-1) + \frac{3x-y-2z}{6}(2,0,0)$$

e dunque segue, per linearità

$$L(x,y,z) = \frac{y+2z}{3}L(1,1,1) + \frac{y-z}{3}L(0,2,-1) + \frac{3x-y-2z}{6}L(2,0,0)$$

$$= (y+2z, y-z)$$

Poiché $L(1,0,1) = (2,-1)$, l'applicazione cercata non esiste.

Esercizio 10.5. *Considerata l'applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^3$, definita da*

$$L(x,y,z) = (2x+y, y-z, x+z),$$

si provi che essa è un isomorfismo e se ne determini l'inversa.

Soluzione. Il nucleo di L coincide con lo spazio delle soluzioni del sistema lineare omogeneo

$$\begin{cases} 2x + y = 0 \\ y - z = 0 \\ x + z = 0 \end{cases}$$

e quindi $Ker(L) = \{(0,0,0)\}$ e L è iniettiva; per il Teorema 10.12 $\dim(Im(L))$ è 3 e pertanto è suriettiva e quindi un isomorfismo. Dato un vettore $(a,b,c) \in \mathbb{R}^3$ esiste quindi un unico vettore $(x,y,z) \in \mathbb{R}^3$ tale che

$$L(x,y,z) = (a,b,c) \qquad \Longleftrightarrow \qquad \begin{cases} 2x + y = a \\ y - z = b \\ x + z = c \end{cases}.$$

L'unica soluzione è data da $(a - b - c, -a + 2b + 2c, -a + b + 2c)$ quindi

$$L^{-1}(x,y,z) = (x - y - z, -x + 2y + 2z, -x + y + 2z).$$

Esercizio 10.6. *Determinare se esiste un'applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^3$ tale che*

$$L(1,0,0) = (4,5,-2), L(0,1,0) = (-2,-2,1),$$

$$L(1,0,-1) = (5,6,-3), L(1,3,0) = (-2,-1,1).$$

In caso affermativo studiare L.

Soluzione. I vettori $(1,0,0), (0,1,0), (1,0,-1)$ costituiscono una base di $\mathbb{R}^3$, pertanto esiste un'unica applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^3$ tale che

$$L(1,0,0) = (4,5,-2), L(0,1,0) = (-2,-2,1), L(1,0,-1) = (5,6,-3).$$

Dato $(x,y,z) \in \mathbb{R}^3$ si ha

$$(x,y,z) = (x+z)(1,0,0) + y(0,1,0) - z(1,0,-1),$$

quindi

$$\begin{aligned} L(x,y,z) &= (x+z)(4,5,-2) + y(-2,-2,1) - z(5,6,-3) \\ &= (4x - 2y - z, 5x - 2y - z, -2x + y + z). \end{aligned}$$

Poiché $L(1,3,0) = (-2,-1,1)$ il problema ha risposta positiva. Infine si noti che $Im(L) = \langle (4,5,-2), (-2,-2,1), (5,6,-3) \rangle$ che sono linearmente indipendenti e quindi $\dim(Im(L)) = 3$ e L è un isomorfismo.

Esercizio 10.7. *Verificare che l'applicazione lineare* $L : \mathbb{R}^3 \to \mathbb{R}^3$ *definita da*

$$L(x, y, z) = (x + 2y, 2x - y - z, 2y + 3z)$$

è invertibile e determinarne l'inversa.

Soluzione. Per ogni $(a, b, c) \in \mathbb{R}^3$

$$L(x, y, z) = (a, b, c) \qquad \Longleftrightarrow \qquad \begin{cases} x + 2y = a \\ 2x - y - z = b \\ 2y + 3z = c \end{cases} .$$

Il precedente sistema è di Cramer ed ammette come unica soluzione la terna

$$\left(\frac{a - 6b + 2c}{13}, \frac{6a + 3b - c}{13}, \frac{-4a - 2b + 5c}{13} \right).$$

Dunque

$$L^{-1}(x, y, z) = \left(\frac{x - 6y + 2z}{13}, \frac{6x + 3y - z}{13}, \frac{-4x - 2y + 5z}{13} \right).$$

Esercizio 10.8. *Sia* $L : \mathbb{R}^3 \to \mathbb{R}^3$ *l'applicazione lineare definita da*

$$L(e_1) = 2e_2 + 3e_3,\ L(e_2) = 2e_1 - 5e_2 - 8e_3,\ L(e_3) = -e_1 + 4e_2 + 6e_3,$$

essendo $\{e_1, e_2, e_3\}$ *la base canonica di* $\mathbb{R}^3$*. Determinare la matrice canonicamente associata a* $L^2 = L \circ L$*. Determinare inoltre il nucleo delle applicazioni* $L - id_{\mathbb{R}^3}$ *ed* $L^2 + id_{\mathbb{R}^3}$*.*

Esercizio 10.9. *Si considerino le applicazioni lineari* $f : \mathbb{R}^2 \to \mathbb{R}^3$ *definita da* $f(x, y) = (x, 2y, x + y)$ *e* $g : \mathbb{R}^3 \to \mathbb{R}^3$ *canonicamente associata alla matrice*

$$B = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 4 \\ 3 & 1 & 5 \end{pmatrix}.$$

Determinare una base di $Im(g \circ f)$*.*

Soluzione. L'applicazione lineare g è data da

$$g(x, y, z) = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 4 \\ 3 & 1 & 5 \end{pmatrix} (x, y, z)^T = (x + z, 2x + y + 4z, 3x + y + 5z).$$

Allora

$$g(f(x, y)) = g(x, 2y, x + y) = (2x + y, 6x + 6y, 8x + 7y).$$

Si ha

$$Im(g \circ f) = \{(2x + y, 6x + 6y, 8x + 7y) \mid x, y \in \mathbb{R}\} = \langle (2, 6, 8), (1, 6, 7) \rangle.$$

Si vede facilmente che $(2, 6, 8), (1, 6, 7)$ è una base di $Im(g \circ f)$ che quindi ha dimensione 2.

Esercizio 10.10. *Verificare che le relazioni*

$$L(1, 1, 1) = (-1, 2), \quad L(0, 1, 1) = (0, 4) \quad L(1, 1, 0) = (2, 1)$$

definiscono un'unica applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^2$.

- *Scrivere la matrice canonicamente associata a* L.
- *Trovare una base di* $Im(L)$ *e di* $Ker(L)$.

Esercizio 10.11. *Si consideri la seguente applicazione lineare*

$$L : \mathbb{R}^3 \to \mathbb{R}^3$$

definita da

$$L(x, y, z) = (kx, (k + 1)y + (k - 1)z, 2ky + 3kz).$$

Si stabilisca per quali valori del parametro k *l'applicazione* L *è iniettiva. Quando non è iniettiva si determini una base di* $Im(L)$ *e* $Ker(L)$.

Soluzione. La matrice canonicamente associata a L è

$$M = \begin{pmatrix} k & 0 & 0 \\ 0 & k + 1 & k - 1 \\ 0 & 2k & 3k \end{pmatrix}.$$

Il rango di tale matrice corrisponde alla dimensione di $Im(L)$. Pertanto il suo rango è 3 se e solo se $\dim(Im(L)) = 3$, se e solo se $\dim(Ker(L)) = 0$, se e solo se L è iniettiva.

Poiché $\det(M) = k(k^2 + 5k)$, l'applicazione L è iniettiva se e solo se $k \neq 0$ e $k \neq -5$.

- Se $k = 0$ allora

$$M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

e quindi l'immagine ha dimensione 1 ed è generata da $(0, 1, 0)$. Il $Ker(L)$ ha dimensione 2 e contiene tutti i vettori (x, y, z) tali che $y - z = 0$, e quindi una sua base è $(1, 0, 0), (0, 1, 1)$.

- Se $k = -5$ allora
$$M = \begin{pmatrix} -5 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & -10 & -15 \end{pmatrix}$$
e quindi l'immagine ha dimensione 2 ed è generata da $(1,0,0),(0,2,5)$. Il $Ker(L)$ ha dimensione 1 e contiene tutti i vettori (x,y,z) tali che $x = 0$ e $-4y - 6z = 0$, e quindi una sua base è $(0,3,-2)$.

Esercizio 10.12. *Sia $L : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione lineare definita da $L(x,y,z) = (x^2, y, 2z)$. Stabilire se L è lineare.*

Svolgimento. Se L fosse lineare in particolare dovrebbe accadere che $L(2v) = 2L(v) \forall v \in \mathbb{R}^3$. Sia $v = (1,0,0)$, si ha

$$L(v) = L(1,0,0) = (1,0,0) \Rightarrow 2L(v) = (2,0,0)$$

$$L(2v) = (4,0,0).$$

Quinidi $L(2v) \neq 2L(v)$, perció L non è lineare.

Esercizio 10.13. *Determinare una applicazione lineare $L : \mathbb{R}^2 \to \mathbb{R}^2$ tale che*

$$L(1,1) = (1,2), L(0,2) = (4,4).$$

Svolgimento. Scriviamo il generico elemento $(x,y) \in \mathbb{R}^2$ come combinazione lineare degli elementi di cui conosciamo l'immagine (che formano una base di $\mathbb{R}^2$): $(1,1),(0,2)$. Dobbiamo quindi risolvere l'equazione

$$(x,y) = a(1,1) + b(0,2) \Rightarrow \begin{cases} a = x \\ a + 2b = y \end{cases} \Rightarrow \begin{cases} a = x \\ b = \frac{-x+y}{2} \end{cases}.$$

Quindi

$$(x,y) = x(1,1) + \frac{-x+y}{2}(0,2),$$

essendo L lineare per ipotesi risulta

$$L(x,y) = xT(1,1) + \frac{-x+y}{2}T(0,2) + = x(1,2) + \frac{-x+y}{2}(4,4)$$

$$= (x,2x) + (-2x+2y, -2x+2y) = (-x+2y, 2y).$$

Esercizio 10.14. *Sia $L : \mathbb{R}^2 \to \mathbb{R}^3$ l'applicazione definita da $L(x,y) = (x+y, 2x, x-y)$.*

1. *Verificare che L è lineare;*
2. *Determinare Nucleo e Immagine di L.*

Svolgimento. 1. Dobbiamo verificare che

$$L(v_1 + v_2) = L(v_1) + L(v_2),\ \forall\ v_1, v_2 \in \mathbb{R}^2$$

$$L(\lambda v) = \lambda L(v),\ \forall\ \lambda \in \mathbb{R}, \forall v \in \mathbb{R}^2$$

Siano $v_1 = (x_1, y_1), v_2 = (x_2, y_2)$, allora

$$L(v_1 + v_2) = L(x_1 + x_2, y_1 + y_2) = (x_1 + x_2 + y_1 + y_2, 2x_1 + 2x_2, x_1 + x_2 - y_1 - y_2)$$

$$\begin{aligned} L(v_1) + L(v_2) &= (x_1 + y_1, 2x_1, x_1 - y_1) + (x_2 + y_2, 2x_2, x_2 - y_2) \\ &= (x_1 + x_2 + y_1 + y_2, 2x_1 + 2x_2, x_1 + x_2 - y_1 - y_2). \end{aligned}$$

Quindi la prima proprietà è verificata. Analogamente

$$L(\lambda v) = L(\lambda x, \lambda y) = (\lambda x + \lambda y, 2\lambda x, \lambda x - \lambda y)$$

$$\lambda L(v) = \lambda(x + y, 2x, x - y) = (\lambda x + \lambda y, 2\lambda x, \lambda x - \lambda y),$$

anche la seconda proprietà è verificata.
2. Per definizione sappiamo che

$$Ker(L) = \{v \in \mathbb{R}^2 | L(v) = 0\} = \{(x, y)\mathbb{R}^2 | (x + y, 2x, x - y) = (0, 0, 0\} \subseteq \mathbb{R}^2.$$

Pertanto dobbiamo cercare le soluzioni del sistema omogeneo:

$$\begin{cases} x + y = 0 \\ 2x = 0 \\ x - y = 0 \end{cases} \Rightarrow \begin{cases} x = 0 \\ y = 0 \end{cases} \Rightarrow Ker(L) = \{(0, 0)\}.$$

Analogamente

$$\begin{aligned} Im(L) &= \{L(v) | v \in \mathbb{R}^2\} \\ &= \{(x + y, 2x, x - y) | x, y \in \mathbb{R} \\ &= \{(1, 2, 1)x + (1, 0, -1)y | x, y \in \mathbb{R} \\ &= \langle (1, 2, 1), (1, 0, -1) \rangle. \end{aligned}$$

A questo punto per trovare una base di $Im(L)$ dobbiamo studiare la dipendenza lineare dei generatori. Poichè

$$\operatorname{rk} \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 1 & -1 \end{pmatrix} = 2,$$

i generatori di $Im(L)$ sono lineramente indipendenti, quindi costituiscono una base.

Esercizio 10.15. *Sia $L : \mathbb{R}^2 \to \mathbb{R}^3$ l'applicazione definita sulla base canonica $\{e_1, e_2\}$ di $\mathbb{R}^2$ nel seguente modo: $L(e_1) = (1, 2, 1), L(e_2) = (1, 0, -1)$.*

1. *Esplicitare $L(x, y)$;*
2. *Determinare la matrice A canonicamente associata a L.*

Svolgimento. 1. Sia $v = (x, y)$ un generico vettore di $\mathbb{R}^2$, si può esprimere come $v = x \cdot e_1 + y \cdot e_2$. Per la linearità di L abbiamo

$$L(v) = x \cdot L(e_1) + y \cdot L(e_2) = x \cdot (1, 2, 1) + y \cdot (1, 0, -1) = (x + y, 2x, x - y)$$

2. La matrice associata A è la matrice che ha per colonne le immagini della base canonica di $\mathbb{R}^2$. Avendo già $T(e_1)$ e $T(e_2)$ è immediato ricavare:

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 1 & -1 \end{pmatrix}.$$

Esercizio 10.16. *Sia $T : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione tale che*

$$L(x, y, z) = (x + y, kx + y + z, kx + y + kz)$$

con $k \in \mathbb{R}$.

1. *Determinare la matrice A canonicamente associata a T rispetto alla base canonica;*
2. *Determinare la dimensione e una base dello spazio vettoriale $Im(T) \subseteq \mathbb{R}^3$ al variare di k.*

Svolgimento. 1. Dobbiamo calcolare le immagini dei vettori della base canonica:

$$T(1, 0, 0) = (1, k, k)$$

$$T(0, 1, 0) = (1, 1, 1)$$

$$T(0, 0, 1) = (0, 1, k),$$

quindi

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

2. Per determinare la dimensione e una base dell'immagine di L riduciamo la matrice a gradini

$$A = \begin{pmatrix} 1 & 1 & k \\ k & 1 & 1 \\ k & 1 & k \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & k \\ 0 & 1-k & 1 \\ 0 & 0 & k-1 \end{pmatrix}.$$

Quindi distinguiamo i due casi:

- $k \neq 1$ la matrice ha rango 3, di conseguenza i tre vettori sono linearmente indipendenti e una base di $Im(L)$ è quindi $\{(1,k,k),(1,1,1),\ (0,1,k)\}$.
- $k = 1$ la matrice ha rango 2. In particolare risultano linearmente indipendenti la prima e terza colonna della matrice. Quindi dim $(Im(L)) = 2$ e una base è $\{(1,1,1),(0,1,k)\}$.

Capitolo 11

Autovalori e diagonalizzazione

11.1 Autovalori e autovettori

Definizione 11.1. *Sia V un $\mathbb{K}$-spazio vettoriale e sia $f : V \to V$ un endomorfismo di V.*

- *Uno scalare $\lambda \in \mathbb{K}$ si dice un* autovalore *di f se esiste un vettore non nullo $v \in V$ tale che $f(v) = \lambda v$.*
- *Un vettore $v \in V$ si dice un* autovettore *di f se esiste uno scalare $\lambda \in \mathbb{K}$ tale che $f(v) = \lambda v$.*
- *Se $\lambda \in \mathbb{K}$ è un autovalore di f e $v \in V$ soddisfa $f(v) = \lambda v$, allora v è detto un autovettore relativo a all'autovalore λ; se inoltre $v \neq 0$, λ è detto l'autovalore relativo all'autovettore v.*
- *Se $\lambda \in \mathbb{K}$ è un autovalore di f, allora $V_\lambda(f) := \{v \in V \colon f(v) = \lambda v\}$ è detto l'*autospazio *relativo all'autovalore λ.*

Se A è una matrice in $\mathbb{K}^{n\times n}$, chiamiamo autovalori, autovettore, autospazi di A quelli dell'endomorfismo canonicamente associato ad A, cioè $f_A : \mathbb{K}^n \to \mathbb{K}^n$, $X \mapsto A \cdot X$.

Quindi $\lambda \in \mathbb{K}$ è un autovalore di $A \in \mathbb{K}^{n\times n}$ se esiste un vettore non nullo $X \in \mathbb{K}^n$ tale che $AX = \lambda X$; in tal caso, X è detto un autovettore relativo all'autovalore λ. L'insieme $V_\lambda(A) := \{X \in \mathbb{K}^n \colon AX = \lambda X\}$ è detto autospazio reativo all'autovalore λ.

Proposizione 11.2. *Sia $f : V \to V$ un endomorfismo e $\lambda \in \mathbb{K}$ un suo autovalore. Allora l'autospazio $V_\lambda(f)$ è un sottospazio vettoriale di V, di dimensione maggiore di zero.*

Dimostrazione. Poichè $f(\underline{0}) = \underline{0} = \lambda\underline{0}$, allora $\underline{0} \in V_\lambda(f)$. Se $v_1, v_2 \in V_\lambda(f)$, allora $f(v_1 + v_2) = f(v_1) + f(v_2) = \lambda v_1 + \lambda v_2 = \lambda(v_1 + v_2)$, e quindi $v_1 + v_2 \in V_\lambda(f)$. Se $v \in V_\lambda(f)$ e $\mu \in \mathbb{K}$, allora $f(\mu v) = \mu f(v) = \mu(\lambda v) = \lambda(\mu v)$, e quindi $\mu v \in V_\lambda(f)$. Perciò $V_\lambda(f)$ è un sottospazio vettoriale di V. Per definizione di autovalore, $V_\lambda(f)$ contiene almeno un vettore non nullo, e quindi ha dimensione positiva. □

Osservazione 11.3. *Mentre ci sono diversi autovettori relativi ad uno stesso autovalore λ (tutti gli elementi del suo autospazio), l'autovalore relativo ad un autovettore non nullo è unico. Infatti, se $f(v) = \lambda_1 v$ e $f(v) = \lambda_2 v$ con $v \neq \underline{0}$, allora $(\lambda_1 - \lambda_2)v = \underline{0}$, da cui $\lambda_1 + \lambda_2 = 0$ perchè $v \neq \underline{0}$; e quindi $\lambda_1 = \lambda_2$.*

Proposizione 11.4. *Autovettori non nulli relativi ad autovalori distinti sono linearmente indipendenti.*

Dimostrazione. Facciamo la dimostrazione solo nel caso di due vettori. Siano dunque v_1, v_2 autovettori non nulli relativi rispettivamente agli autovalori λ_1, λ_2 con $\lambda_1 \neq \lambda_2$. Supponiamo per assurdo che v_1 e v_2 siano linearmente dipendenti. Allora, ricordando che $v_1 \neq \underline{0}$ $v_2 \neq \underline{0}$, la lineare dipendenza implica che $v_2 = \alpha v_1$ per qualche $\alpha \in \mathbb{K}$ con $\alpha \neq 0$. Allora, usando la linearità di f, si ha $f(v_2) = f(\alpha v_1) = \alpha f(v_1) = \alpha(\lambda_1 v_1)$; d'altra parte, si ha $f(v_2) = \lambda_2 v_2 = \lambda_2(\alpha v_1) = \alpha(\lambda_2 v_1)$. Da $\alpha(\lambda_1 v_1) = \alpha(\lambda_2 v_1)$ segue $\lambda_1 v_1 = \lambda_2 v_1$ perchè $\alpha \neq 0$, e quindi $\lambda_1 = \lambda_2$ perché $v_1 \neq \underline{0}$. Questo è una contraddizione, e quindi la tesi è dimostrata (nel caso di due autovettori non nulli). □

Data una matrice $A \in \mathbb{K}^{n\times n}$, si dice *polinomio caratteristico* di A il seguente polinomio a coefficienti in $\mathbb{K}$:

$$p_A(x) := \det(A - xI_n).$$

L'equazione algebrica $p_A(x) = 0$ è detta *equazione caratteristica* di A

Osservazione 11.5. *Il polinomio caratteristico $p_A(x)$ di una matrice $A \in \mathbb{K}^{n\times n}$ ha grado n. Quindi l'equazione $p_A(x) = 0$ ha al più n soluzioni in $\mathbb{K}$, contate con molteplicità.*

Proposizione 11.6. *Sia $A \in \mathbb{K}^{n\times n}$. Gli autovalori in $\mathbb{K}$ di A sono le soluzioni in $\mathbb{K}$ dell'equazione caratteristica $p_A(x) = 0$.*

Dimostrazione. Uno scalare $\lambda \in \mathbb{K}$ è un autovalore di A se e solo se esiste un vettore non nullo $X \in \mathbb{K}^n$ tale che $AX = \lambda X = \lambda I_n X$, cioè se e solo se il sistema lineare omogeneo $(A - \lambda I_n)X = \underline{0}$ ammette altre soluzioni oltre a quella nulla. Poiché il sistema ha n incognite,

questo accade se e solo se $A-\lambda I_n$ ha rango minore di n; cioè, se e solo se $\det(A-\lambda I_n)=0$, che è equivalente a chiedere che λ sia una soluzione dell'equazione caratteristica $p_A(x)=0$. $\square$

Definizione 11.7. *Sia $\lambda \in \mathbb{K}$ un autovalore di $A \in \mathbb{K}^{n\times n}$.*

- *Si dice* molteplicità algebrica *di λ, e si indica con $m.a.(\lambda)$, la molteplicità di λ come soluzione dell'equazione caratteristica, cioè il più grande numero intero positivo $m \geq 1$ tale che $(x-\lambda)^m$ divide $p_A(x)$.*

- *Si dice* molteplicità geometrica *di λ, e si indica con $m.g.(\lambda)$, la dimensione* $\dim V_\lambda \geq 1$ *dell'autospazio V_λ relativo a λ.*

Si noti che, se $\lambda \in \mathbb{K}$ è un autovalore di $A \in \mathbb{K}^{n\times n}$, allora il suo autospazio V_λ è l'insieme delle soluzioni del sistema omogeneo $(A-\lambda I_n)X = \underline{0}$.

In altre parole, V_λ è il nucleo della funzione lineare $\mathbb{K}^n \to \mathbb{K}^n$, $X \mapsto (A-\lambda I_n)X$. Perciò:

$$m.g.(\lambda) = n - \mathrm{rk}(A-\lambda I_n).$$

Osservazione 11.8. *Lo scalare $\lambda = 0$ è un autovalore della matrice A se e solo se* $\det(A) = 0$.

Il seguente risultato mette in relazione la molteplicità algebrica di un autovalore con la sua molteplicità geometrica; ne omettiamo la dimostrazione.

Proposizione 11.9. *Sia $\lambda \in \mathbb{K}$ un autovalore della matrice $A \in \mathbb{K}^{n\times n}$. Allora:*

$$1 \leq m.g.(\lambda) \leq m.a.(\lambda) \leq n.$$

In particolare, si noti che un autovalore con molteplicità algebrica 1 ha anche molteplicità geometrica 1.

Definizione 11.10. *$A \in \mathbb{K}^{n\times n}$ si dice una matrice* a spettro semplice *se A ha n autovalori distinti in $\mathbb{K}$.*

Equivalentemente, una matrice $n \times n$ su $\mathbb{K}$ è a spettro semplice se e solo se $p_A(x)$ ha n zeri distinti in $\mathbb{K}$.

11.2 Matrici diagonalizzabili

Definizione 11.11. *Date due matrici quadrate $A, B \in \mathbb{K}^{n\times n}$, si dice che A è simile a B se esiste una matrice invertibile $E \in \mathbb{K}^{n\times n}$ tale che $E^{-1}AE = B$.*

Osservazione 11.12. *Si dimostra facilmente che la relazione di similitudine tra matrici di $\mathbb{K}^{n\times n}$ è una relazione di equivalenza (riflessiva, simmetrica, transitiva) su $\mathbb{K}^{n\times n}$.*

Proposizione 11.13. *Due matrici simili hanno lo stesso determinante, lo stesso polinomio caratteristico, gli stessi autovalori con le stesse molteplicità algebriche e gometriche.*

Dimostrazione. Se $E^{-1}AE = B$ per qualche matrice invertibile $E \in \mathbb{K}^{n\times n}$, allora $p_B(x) = \det(E^{-1}AE - xI_n) = \det(E^{-1}AE - E^{-1}xI_nE) = \det(E^{-1}(A - xI_n)E) = \det(E^{-1})\det(A - xI_n)\det(E) = \det(E)^{-1}p_A(x)\det(E) = p_A(x)$. Dall'uguaglianza dei polinomi caratteristici segue anche l'uguaglianza degli autovalori e delle loro molteplicità algebriche; ne segue anche l'uguaglianza dei determinanti (ponendo $x = 0$). Lasciamo non dimostrata l'uguaglianza delle molteplicità geometriche. □

Definizione 11.14. *Una matrice $A \in \mathbb{K}^{n\times n}$ si dice* diagonalizzabile (per similitudine) *se è simile a una matrice diagonale; cioè se esistono una matrice invertibile $E \in \mathbb{K}^{n\times n}$ e una matrice diagonale $D \in \mathbb{K}^{n\times n}$ tali che $E^{-1}AE = D$.*

In tal caso, la matrice E è detta una matrice diagonalizzante*, o* che diagonalizza *A.*

Teorema 11.15. *Sia data una matrice $A \in \mathbb{K}^{n\times n}$, e siano $\lambda_1, \ldots, \lambda_h \in \mathbb{K}$ tutti i suoi autovalori distinti in $\mathbb{K}$. Allora le seguenti proprietà sono equivalenti:*

1. *A è diagonalizzabile;*
2. *esiste una* base spettrale *rispetto ad A, cioè una base di $\mathbb{K}^n$ fatta di auttovettori di A;*
3. *$\sum_{i=1}^{h} m.g.(\lambda_i) = n$.*

Se tali proprietà sono verificate: una matrice $E \in \mathbb{K}^{n\times n}$ diagonalizza A se e solo se le colonne di E formano una base spettrale rispetto ad A; in tal caso, $E^{-1}AE = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$, dove α_i è l'autovalore corrispondente all'autovettore che sta nella colonna i-esima di E.

Dimostrazione. Supponiamo che valga la proprietà (1), cioè che A sia diagonalizzabile, e scriviamo $E^{-1}AE = D$, con $E \in \mathbb{K}^{n\times n}$ invertibile e $D \in \mathbb{K}^{n\times n}$ diagonale. Si noti che l'invertibilità di E è equivalente alla condizione $\det(E) \neq 0$, che vale se e solo se $\mathrm{rk}(E) = n$;

ciò è equivalente a chiedere che le n colonne di E siano linearmente indipendenti, e quindi che le colonne di E formino una base di $\mathbb{K}^n$.

Moltiplicando a sinistra per E entrambi i membri dell'uguaglianza $E^{-1}AE = D$, si ottiene l'uguaglianza equivalente $AE = ED$. Si noti ora che la i-esima colonna di AE si ottiene come prodotto $AE_{(i)}$ tra A e la i-esima colonna $E_{(i)}$ di E. Poichè D è diagonale, la i-esima colonna di ED è uguale al prodotto $d_{ii}E_{(i)}$ tra l'i-esimo elemento $d_{ii} \in \mathbb{K}$ sulla diagonale di D e $E_{(i)}$. Perciò vale l'uguaglianza $AE_{(i)} = d_{ii}E_{(i)}$. Quindi $\{E_{(1)}, \ldots, E_{(n)}\}$ è una base di $\mathbb{K}^n$ spettrale rispetto ad A, con autovalori corrispondenti $d_{11}, \ldots, d_{nn}$ rispettivamente.

Viceversa, supponiamo che valga la proprietà (2). Sia $B = \{v_1, \ldots, v_n\}$ una base di $\mathbb{K}^n$ spettrale per A, con autovalori corrispondenti $\mu_1, \ldots, \mu_n$ rispettivamente. Allora possiamo costruire una matrice E scegliendo v_i come i-esima colonna, e una matrice diagonale $D = \mathrm{diag}(\mu_1, \ldots, \mu_n)$. La matrice E è invertibile (perché ha rango n), e ragionando come sopra si ha $AE = ED$. Quindi $E^{-1}AE = D$, e vale la proprietà (1). Perciò le proprietà (1) e (2) sono equivalenti.

Ora, consideriamo tutti gli autovalori distinti $\lambda_1, \ldots, \lambda_h$ in $\mathbb{K}$ di A, e per ciascuno dei relativi autospazi $V_{\lambda_1}, \ldots, V_{\lambda_h}$ consideriamo una base; chiamiamo queste basi $B_1, \ldots, B_h$ rispettivamente. Sia $B := B_1 \cup \cdots \cup B_h$ l'unione delle basi di tutti gli autospazi. Usando la proposizione 11.4, si ha che B è linearmente indipendente. Inoltre, il numero di vettori in B è $|B_1| + \cdots + |B_h| = \sum_{i=1}^{h} m.g.(\lambda_i)$. Poichè B è un insieme di vettori linearmente indipendenti in $\mathbb{K}^n$, il numero di vettori in B è minore o uguale a n. Quindi $\sum_{i=1}^{h} m.g.(\lambda_i) \leq n$. Se vale la proprietà (3), cioè $\sum_{i=1}^{h} m.g.(\lambda_i) = n$, allora B è un insieme di n autovettori linearmente indipendenti, quindi è una base spettrale rispetto ad A, e vale la proprietà (2). Viceversa, supponiamo che valga la proprietà (2) e sia $\tilde{B}$ una base di $\mathbb{K}^n$ spettrale rispetto ad A. Per ogni autovalore $\lambda_i \in \mathbb{K}$ di A e relativo autospazio V_{λ_i}, possiamo costruire una base di V_{λ_i} che contenga tutti gli autovettori in $\tilde{B}$ che sono relativi all'autovalore λ_i; perciò, $m.g.(\lambda_i)$ è maggiore o uguale al numero di autovettori in $\tilde{B}$ relativi all'autovalore λ_i. Sommando per $i = 1, \ldots, h$, si ottiene $\sum_{i=1}^{h} m.g.(\lambda_i) \geq |\tilde{B}| = n$. Poichè $m.g.(\lambda_i) \leq m.a.(\lambda_i)$ e $\sum_{i=1}^{h} m.a.(\lambda_i)$, allora vale anche la disuguaglianza opposta $\sum_{i=1}^{h} m.g.(\lambda_i) \leq n$. Unendo le due disuguaglianze, otteniamo la proprietà (3): $\sum_{i=1}^{h} m.g.(\lambda_i) = n$. Il teorema è completamente dimostrato. □

Se $A \in \mathbb{K}^{n \times n}$ è una matrice a spettro semplice, allora A è diagonalizzabile: infatti, se A ha n autovalori distinti $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$, allora essi hanno tutti molteplicità algebrica 1, e quindi per la proposizione 11.9 anche tutte le molteplicità geometriche sono uguali a 1.

Osservazione 11.16. *Il teorema precedente mostra come procedere per diagonalizzare una matrice $A \in \mathbb{K}^{n\times n}$:*

- *Calcolare il polinomio caratteristico $p_A(x)$.*
- *Calcolare gli autovalori in $\mathbb{K}$ di A e le relative molteplicità algebriche.*
- *Se $p_A(x)$ non ha tutte le radici in $\mathbb{K}$ (cioè, se la somma delle molteplicità algebriche degli autovalori in $\mathbb{K}$ è minore di n), allora A non è diagonalizzabile; se invece la somma delle molteplicità algebriche degli autovalori in $\mathbb{K}$ è uguale a n, allora procedere.*
- *Calcolare tutte le molteplicità geometriche $m.g.(\lambda) = n - \mathrm{rk}(A - \lambda I_n)$ degli autovalori $\lambda \in \mathbb{K}$.*
- *Se qualche molteplicità geometrica è strettamente minore della corrispondente molteplicità algebrica, allora A non è diagonalizzabile; altrimenti, tutte le molteplicità geometriche sono uguali alle corrispondenti molteplicità algebriche, e A è diagonalizzabile. In tal caso, procedere.*
- *Per ogni autovalore $\lambda \in \mathbb{K}$, trovare una base dell'autospazio V_λ, cioè delle soluzioni del sistema omogeneo $(A - \lambda I_n)X = \underline{0}$.*
- *Mettere i vettori delle basi degli autospazi come colonne di una matrice $E \in \mathbb{K}^{n\times n}$.*
- *Costruire una matrice diagonale D, mettendo all'i-esimo posto della diagonale principale l'autovalore corrispondente all'autovettore che sta nella i-esima colonna di E.*
- *A è simile alla matrice diagonale D tramite la matrice E, cioè: $E^{-1}AE = D$.*

11.3 Matrici reali ortogonalmente diagonalizzabili

In questo capitolo, il campo considerato sarà sempre quello dei numeri reali: $\mathbb{K} = \mathbb{R}$.

Definizione 11.17. *Una matrice quadrata $P \in \mathbb{R}^{n\times n}$ si dice* ortogonale *se è invertibile con inversa uguale alla trasposta: $P^{-1} = P^T$.*

Esempio 11.18. *La matrice*

$$P = \begin{pmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 0 & 1 & 0 \end{pmatrix}$$

è una matrice ortogonale. Infatti, si verifica facilmente che $P \cdot P^T = P^T \cdot P = I_3$*, e quindi* P *è invertibile con inversa* $P^{-1} = P^T$*.*

Proposizione 11.19. *Data una matrice* $P \in \mathbb{R}^{n\times n}$*, le seguenti proprietà sono equivalenti:*

- P *è una matrice ortogonale;*
- *le righe di* P *formano una base ortonormale di* $\mathbb{R}^n$*;*
- *le colonne di* P *formano una base ortonormale di* $\mathbb{R}^n$*.*

Dimostrazione. L'elemento a^i_j di posto (i, j) in $P \cdot P^T$ è uguale al prodotto scalare tra la riga i-esima $P^{(i)}$ di P e la colonna j-esima di P^T, che è la riga j-esima $P^{(j)}$ di P; quindi $a^i_j = \langle P^{(i)}, P^{(j)}\rangle$. D'altra parte, l'elemento di posto (i, j) in I_n è 1 se $i = j$, 0 se $i \neq j$. Ne segue che $P \cdot P^T = I_n$ se e solo se le righe di P formano una base ortonormale di $\mathbb{R}^n$. Allo stesso modo, si ha che $P^T \cdot P = I_n$ se e solo se le colonne di P formano una base ortonormale di $\mathbb{R}^n$. □

Definizione 11.20. *Una matrice* $A \in \mathbb{R}^{n\times n}$ *si dice* ortogonalmente diagonalizzabile *(o* diagonalizzabile per congruenza*) se è diagonalizzabile ed esiste una matrice ortogonale che la diagonalizza; cioè, se esiste una matrice invertibile* $P \in \mathbb{R}^{n\times n}$ *tale che* $P^{-1} = P^T$ *e* $P^T AP$ *è una matrice diagonale.*

Osservazione 11.21. *Il fatto che una matrice* A *sia ortogonalmente diagonalizzabile significa che esiste una matrice ortogonale che diagonalizza* A*, non significa che ogni matrice che diagonalizza* A *è ortogonale.*

Se una matrice invertibile $E \in \mathbb{R}^{n\times n}$ *è tale che* $E^{-1}AE$ *è una matrice diagonale* D*, quello che sappiamo è solo che le colonne di* E *formano una base di* $\mathbb{R}^n$ *fatta di autovettori per* A*, e che sulla diagonale principale di* D *abbiamo i corrispondenti autovalori.*

Si vede facilmente che, se $A \in \mathbb{R}^{n\times n}$ è ortogonalmente diagonalizzabile, allora A è simmetrica. Infatti, se P è una matrice ortogonale e D è una matrice diagonale tali che $P^T AP = D$, allora $(P^T AP)^T = D^T$, che implica $P^T A^T P = D$; dunque $P^T AP = P^T AP$, da cui, moltiplicando a sinistra per P e a destra per P^T, si ottiene $A = A^T$.

In realtà vale anche il viceversa (non lo dimostriamo), cioé: una matrice reale simmetrica è ortogonalmente diagonalizzabile. Riassumiamo tutto nel seguente teorema

Teorema 11.22. (Teorema spettrale) *Sia* $A \in \mathbb{R}^{n\times n}$*. Le seguenti proprietà sono equivalenti:*

- *A è simmetrica;*
- *A è ortogonalmente diagonalizzabile;*
- *esiste una base ortonormale di $\mathbb{R}^n$ fatta di autovettori per A.*

Osservazione 11.23. *Per diagonalizzare ortogonalmente una matrice reale simmetrica $A \in \mathbb{R}^{n\times n}$ bisogna procedere come segue.*

- *Trovare autovalori e autospazi, e la matrice D diagonale simile ad A (come nella diagonalizzazione per similitudine).*
- *Autovettori relativi ad autovalori diversi di A sono già ortogonali. Quindi, quello che occorre è trovare, per ciascun autospazio, una sua base ortogonale (cioè fatta da vettori a due a due ortogonali).*
- *Unendo le basi ortogonali di ciascun autospazio, si ottiene una base ortogonale $\{v_1, \dots, v_n\}$ di $\mathbb{R}^n$ fatta di autovettori.*
- *Dividendo ciascun vettore v_i per la sua norma, si ottiene una base ortonormale $B = \{\frac{1}{||v_1||}v_1, \dots, \frac{1}{||v_n||}v_n\}$ di autovettori.*
- *Si mette i vettori di B come colonne di una matrice P (in posizione corrispondente agli autovalori sulla diagonale di D). Ora $P^{-1} = P^T$ e $P^T AP = D$.*

11.4 Esercizi

Esercizio 11.1. *Diagonalizzare, se possibile, le seguenti matrici.*

$$\begin{pmatrix} 5 & -2 \\ 4 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 0 & -3 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Esercizio 11.2. *Determinare autovalori e autovettori della seguente matrice. La matrice è diagonalizzabile?*

$$\begin{pmatrix} 4 & 1 & 1 \\ 2 & 5 & -2 \\ -1 & -2 & 2 \end{pmatrix}$$

Esercizio 11.3. *Determinare per quale valore di h la seguente matrice ha 1 come autovalore. In questo caso la matrice è diagonalizzabile?*

$$\begin{pmatrix} 1 & h & 0 \\ 1 & 0 & 0 \\ 0 & 1 & -2/h \end{pmatrix}$$

Esercizio 11.4. *Determinare autovalori e autovettori della seguente matrice. La matrice è diagonalizzabile?*

$$\begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Esercizio 11.5. *Determinare autovalori e autovettori della seguente matrice. La matrice è diagonalizzabile?*

$$\begin{pmatrix} 5 & -2 & 2 \\ 4 & 1 & 4 \\ 4 & -1 & 9 \end{pmatrix}$$

Esercizio 11.6. *Determinare autovalori e autovettori della seguente matrice. La matrice è diagonalizzabile?*

$$\begin{pmatrix} 1 & -3 \\ -2 & 2 \end{pmatrix}$$

Esercizio 11.7. *Determinare autovalori e autovettori della seguente matrice. La matrice è diagonalizzabile?*

$$\begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ 3 & 3 & 5 \end{pmatrix}$$

Esercizio 11.8. *Data la seguente matrice*

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

determinarne gli autovalori ed i corrispettivi autovettori. La matrice è diagonalizzabile? In caso affermativo esibire le matrici P e D tali che

$$A = P^{-1}DP.$$

Soluzione. Il polinomio caratteristico della matrice A è dato da

$$\det(A-\lambda\mathbb{I}_4)=\det\begin{pmatrix}1-\lambda & 0 & 0 & 1\\ 0 & 1-\lambda & 1 & 0\\ 0 & 1 & 1-\lambda & 0\\ 1 & 0 & 0 & 1-\lambda\end{pmatrix}=\lambda^2(2-\lambda)^2.$$

Pertanto gli autovalori sono $0, 2$ entrambi con molteplicità algebrica 2.

Nel caso $\lambda=0$ il rango di $A-0\mathbb{I}=A$ è esattamente 2. Pertanto la molteplicità geometrica è $4-2=2$. Gli autovettori $(x,y,z,t)\in\mathbb{R}^4$ soddisfano

$$\begin{cases}x+t=0\\ y+z=0\\ y+z=0\\ x+t=0\end{cases}$$

e quindi sono dati da

$$A_0:=\{(-\alpha,-\beta,\alpha,\beta)\mid\alpha,\beta\in\mathbb{R}\}.$$

Nel caso $\lambda=2$ il rango di $A-2\mathbb{I}=A$ è esattamente 2. Pertanto la molteplicità geometrica è $4-2=2$. Gli autovettori $(x,y,z,t)\in\mathbb{R}^4$ soddisfano

$$\begin{cases}-x+t=0\\ -y+z=0\\ y-z=0\\ x-t=0\end{cases}$$

e quindi sono dati da

$$A_2:=\{(\alpha,\beta,\alpha,\beta)\mid\alpha,\beta\in\mathbb{R}\}.$$

La matrice è diagonalizzabile poichè pr ogni autovalore la molteplicità algebrica è uguale alla molteplicità geometrica. Le matrici P e D sono date ad esempio da

$$P=\begin{pmatrix}-1 & 0 & 1 & 0\\ 0 & -1 & 0 & 1\\ 0 & 1 & 0 & 1\\ 1 & 0 & 1 & 0\end{pmatrix},\qquad D=\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}.$$

Esercizio 11.9. *Data la seguente matrice*

$$A=\frac{1}{2}\begin{pmatrix}1 & 1 & -1 & 1\\ 1 & 1 & 1 & -1\\ -1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1\end{pmatrix},$$

determinarne gli autovalori ed i corrispettivi autovettori. La matrice è diagonalizzabile? In caso affermativo esibire le matrici P e D tali che

$$A = P^{-1}DP.$$

Soluzione.

Il polinomio caratteristico della matrice A è dato da $\det(A - \lambda\mathbb{I}_4) =$

$$\frac{1}{16}\det\begin{pmatrix} 1-2\lambda & 1 & -1 & 1 \\ 1 & 1-2\lambda & 1 & -1 \\ -1 & 1 & 1-2\lambda & 1 \\ 1 & -1 & 1 & 1-2\lambda \end{pmatrix} = (\lambda-1)^3(\lambda+1).$$

Pertanto l'autovalore 1 ha molteplicità algebrica 3 e l'autovalore -1 ha molteplicità algebrica 1.

Nel caso $\lambda = 1$ il rango di $A - 1\mathbb{I}$ è esattamente 1. Pertanto la molteplicità geometrica è $4 - 1 = 3$. Gli autovettori $(x, y, z, t) \in \mathbb{R}^4$ soddisfano $x - y + z - t = 0$ e quindi sono dati da

$$A_1 := \{(\alpha - \beta + \gamma, \alpha, \beta, \gamma) \mid \alpha, \beta, \gamma \in \mathbb{R}\}.$$

Nel caso $\lambda = -1$ il rango di $A + 1\mathbb{I}$ è esattamente 3. Pertanto la molteplicità geometrica è $4 - 3 = 1$. Gli autovettori $(x, y, z, t) \in \mathbb{R}^4$ soddisfano ad esempio

$$\begin{cases} 3x + y - z + t = 0 \\ 2y + z - t = 0 \\ y + z = 0 \end{cases}$$

e quindi sono dati da

$$A_{-1} := \{(\alpha, -\alpha, \alpha, -\alpha) \mid \alpha \in \mathbb{R}\}.$$

La matrice è diagonalizzabile poichè per ogni autovalore la molteplicità algebrica è uguale alla molteplicità geometrica. Le matrici P e D sono date ad esempio da

$$P = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \qquad D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Esercizio 11.10. *Determinare per quale valore di $k \in \mathbb{R}$ la matrice*

$$A_k = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & k & k \end{pmatrix},$$

è diagonalizzabile. In caso affermativo esibire le matrici P e D tali che

$$A = P^{-1}DP.$$

Il polinomio caratteristico della matrice A_k è dato da $\det(A_k - \lambda \mathbb{I}_3) =$

$$\det \begin{pmatrix} 2-\lambda & 0 & -1 \\ 0 & 1-\lambda & 1 \\ 0 & k & k-\lambda \end{pmatrix} = (2-\lambda)\lambda(\lambda - k - 1).$$

Pertanto gli autovalori sono $0, 2, k+1$.

Caso 1. $k+1 \neq 0, 2$. In questo caso gli autovalori sono tutti distinti e quindi la matrice è diagonalizzabile. Si ha che

$$A_0 = \{(\alpha, -2\alpha, 2\alpha) \mid \alpha \in \mathbb{R}\};$$

$$A_2 = \{(\alpha, 0, 0) \mid \alpha \in \mathbb{R}\};$$

$$A_{k+1} = \left\{ \left(\frac{k}{1-k}\alpha, \alpha, k\alpha \right) \mid \alpha \in \mathbb{R} \right\}.$$

Pertanto possiamo scegliere

$$P^{-1} = \begin{pmatrix} 1 & 1 & k \\ -2 & 0 & 1-k \\ 2 & 0 & k-k^2 \end{pmatrix}, \qquad D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & k+1 \end{pmatrix}.$$

Caso 2. $k+1 = 0$. In questo caso gli autovalori sono 0 con molteplicità 2 e 2 con molteplicità 1. La molteplicità geometrica di 0 è pari a 1 e pertanto la matrice non è diagonalizzabile.

Caso 3. $k+1 = 2$. In questo caso gli autovalori sono 0 con molteplicità 1 e 2 con molteplicità 2. La molteplicità geometrica di 2 è pari a 1 e pertanto la matrice non è diagonalizzabile.

Esercizio 11.11. *Determinare per quale valore di $k \in \mathbb{R}$ la matrice*

$$A_k = \begin{pmatrix} k+20 & 2k+22 & -4k+16 \\ k-7 & 2k-5 & 2k-8 \\ -9 & -18 & 3k-3 \end{pmatrix},$$

è diagonalizzabile. In caso affermativo esibire le matrici P e D tali che

$$A = P^{-1}DP.$$

Il polinomio caratteristico della matrice A_k è dato da $\det(A_k - \lambda \mathbb{I}_3) =$

$$\det \begin{pmatrix} k+20-\lambda & 2k+22 & -4k+16 \\ k-7 & 2k-5-\lambda & 2k-8 \\ -9 & -18 & 3k-3-\lambda \end{pmatrix} = -(\lambda-9)(\lambda-3k-6)(\lambda-3k+3).$$

Pertanto gli autovalori sono $9, 3k+6, 3k-3$.

Caso 1. $k \neq 1, 4$. In questo caso gli autovalori sono tutti distinti e quindi la matrice è diagonalizzabile. Si lascia al lettore il calcolo degli autospazi.

Caso 2. $k = 1$. In questo caso l'autovalore 9 ha molteplicità 2. La relativa molteplicità geometrica è 2. La matrice è pertanto diagonalizzabile. L'autospazio relativo è

$$A_9 := \{(-2y - z, y, z) \mid y, z \in \mathbb{R}\}.$$

Inoltre

$$A_0 := \{(-4y, 2y, 3y) \mid y \in \mathbb{R}\}.$$

Le matrici P^{-1} e D sono

$$P^{-1} = \begin{pmatrix} -2 & -1 & -4 \\ 1 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix}, \qquad D = \begin{pmatrix} 9 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Caso 3. $k = 4$. In questo caso l'autovalore 9 ha molteplicità 2. La relativa molteplicità geometrica è 2. La matrice è pertanto diagonalizzabile. L'autospazio relativo è

$$A_9 := \{(-2y, y, z) \mid y, z \in \mathbb{R}\}.$$

Inoltre

$$A_{18} := \{(-5y, y, 3y) \mid y \in \mathbb{R}\}.$$

Le matrici P^{-1} e D sono

$$P^{-1} = \begin{pmatrix} -2 & 0 & -5 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \end{pmatrix}, \qquad D = \begin{pmatrix} 9 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 18 \end{pmatrix}.$$

Esercizio 11.12. *Stabilire se la seguente matrice A è diagonalizzabile*

$$\begin{pmatrix} 10 & 8 & 4 \\ -2 & 2 & -2 \\ -3 & -6 & 3 \end{pmatrix}.$$

In caso affermativo determinare le tre matrici P, P^{-1} e D che la diagonalizzano.

Soluzione. La matrice $A - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} 10-\lambda & 8 & 4 \\ -2 & 2-\lambda & -2 \\ -3 & -6 & 3-\lambda \end{pmatrix}$$

e ha determinante pari a $-\lambda^3 + 15\lambda^2 - 72\lambda + 108 = -(\lambda-6)^2(\lambda-3)$. Pertanto gli autovalori sono 6 con molteplicità algebrica 2 e 3 con molteplicità algebrica 1. Calcoliamo le corrispettive molteplicità geometriche.

$$A - 6\mathbb{I}_3 = \begin{pmatrix} 4 & 8 & 4 \\ -2 & -4 & -2 \\ -3 & -6 & -3 \end{pmatrix}.$$

Si vede chiaramente che il rango di tale matrice è pari a 1 in quanto tutte le righe sono proporzionali. Quindi la molteplicità geometrica di $\lambda = 6$ è pari a $3 - 1 = 2$. Inoltre

$$A - 3\mathbb{I}_3 = \begin{pmatrix} 7 & 8 & 4 \\ -2 & -1 & -2 \\ -3 & -6 & 0 \end{pmatrix},$$

che ha rango 2 e quindi la molteplicità geometrica di $\lambda = 3$ è 1. La matrice è pertanto diagonalizzabile. Gli autospazi sono

$$A_6 = \{(-2y - z, y, z) \mid y, z \in \mathbb{R}\}, \qquad A_3 = \{(-4y, 2y, 3y) \mid y \in \mathbb{R}\}.$$

Le matrici P^{-1} e D possono essere pertanto

$$P^{-1} = \begin{pmatrix} -2 & -1 & -4 \\ 1 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix}, \qquad D = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Esercizio 11.13. *Stabilire per quale valore di $h \in \mathbb{R}$ la seguente matrice A_h è diagonalizzabile*

$$\begin{pmatrix} -4 & 0 & 0 \\ 0 & -4 & 0 \\ 2h+4 & 4h+8 & 2h \end{pmatrix}.$$

In caso affermativo determinare le tre matrici P, P^{-1} e D che la diagonalizzano.

Soluzione. La matrice $A - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} -4-\lambda & 0 & 0 \\ 0 & -4-\lambda & 0 \\ 2h+4 & 4h+8 & 2h-\lambda \end{pmatrix}$$

e ha determinante pari a $(\lambda+4)^2(2h-\lambda)$. Pertanto gli autovalori sono -4 e $2h$.

1. Caso 1: $h \neq -2$. In questo caso gli autovalori sono -4 con molteplicità algebrica 2 e $2h$ con molteplicità algebrica 1. Calcoliamo le corrispettive molteplicità geometriche.

$$A + 4\mathbb{I}_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 2h+4 & 4h+8 & 2h+4 \end{pmatrix}.$$

Si vede chiaramente che il rango di questa matrice è 1 (gli elementi della terza riga sono non nulli). Pertanto la molteplicità geometrica di -4 è $3 - 1 = 2$. Inoltre

$$A - 2h\mathbb{I}_3 = \begin{pmatrix} -4-2h & 0 & 0 \\ 0 & -4-2h & 0 \\ 2h+4 & 4h+8 & 0 \end{pmatrix}.$$

Si vede che il rango è 2 e quindi la molteplicità geometrica di $2h$ è pari a 1. La matrice è pertanto diagonalizzabile. Gli autospazi sono

$$A_{-4} = \{(-2y - z, y, z) \mid y, z \in \mathbb{R}\}, \qquad A_{2h} = \{(0, 0, z) \mid z \in \mathbb{R}\}.$$

Le matrici P^{-1} e D possono essere pertanto

$$P^{-1} = \begin{pmatrix} -2 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} -4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 2h \end{pmatrix}.$$

2. Caso 2: $h = -2$. In questo caso $\lambda = -4$ è autovalore con molteplicità algebrica 3. Si ha che

$$A + 4\mathbb{I}_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ha chiaramente rango 0 e pertanto la molteplicità geometrica di $\lambda = -4$ è 3. La matrice è quindi diagonalizzabile e si ha che

$$A_{-4} = \mathbb{R}^3.$$

Le matrici P^{-1} e D possono essere pertanto

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} -4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix}.$$

Esercizio 11.14. *Stabilire per quale valore di $h \in \mathbb{R}$ la seguente matrice A_h è diagonalizzabile*

$$\begin{pmatrix} -2h-8 & -4h-8 & -2h-4 & 0 \\ h+2 & 2h & h+2 & 0 \\ 2h+4 & 4h+8 & 2h & 0 \\ -7h-14 & -8h-16 & -3h-6 & 2h \end{pmatrix}.$$

Soluzione. La matrice $A - \lambda \mathbb{I}_4$ è data da

$$\begin{pmatrix} -2h-8-\lambda & -4h-8 & -2h-4 & 0 \\ h+2 & 2h-\lambda & h+2 & 0 \\ 2h+4 & 4h+8 & 2h-\lambda & 0 \\ -7h-14 & -8h-16 & -3h-6 & 2h-\lambda \end{pmatrix}$$

e ha determinante pari a

$$\lambda^4 - 4\lambda^3 h + 8\lambda^3 + 4\lambda^2 h^2 - 32\lambda^2 h + 16\lambda^2 + 32\lambda h^2 - 64\lambda h + 64h^2 = (\lambda+4)^2(\lambda-2h)^2.$$

Pertanto gli autovalori sono -4 e $2h$.

1. Caso 1: $h \neq -2$. In questo caso gli autovalori sono -4 con molteplicità algebrica 2 e $2h$ con molteplicità algebrica 2. Calcoliamo le corrispettive molteplicità geometriche.

$$A + 4\mathbb{I}_4 = \begin{pmatrix} -2h-4 & -4h-8 & -2h-4 & 0 \\ h+2 & 2h+4 & h+2 & 0 \\ 2h+4 & 4h+8 & 2h+4 & 0 \\ -7h-14 & -8h-16 & -3h-6 & 2h+4 \end{pmatrix}.$$

Le prime tre righe sono proporzionali. La prima riga non è proporzionale con la quarta ($h \neq -2$) e quindi il rango è 2. Pertanto la molteplicità geometrica di -4 è $4-2=2$. Inoltre

$$A - 2h\mathbb{I}_3 = \begin{pmatrix} -4h-8 & -4h-8 & -2h-4 & 0 \\ h+2 & 0 & h+2 & 0 \\ 2h+4 & 4h+8 & 0 & 0 \\ -7h-14 & -8h-16 & -3h-6 & 0 \end{pmatrix}.$$

Poiché $h \neq -2$ il rango di questa matrice equivale al rango della matrice

$$\begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 7 & 8 & 3 & 0 \end{pmatrix}.$$

Si vede che la prima riga è la somma della seconda e della terza, mentre la quarta è la somma di 3 volte la seconda riga e di quattro volte la terza. Pertanto il rango di tale matrice è 2 e quindi la molteplicità geometrica di $2h$ è pari a 2. La matrice è pertanto diagonalizzabile.

2. Caso 2: $h = -2$. In questo caso $\lambda = -4$ è autovalore con molteplicità algebrica 4. Si ha che
$$A + 4\mathbb{I}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$
ha chiaramente rango 0 e pertanto la molteplicità geometrica di $\lambda = -4$ è 4. La matrice è quindi diagonalizzabile.

Esercizio 11.15. *Determinare autovalori e autovettori della seguente matrice*
$$A = \begin{pmatrix} 1 & 2 & 2 & 4 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & -2 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$
Dire se tale matrice è diagonalizzabile e in caso affermativo esibire la matrici P e D tali che $A = P^{-1}DP$.

Esercizio 11.16. *Data la seguente matrice*
$$A = \begin{pmatrix} -7 & -3 & -16 \\ -2 & 0 & -2 \\ 6 & 3 & 15 \end{pmatrix}$$
determinarne gli autovalori ed i corrispettivi autovettori. La matrice è diagonalizzabile?

Soluzione. La matrice $A - \lambda\mathbb{I}_3$ è data da
$$\begin{pmatrix} -7-\lambda & -3 & -16 \\ -2 & 0-\lambda & -2 \\ 6 & 3 & 15-\lambda \end{pmatrix}$$
e ha determinante pari a $\lambda(1+\lambda)(9-\lambda)$. Pertanto gli autovalori sono $\lambda_1 = 0$ con molteplicità algebrica 1, $\lambda_2 = -1$ con molteplicità algebrica 1 e $\lambda_3 = 9$ con molteplicità algebrica 1. Poichè la molteplicità geometrica è minore uguale di quella algebrica tutti gli autivalori hanno molteplicità geometrica pari a 1.Possiamo quindi concludere che tale matrice è diagonalizzabile. Gli autospazi sono
$$A_0 = \{(3\alpha, -\alpha, \alpha) \mid \alpha \in \mathbb{R}\}, \qquad A_{-1} = \left\{\left(-\frac{7}{4}\alpha, -\frac{3}{2}\alpha, \alpha\right) \mid \alpha \in \mathbb{R}\right\}$$
$$A_9 = \{(\alpha, 0, -\alpha) \mid \alpha \in \mathbb{R}\}.$$

Esercizio 11.17. *Data la seguente matrice*

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 1 & 0 \\ 1 & 3 & 4 \end{pmatrix}$$

determinarne gli autovalori ed i corrispettivi autovettori. La matrice è diagonalizzabile? In caso affermativo determinare le tre matrici P, P^{-1} e D che la diagonalizzano.

Soluzione. La matrice $A - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} 2-\lambda & 0 & 0 \\ 3 & 1-\lambda & 0 \\ 1 & 3 & 4-\lambda \end{pmatrix}$$

e ha determinante pari a $(2-\lambda)(1-\lambda)(4-\lambda)$. Pertanto gli autovalori sono $\lambda_1 = 2$ con molteplicità algebrica 1, $\lambda_2 = 1$ con molteplicità algebrica 1 e $\lambda_3 = 4$ con molteplicità algebrica 1. Ogni autovalore ha molteplicità geometrica pari a 1, dal fatto che la molteplicità geometrica è $\leq$ di quella algebrica. Quindi la matrice A è diagonalizzabile. Calcoliamo i relativi autospazi dati da $AX = \lambda X$, si ha

$$\lambda_1 = 2 \Rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 3 & 1 & 0 \\ 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 2 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} 2x = 2x \\ 3x + y = 2y \\ x + 3y + 4z = 2z \end{cases}$$

$$\Rightarrow \begin{cases} 3x - y = 0 \\ x + 3y + 2z = 0 \end{cases} \Rightarrow \begin{cases} y = 3x \\ z = -5x \end{cases}$$

$$\lambda_2 = 1 \Rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 3 & 1 & 0 \\ 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} 2x = x \\ 3x + y = y \\ x + 3y + 4z = z \end{cases}$$

$$\Rightarrow \begin{cases} x = 0 \\ 3y + 3z = 0 \end{cases} \Rightarrow \begin{cases} x = 0 \\ y = -z \end{cases}$$

$$\lambda_3 = 4 \Rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 3 & 1 & 0 \\ 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 4 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} 2x = 4x \\ 3x + y = 4y \\ x + 3y + 4z = 4z \end{cases}$$

$$\Rightarrow \begin{cases} x = 0 \\ y = 0 \end{cases}$$

Gli autospazi sono

$$A_2 = \{(\alpha, 3\alpha, -5\alpha) \mid \alpha \in \mathbb{R}\}, \qquad A_1 = \{(0, \alpha, -\alpha) \mid \alpha \in \mathbb{R}\}$$

$$A_4 = \{(0,0,\alpha) \mid \alpha \in \mathbb{R}\}.$$

Le matrici P e D sono

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ -5 & -1 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Esercizio 11.18. *Data la seguente matrice*

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

determinarne gli autovalori ed i corrispettivi autovettori. La matrice è diagonalizzabile? In caso affermativo determinare le tre matrici P, P^{-1} e D che la diagonalizzano.

Soluzione. La matrice $A - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} 1-\lambda & 0 & 1 \\ 0 & 1-\lambda & 1 \\ 0 & 1 & 0-\lambda \end{pmatrix}$$

il cui determinate è $(1-\lambda)(\lambda^2-1)$. Gli autovalori sono $\lambda_1 = 1$ con molteplicità algebrica 2 e $\lambda_2 = -1$ con molteplicità algebrica 1 . Calcoliamo i relativi autospazi dati da $AX = \lambda X$, si ha

$$\lambda_1 = 1 \Rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} x+z = x \\ y+z = y \\ y = z \end{cases}$$

$$\Rightarrow \begin{cases} y = 0 \\ z = 0 \end{cases}.$$

L'autospazio relativo è $A_1 = \{(\alpha, 0, 0) \mid \alpha \in \mathbb{R}\}$ ed ha dimensione 1.

$$\lambda_2 = -1 \Rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} x+z = -x \\ y+z = -y \\ y = -z \end{cases}$$

$$\Rightarrow \begin{cases} 2x+z = 0 \\ 2y+z = 0 \\ y+z = 0 \end{cases} \Rightarrow \begin{cases} z = -2x \\ y = 2x \end{cases}.$$

L'autospazio relativo è $A_{-1} = \{(1, 2, -2) \mid \alpha \in \mathbb{R}\}$ ed ha dimensione 1. Poiché l'autospazio corrispondente all'autovalore 1 ha molteplicità algebrica 2 ma dimensione (molteplicità geometrica) 1, la matrice A non è diagonalizzabile .

Esercizio 11.19. *Determinare il parametro h in modo che la matrice assegnata A ammetta un autovalore $\lambda = 1$. Determinare poi gli autovalori in virtù del parametro h trovato.*

$$\begin{pmatrix} h & 1 & 0 \\ 1-h & 0 & 2 \\ 1 & 1 & h \end{pmatrix}$$

Soluzione. La matrice $A - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} h-\lambda & 1 & 0 \\ 1-h & 0-\lambda & 2 \\ 1 & 1 & h-\lambda \end{pmatrix}.$$

Affinché $\lambda = 1$ sia un autovalore, il determinante della matrice $A - 1\mathbb{I}_3$ deve essere 0. Quindi

$$\begin{vmatrix} h-1 & 1 & 0 \\ 1-h & -1 & 2 \\ 1 & 1 & h-1 \end{vmatrix} = 0 \Rightarrow 2(h-2) = 0 \Rightarrow h = 2.$$

Per $h = 2$ la matrice A diventa

$$A_{h=2} = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 2 \\ 1 & 1 & 2 \end{pmatrix}.$$

Calcoliamo quindi gli autovalori. La matrice $A_{h=2} - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} 2-\lambda & 1 & 0 \\ -1 & -\lambda & 2 \\ 1 & 1 & 2-\lambda \end{pmatrix}$$

il cui determinante è $\lambda(\lambda-1)(\lambda-3)$. Quindi gli autovalori di $A_{h=2}$ sono 0,1,3.

Esercizio 11.20. *Discutere la diagonalizzabilità della seguente matrice al variare del parametro reale k.*

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

Soluzione. La matrice $A - \lambda \mathbb{I}_3$ è data da

$$\begin{pmatrix} 1-\lambda & 1 & 0 \\ 0 & k-\lambda & 0 \\ 0 & 0 & 2-\lambda \end{pmatrix}$$

il cui determinate è $(1-\lambda)(k-\lambda)(2-\lambda)$. Gli autovalori sono $\lambda_1 = 1$,$\lambda_2 = 2$ e $\lambda_3 = k$. Vanno quindi distinti tre casi:

Caso 1. $k \neq 1, 2$, allora A ha 3 autovalori distinti con molteplicità algebrica e geometrica 1, quindi è diagonalizzabile.
Caso 2. $k = 1$, la matrice A diventa

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

quindi la matrice $A\lambda\mathbb{I}_3$ è data da

$$\begin{pmatrix} 1-\lambda & 1 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & 2-\lambda \end{pmatrix}.$$

il cui determinate è $(1-\lambda^2)(2-\lambda)$. Gli autovalori sono $\lambda_1 = 1$ con molteplicità algebrica 2 e $\lambda_2 = 2$ con molteplicità algebrica 1 e quindi anche molteplicità geometrica pari a 1. Dobbiamo quindi controllare se $\lambda = 1$ ha anche molteplicità geometrica 2. Calcoliamo quindi l'autospazio associato a $\lambda_1 = 1$ è dato da $AX = 1X$, si ha

$$\lambda_1 = 1 \Rightarrow \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} x + y = x \\ y = y \\ 2z = z \end{cases}$$

$$\Rightarrow \begin{cases} y = 0 \\ z = 0 \end{cases},$$

l'autospazio quindi è $A_1 = \{\alpha, 0, 0) \mid \alpha \in \mathbb{R}\}$. Quindi λ_1 ha molteplicità algebrica 2, ma molteplicità geometrica 1, perciò A non è diagonalizzabile. **Caso 3,** $k = 2$ la matrice A diventa

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

quindi la matrice $A\lambda\mathbb{I}_3$ è data da

$$\begin{pmatrix} 1-\lambda & 1 & 0 \\ 0 & 2-\lambda & 0 \\ 0 & 0 & 2-\lambda \end{pmatrix}.$$

il cui determinate è $(1-\lambda)(2-\lambda)^2$. Gli autovalori sono $\lambda_1 = 1$ con molteplicità algebrica 1 e quindi anche molteplicità geometrica 1 e $\lambda_1 = 2$ con molteplicità algebrica pari a 2. Vediamo quindi la dimensione dell'autospazio relativo a $\lambda_2 = 2$ per stabilirne la molteplicità

geometrica. L'autospazio associato a $\lambda_2 = 2$ è dato da $AX = 2X$, si ha

$$\lambda_2 = 2 \Rightarrow \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 2 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow \begin{cases} x + y = 2x \\ 2y = 2y \\ 2z = 2z \end{cases},$$

l'autospazio quindi è $A_2 = \{(\alpha, \alpha, 0), (0, 0, \beta) \ | \alpha, \beta \in \mathbb{R}\}$. Quindi $\lambda = 2$ ha molteplicità algebrica e geometrica 2 e A è diagonalizzabile.