NOTE DI ALGEBRA E GEOMETRIA

Corso di Matematica discreta - Vercelli 2022-23

Leonardo Castellani

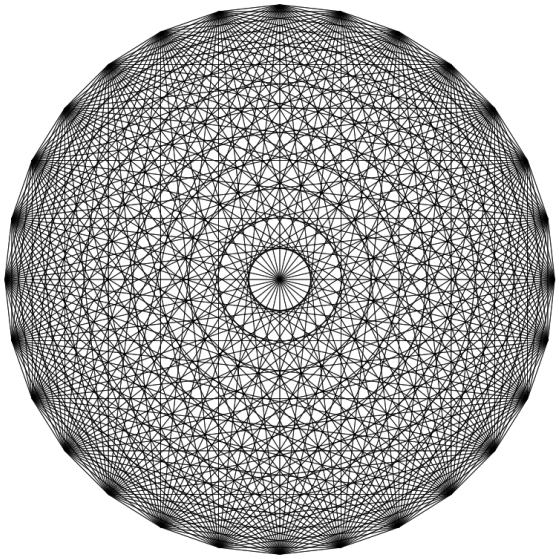
Dipartimento di Scienze e Innovazione Tecnologica
Università del Piemonte Orientale, viale T. Michel 11, 15121 Alessandria, Italia

INFN, Sezione di Torino, via P. Giuria 1, 10125 Torino, Italia

Regge Center for Algebra, Geometry and Theoretical Physics, via P. Giuria 1, 10125 Torino, Italia

Abstract

Note sintetiche delle lezioni di Algebra e Geometria (Matematica discreta) per il Corso di Laurea triennale in Informatica, a.a. 2022-23.



Febbraio 2023

leonardo.castellani@uniupo.it

Contents

1 Insiemi

1.1 Insiemi

• Insieme: collezione di oggetti, gli *elementi* dell' insieme. Esempi:
$\mathbb{N}$: insieme dei numeri naturali.
$\mathbb{Z}$: insieme dei numeri interi (relativi). Sono i numeri naturali con segno.
$\mathbb{Q}$: insieme dei numeri razionali.
$\mathbb{R}$: insieme dei numeri reali.
$\mathbb{R}^+$ ($\mathbb{R}^-$): insieme dei numeri reali positivi (negativi).
$\mathbb{R}_{\geq 0}$: insieme dei numeri reali ≥ 0, e analoga notazione per ≤ 0.
$\mathbb{R}^*$: insieme dei numeri reali senza lo 0. Analoghe notazioni per $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$.

• Se a appartiene a un insieme A, si scrive $a \in A$. Se non appartiene, si scrive $a \notin A$. Esempio: $3 \in \mathbb{N}, \frac{3}{2} \notin \mathbb{N}$.

• Modi per denotare un insieme. Si usano parentesi graffe.
- $\{a, b, c\}$: insieme che contiene gli elementi a, b, c
- specificando proprietà a cui devono soddisfare gli elementi dell' insieme. Esempio: $\{x \mid x \in \mathbb{N} \text{ e } x \leq 5\}$ si legge: "l' insieme degli elementi x tali che x appartiene a $\mathbb{N}$ e x è minore o uguale a 5", cioè l' insieme $\{0, 1, 2, 3, 4, 5\}$

Quindi l' insieme $\mathbb{Q}$ dei numeri razionali può scriversi come
$\mathbb{Q} = \{x \mid x = p/q \text{ con } p, q \in \mathbb{Z} \text{ e } q \neq 0\}$

Esercizio: denotare l' insieme dei numeri pari, dispari, primi

• L' insieme che non contiene nessun elemento si chiama *insieme vuoto* e si denota con il simbolo $\varnothing$. Esempio: $\{x \mid x \in \mathbb{R}, x > 5 \text{ e } x < 3\} = \varnothing$.

• A è un *sottoinsieme* di B se ogni elemento di A è anche elemento di B, e si indica con $A \subseteq B$. Esempi: $\mathbb{N} \subseteq \mathbb{Z}$, $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$, etc. Quando A è un sottoinsieme di B, e $A \neq B$, si può denotare l' inclusione anche con $A \subset B$. Dalla definizione segue che ogni insieme A è sottoinsieme di se stesso: $A \subseteq A$. Si conviene che ogni insieme abbia come sottoinsieme l' insieme vuoto: $\varnothing \subseteq A$, $\forall A$. Per ogni insieme A, i sottoinsiemi A e $\varnothing$ sono chiamati *sottoinsiemi impropri* di A. Tutti gli altri sottoinsiemi sono *sottoinsiemi propri*.

• Se $A \subseteq B$ e $B \subseteq A$, allora $A = B$, cioè A e B contengono gli stessi elementi.

Esercizio: quanti sono i diversi sottoinsiemi di un insieme con N elementi ? Risposta: 2^N.

• L' *insieme delle parti* di A è l' insieme di tutti i sottoinsiemi di A, e si denota con $\mathcal{P}(A)$. Quindi $\mathcal{P}(A)$ ha 2^N elementi. Per esempio se $A = \{1, 2, 3\}$, $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

• Attenzione a non confondere l' elemento a con l' insieme $\{a\}$ che contiene a come unico elemento. Per esempio l' insieme vuoto $\varnothing$ è diverso dall' insieme $\{\varnothing\}$ che contiene $\varnothing$ come unico elemento: il primo è l' insieme senza elementi, il secondo è un insieme con un elemento.

1.2 Operazioni tra insiemi

• **Unione:** $A \cup B$ è l' insieme degli elementi che appartengono ad A, o a B o a entrambi: $A \cup B = \{x \mid x \in A \ o \ x \in B\}$. Si legge "$A$ unione B".

• **Intersezione:** $A \cap B$ è l' insieme degli elementi che appartengono sia ad A che a B: $A \cap B = \{x \mid x \in A \ e \ x \in B\}$. Si legge "$A$ intersezione B". Gli insiemi A e B si dicono *disgiunti* se $A \cap B = \varnothing$.

• **Differenza:** $A \setminus B$ è l' insieme degli elementi che appartengono ad A e non a B. Quindi $A \setminus B = \{x \mid x \in A \ e \ x \notin B\}$. Si legge "$A$ meno B" oppure "complementare di B in A".

• **Differenza simmetrica:** $A \triangle B$ è l' insieme degli elementi che appartengono ad A o a B ma non a entrambi. Quindi $A \triangle B = \{x \mid x \in A \ o \ x \in B, x \notin A \cap B\}$, che si può anche scrivere come $A \triangle B = (A \cup B) \setminus (A \cap B)$.

• **Prodotto cartesiano** $A \times B$: insieme delle coppie ordinate (a, b), con $a \in A$ e $b \in B$. Esempio: se $A = \{1, 2\}$ e $B = \{3, 4, 5\}$, allora

$$A \times B = \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5).$$

Nota: ll prodotto cartesiano $A \times A$ può scriversi A^2.
Esempio: il piano cartesiano $\mathbb{R} \times \mathbb{R}$ può scriversi $\mathbb{R}^2$.

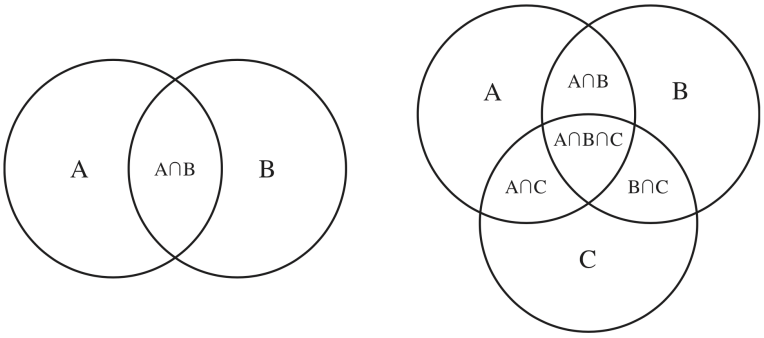


Fig. 1.1 Diagrammi di Venn.

• *Proprietà associativa* di unione: $(A \cup B) \cup C = A \cup (B \cup C)$
• *Proprietà associativa* di intersezione: $(A \cap B) \cap C = A \cap (B \cap C)$
Quindi si possono tralasciare le parentesi e scrivere $A \cup B \cup C$, $A \cap B \cap C$

• *Proprietà distributive*: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Queste proprietà sono dimostrabili facilmente usando i diagrammi di Venn (vedi Fig. 1.1)

1.3 Corrispondenze tra insiemi

Una *corrispondenza* tra l' insieme A e l' insieme B è una legge ψ che fa corrispondere a ogni elemento a di A uno o più elementi b di B.

Esempi:

1) $\psi : \mathbb{R} \longrightarrow \mathbb{R}$ data da $\psi(x) = \{+x, -x\}$
2) $\psi : \mathbb{R} \longrightarrow \mathbb{R}$ data da $\psi(x) = \{+\sqrt{1-x^2}, -\sqrt{1-x^2}\}$ per $|x| \leq 1$ e $\psi(x) = 0$ per $|x| > 1$.
3) $\psi : \mathbb{R} \longrightarrow \mathbb{R}$ data da $\psi(x) = \{y \mid x \leq y\}$

Si dice *grafico* della corrispondenza ψ il sottoinsieme di $A \times B$ definito da

$$\{(x, y) \mid x \in A,\ y \in B,\ y \in \psi(x)\} \tag{1.1}$$

Esercizio: disegnare i grafici degli esempi di sopra per ψ.

1.4 Applicazioni tra insiemi

Un' *applicazione* (o *funzione*, o *mappa*) tra l' insieme A e l' insieme B è una legge φ che fa corrispondere a ogni elemento a di A un elemento b di B (e non più di uno). Si scrive $\varphi : A \to B$ e

$$\varphi(a) = b \tag{1.2}$$

L' insieme A si dice *dominio* dell' applicazione φ. Si dice invece *immagine* di φ l' insieme degli elementi b di B tali che esiste un $a \in A$ per cui $b = \varphi(a)$, cioè l'insieme degli elementi di B che vengono "raggiunti" dall' applicazione. Si dice *controimmagine* di $b \in B$ l' insieme dei punti di A tali che $\varphi(a) = b$.

Esempio:
sia $\varphi : \mathbb{R} \to \mathbb{R}$ l' applicazione che porta un numero reale nel suo quadrato:

$$\varphi(x) = x^2 \tag{1.3}$$

In questo caso il dominio di φ è $\mathbb{R}$, l' immagine è $\mathbb{R}_{\geq 0}$ (i reali maggiori o uguali a zero), la controimmagine di ogni $x \in \mathbb{R}_{\geq 0}$ è l' insieme $\{\sqrt{x}, -\sqrt{x}\}$

• Una applicazione $\varphi : A \to B$ è

iniettiva: se elementi distinti di A hanno immagini distinte in B.

suriettiva: se l' immagine di A coincide con B, cioè se per ogni elemento b di B esiste un elemento a di A tale che $b = \varphi(a)$

biiettiva: se è iniettiva e suriettiva. In questo caso la corrispondenza tra elementi di A e B è biunivoca, e l' applicazione si dice anche *biiezione*.

• i_A: applicazione *identità* sull' insieme A, definita da $i_A(a) = a, \forall a \in A$.

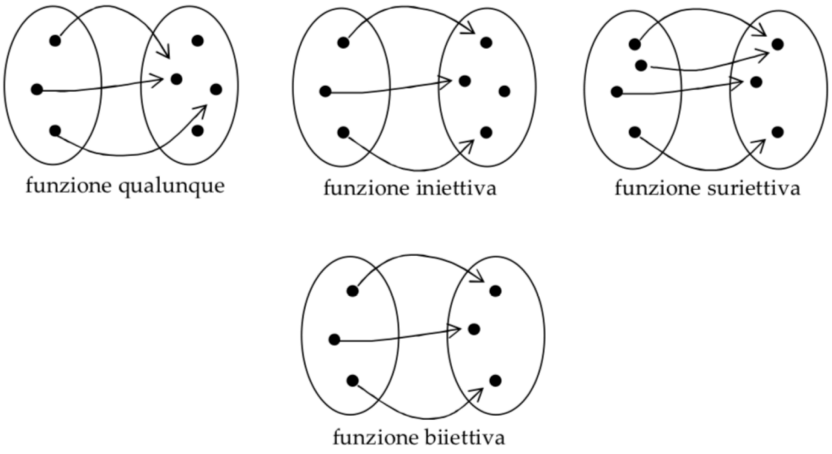


Fig. 1.2 Applicazioni generiche, iniettive, suriettive, biiettive.

1.5 Composizione di applicazioni

Se si hanno due applicazioni $\varphi : A \to B$ e $\psi : B \to C$, si definisce l' applicazione composta $\psi \circ \varphi : A \to C$:

$$(\psi \circ \varphi)(a) \equiv \psi(\varphi(a)) \tag{1.4}$$

Esempi:

1) $\varphi : \mathbb{Z} \to \mathbb{N}$, $\varphi(x) = x^2$
$\psi : \mathbb{N} \to \mathbb{N}$, $\psi(x) = 2x$
$\psi \circ \varphi : \mathbb{Z} \to \mathbb{N}, \quad (\psi \circ \varphi)(x) = \psi(\varphi(x)) = \psi(x^2) = 2x^2$

2) $g : \mathbb{Z} \to \mathbb{R}$, $g(x) = 2^x$
$f : \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{1}{1+x^2}$
$f \circ g : \mathbb{Z} \to \mathbb{R}, \quad (f \circ g)(x) = f(g(x)) = f(2^x) = \frac{1}{1+(2^x)^2} = \frac{1}{1+2^{2x}}$

• La composizione di applicazioni è *associativa*: $(\varphi \circ \psi) \circ \chi = \varphi \circ (\psi \circ \chi)$.

La dimostrazione è immediata usando la definizione di composizione. Si può quindi scrivere $\varphi \circ \psi \circ \chi$ senza parentesi.

• Data un' applicazione biiettiva $\varphi : A \to B$, per ogni $b \in B$, $\exists!\ a \in A \mid \varphi(a) = b$. Si può allora definire l' applicazione *inversa* φ^{-1} tale che $\varphi^{-1}(b) = a$.

Esempi:
$\varphi(x) = 2x$ è un' applicazione biiettiva da $\mathbb{R}$ in $\mathbb{R}$. La sua inversa è $\varphi^{-1}(x) = \frac{1}{2}x$
$\varphi(x) = x^2$ è un' applicazione biiettiva da $\mathbb{R}_{\geq 0}$ in $\mathbb{R}_{\geq 0}$. La sua inversa è $\varphi^{-1}(x) = \sqrt{x}$

Esercizio: dimostrare che $\varphi \circ \varphi^{-1} = i_B$ e $\varphi^{-1} \circ \varphi = i_A$.

Esercizio: dimostrare che $(\varphi^{-1})^{-1} = \varphi$.

Esercizio: se $\varphi : A \to B$ e $\psi : B \to C$ sono due applicazioni biiettive, dimostrare che $(\psi \circ \varphi)^{-1} = \varphi^{-1} \circ \psi^{-1}$

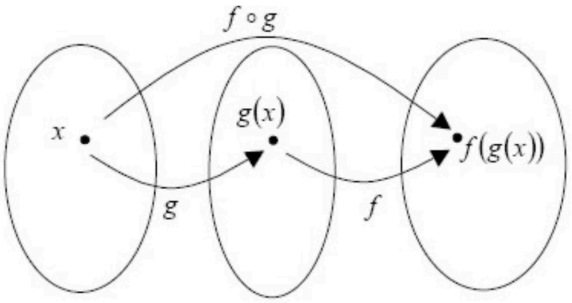


Fig. 1.3 Composizione di applicazioni

2 Richiami di aritmetica

Se non specificato, tutti i numeri considerati in questa Sezione sono numeri naturali ($\mathbb{N}$). Tutti i risultati possono essere estesi immediatamente ai numeri naturali relativi ($\mathbb{Z}$), chiamati anche numeri interi.

2.1 Definizioni e fondamenti

• **Divisione**: se $a, b \in \mathbb{N}$ e $b \neq 0$, esistono degli interi q e r tali che

$$a = bq + r, \qquad 0 \leq r < b \tag{2.1}$$

q e r sono rispettivamente il *quoziente* e il *resto* della divisione di a per b.

• **Divisori e multipli**: la notazione $b|a$ significa che b è un divisore di a (e si legge "b divide a"), cioè $a = bq$ con q intero. In tal caso si ha anche che a è un *multiplo* di b.

• **Numeri primi**: p è primo se i suoi divisori sono solo p e 1. Per convenzione il numero 1 non è primo. Anche 0 non è primo, dato che qualsiasi $n \in \mathbb{N}$ lo divide.

• **Teorema fondamentale dell' aritmetica**[1]**:** ogni numero $a \in \mathbb{N}$ diverso da 0 e 1 è prodotto di numeri primi. Tale fattorizzazione è essenzialmente unica (cioè a meno di riordinamento dei fattori). Per la dimostrazione vedi più avanti, Sezione 2.4.

• **Teorema:** esistono infiniti numeri primi [2].

Dimostrazione (Euclide): supponiamo per assurdo che esistano solo n numeri primi: $p_1, p_2, ...p_n$. Consideriamo il numero $a = p_1 p_2 ...p_n + 1$. Per il teorema fondamentale dell' aritmetica, a deve essere divisibile per almeno un numero primo q. Questo q deve essere compreso nella lista $p_1, p_2, ...p_n$, la lista di tutti i numeri primi. Quindi q divide anche $p_1 p_2 ...p_n$. Ne segue che q divide $a - p_1 p_2 ...p_n = 1$. Ma solo $q = 1$ può dividere 1, mentre q per ipotesi è diverso da 1. Si arriva quindi a una contraddizione, dovuta all' ipotesi che la lista dei numeri primi fosse finita. Ne consegue che la lista deve essere infinita. □

2.2 MCD e MCM

• **Massimo comune divisore (MCD):** d è il MCD due numeri a e b, e si scrive $d = \text{MCD}(a, b)$, se d divide sia a che b, e ogni altro c che divida sia a che b, divide anche d (cosicchè d è il *massimo* dell' insieme dei divisori comuni di a e b).

[1] Euclide, *Elementi*, libro VII, prop. 30, 31, 32; libro IX, prop. 14, circa 300 a.C.
[2] Euclide, *Elementi*, libro IX, prop. 20.

• **Teorema:** siano a,b non nulli. Allora $\exists\ \alpha, \beta \in \mathbb{Z}$ tali che $\mathrm{MCD}(a,b) = \alpha a + \beta b$. Inoltre $\mathrm{MCD}(a,b)$ è anche il più piccolo intero positivo che si può scrivere come $\alpha a + \beta b$.

Dimostrazione: consideriamo l' insieme $S = \{xa + yb$, con $x, y \in \mathbb{Z}$, e $xa + yb > 0\}$. S è un sottoinsieme dei numeri naturali diversi da 0, e non è l' insieme vuoto. Sia allora d il più piccolo dei suoi elementi, che possiamo quindi scrivere come $d = \alpha a + \beta b$ per un certo $\alpha \in \mathbb{Z}$ e un certo $\beta \in \mathbb{Z}$ fissati. Dimostriamo ora che d divide a. In generale si ha

$$a = dq + r, \quad 0 \leq r < d \tag{2.2}$$

da cui segue

$$r = a - dq = a - (\alpha a + \beta b)q = (1 - \alpha q)a + (-\beta q)b \tag{2.3}$$

Dimostriamo ora che il resto r è nullo, e quindi che $d|a$. Se per assurdo fosse $r > 0$, si avrebbe $r \in S$ e $r < d$, una contraddizione poichè d era stato scelto come il più piccolo elemento di S. Pertanto $r = 0$. Analogamente si dimostra che d divide b.

Per dimostrare che d è il massimo dei comuni divisori di a e b, resta da dimostrare che se un c divide a e b (e allora $a = a'c, b = b'c$), divide anche d. Infatti si ha

$$d = \alpha a + \beta b = (\alpha a' + \beta b')c \tag{2.4}$$

e quindi c divide d. In conclusione: il $\mathrm{MCD}(a,b)$ è uguale al più piccolo intero positivo che può scriversi come $xa + yb$, con $x, y \in \mathbb{Z}$. □

• Se $\mathrm{MCD}(a,b) = 1$, a e b hanno 1 come unico divisore comune, e si dicono *coprimi*. In tal caso, per il teorema precedente, esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$.

• **Lemma di Euclide esteso:** se un intero n divide il prodotto ab di due interi, e a è coprimo con n, allora n divide b.

Dimostrazione: se a è coprimo con n, si ha $rn + sa = 1$ con $r, s \in \mathbb{Z}$. Moltiplicando per b si trova $rnb + sab = b$, e siccome n divide rnb e sab (per ipotesi n divide ab), n divide b. □

• **Lemma di Euclide:** se un primo p divide il prodotto ab di due interi, e non divide a, allora divide b.

Dimostrazione: se un primo p non divide un intero a, allora p deve essere coprimo con a, e il Lemma di Euclde segue dal Lemma di Euclide esteso.

• **Minimo comune multiplo (MCM):** $m = MCM(a,b)$ se $a|m$ e $b|m$, e se per ogni c tale che $a|c$ e $b|c$ si ha $m|c$ (e allora m è il *minimo* dei multipli comuni a a e b).

2.3 Algoritmo di Euclide per trovare il MCD

Siano $a, b \in \mathbb{N}$ e $b \neq 0$. Ponendo $r_{-1} = a,\ r_0 = b$, si considera la successione:

$$\begin{aligned} r_{-1} &= r_0\ q_1 + r_1 \\ r_0 &= r_1\ q_2 + r_2 \\ r_1 &= r_2\ q_3 + r_3 \\ &\dots \\ r_{n-3} &= r_{n-2}\ q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1}\ q_n + r_n \\ r_{n-1} &= r_n\ q_{n+1} \end{aligned} \tag{2.5}$$

Quindi q_1 è il quoziente della divisione di a per b, e r_1 il resto. Si procede poi a dividere b per r_1, e si trova il resto r_2, e si continua dividendo tra loro i resti successivi, fino a trovare un resto r_{n+1} nullo.

1) La successione termina dopo un numero finito di passi.
2) r_n, l' ultimo resto non nullo nella successione, è il MCD(a,b)

Dimostrazione:

1) per la prima divisione si ha $0 \leq r_1 < b$. Per la seconda si ha $0 \leq r_1 < r_2$, e così via. Ne consegue che ogni resto è strettamente minore del precedente, e la successione dei resti $b > r_1 > r_2 > r_3 > ....$ deve pertanto terminare con un resto r_{n+1} uguale a 0.

2) dall' ultima equazione della successione, si trova che r_n divide r_{n-1}. Dalla penultima equazione segue allora che r_n divide anche r_{n-2}, e così risalendo si conclude che r_n divide $r_0 = b$, e r_n divide $r_{-1} = a$. Quindi r_n è un divisore comune di a e b. D' altra parte qualunque altro divisore comune c, dalla prima equazione della successione, deve dividere r_1. Per la seconda deve dividere r_2, e così continuando deve dividere r_n. Questo significa che r_n è proprio il massimo comune divisore di a e b. □

Nota: L' algoritmo di Euclide fornisce anche una procedura per trovare $\alpha, \beta \in \mathbb{Z}$ tali che $\text{MCD}(a, b) = \alpha a + \beta b$. Dalla penultima equazione in (2.5) si ha $r_n = \text{MCD}(a, b) = r_{n-2} - r_{n-1}\ q_n$, e si ottiene quindi il MCD come combinazione lineare a coefficienti interi dei resti r_{n-1} e r_{n-2}. Similmente, usando la terzultima e quartultima equazione in (2.5), si possono esprimere r_{n-1} e r_{n-2} come come combinazioni lineari a coefficienti interi dei resti precedenti, e procedendo a ritroso si arriva ad esprimere MCD come combinazione di r_0 e r_{-1}, cioè come combinazione di a e b. □

Esempi:

i) MCD(1956,1992)

$$\begin{aligned} 1956 &= 1992 \cdot 0 + 1956 \\ 1992 &= 1956 \cdot 1 + 36 \\ 1956 &= 36 \cdot 54 + 12 \\ 36 &= 12 \cdot 3 \end{aligned} \tag{2.6}$$

$\Rightarrow$ MCD $= 12$. Inoltre $12 = 54 \cdot 1992 - 53 \cdot 1956$.

ii) MCD(987654321,98765432)

$$\begin{aligned} 987654321 &= 98765432 \cdot 10 + 1 \\ 98765432 &= 1 \cdot 98765432 \end{aligned} \tag{2.7}$$

$\Rightarrow$ MCD $= 1$, e i due numeri sono *coprimi*. Inoltre $1 = 987654321 - 10 \cdot 98765432$.

2.4 Principio di induzione

Serve a verificare se un' asserzione P vale per tutti i numeri naturali n. Supponiamo che

i) P valga per $n = 0$;
ii) se P vale per $n - 1$ (con $n > 0$), allora vale per n

In tal caso P vale per ogni $n \in \mathbb{N}$.

Esempio:

P sia la seguente uguaglianza

$$1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q}, \quad q \in \mathbb{R}, \quad q \neq 1 \tag{2.8}$$

Per dimostrare che vale per ogni $n \in \mathbb{N}$, si verifica che vale per $n = 0$ (quindi col solo termine uguale a 1 nella serie di sinistra). Supposto poi che valga per $n - 1$, si dimostra che vale per n. Infatti si può riscrivere la P come segue

$$\begin{aligned} &1 + q + q^2 + \cdots + q^n = \\ &(1 + q + q^2 + \cdots + q^{n-1}) + q^n = \frac{1 - q^n}{1 - q} + q^n = \frac{1 - q^n + q^n(1 - q)}{1 - q} = \frac{1 - q^{n+1}}{1 - q} \end{aligned} \tag{2.9}$$

dove nel secondo rigo si è usata l' ipotesi che P valga per $n - 1$. $\square$

Esercizio: dimostrare con il principio di induzione le seguenti formule

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{2.10}$$

$$1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2 \tag{2.11}$$

$$(1 - \frac{1}{2})(1 - \frac{1}{3}) \cdots (1 - \frac{1}{n}) = \frac{1}{n} \tag{2.12}$$

Con il principio di induzione e il Lemma di Euclide della Sez. 2.2 possiamo dimostrare il teorema fondamentale dell' aritmetica, che consta di due parti:

1) ogni intero $n > 1$ è primo o prodotto di primi.

2) la fattorizzazione è unica, a meno di riordinamenti dei fattori primi.

L' intero 2 è primo. Quindi assumiamo che valga 1) per gli interi $< n$, e dimostriamo che vale per n. Se n è primo, non c'è nulla da dimostrare. Se n non è primo, ci sono interi a, b tali che $n = ab$ con $1 < a \leq b < n$. Per l' ipotesi di induzione $a = p_1 p_2 \cdots p_j$ e $b = q_1 q_2 \cdots q_k$ sono prodotti di primi. Ma allora anche $n = ab = p_1 p_2 \cdots p_j q_1 q_2 \cdots q_k$ è prodotto di primi. □

Dimostriamo ora l' unicità della fattorizzazione. Supponiamo per assurdo che esistano degli interi con due fattorizzazioni distinte, e sia n il più piccolo di questi interi. Si ha allora $n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$, dove ogni p_i e q_i è un primo. Osserviamo che p_1 divide $q_1 q_2 \cdots q_k$, e quindi deve dividere uno dei q_i per il Lemma di Euclide. Riordiniamo il prodotto in modo che questo q_i sia al primo posto, e quindi sia il q_1. Poichè p_1 e q_1 sono entrambi primi, $p_1 | q_1$ implica $p_1 = q_1$. Possiamo allora scrivere $n' = p_2 \cdots p_j = q_2 \cdots q_k$, con $n' < n$, che però contraddice l' ipotesi che n fosse il più piccolo degli interi con due fattorizzazioni distinte. Da questa contraddizione segue l' unicità della fattorizzazione in numeri primi. □

2.5 Sistema posizionale in base b

Sia $b \geq 2$ un numero naturale.

Ogni $n \in \mathbb{N}$ può essere scritto come somma di potenze di b, con dei coefficienti interi $a_0, a_1, ...$ compresi tra 0 e $b - 1$:

$$n = a_0 b^0 + a_1 b^1 + a_2 b^2 + \cdots + a_N b^N \tag{2.13}$$

A ogni numero naturale $< b$ si associa un simbolo (o *cifra*). Per esempio se $b = 10$, ai numeri naturali minori di 10 si associano i simboli $0, 1, ...9$. La successione $c_N c_{N-1} ... c_2 c_1$, dove c_i è il simbolo associato al numero a_i, è detta *rappresentazione* del numero n in base b.

Per esempio, se $b = 10$, il numero $n = 137$ si può scrivere come

$$137 = 7 \cdot 10^0 + 3 \cdot 10^1 + 1 \cdot 10^2 \tag{2.14}$$

Se $b = 2$, si ha la *rappresentazione binaria*. Per esempio, $n = 14$ in base 10 si scrive 1110 in base 2 poichè

$$14 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 \tag{2.15}$$

Quando $b > 10$, sono necessari extra simboli perchè non bastano più le cifre $0, 1, ...9$ per rappresentare n in base b. Per esempio se $b = 16$, si aggiungono le sei cifre A,B,C,D,E,F che valgono rispettivamente 10,11,12,13,14,15. Quindi in un numero rappresentato in base 16 (esadecimale) potranno comparire questi nuovi simboli, oltre a 0,...9.

I numeri $a_0, a_1, ...a_N$ in (2.13) sono univocamente determinati, una volta dati n e b. Infatti a_0 è il resto della divisione di n con b: tutti gli addendi nella (2.13) sono divisibili per b tranne il primo termine, cioè a_0. Il quoziente della divisione è dato da

$$a_1 b^0 + a_2 b^1 + \cdots + a_N b^{N-1} \tag{2.16}$$

Similmente, si trova a_1 come resto della divisione tra questo quoziente e b. Continuando in questo modo, si determinano tutti i numeri $a_0, a_1, ...a_N$ come resti della successione di divisioni

$$\begin{aligned} n &= bq_0 + a_0 \\ q_0 &= bq_1 + a_1 \\ q_1 &= bq_2 + a_2 \\ &\cdots \\ q_{N-2} &= bq_{N-1} + a_{N-1} \\ q_{N-1} &= bq_N + a_N \end{aligned} \tag{2.17}$$

Esempio: trovare la rappresentazione in base 6 del numero $n = 1243$ in base 10. Procedimento:

$$\begin{aligned} 1243 &= 6 \cdot 207 + 1 \\ 207 &= 6 \cdot 34 + 3 \\ 34 &= 6 \cdot 5 + 4 \\ 5 &= 6 \cdot 0 + 5 \end{aligned}$$

La successione dei resti è : $1, 3, 4, 5$. Pertanto 5431 è la rappresentazione in base 6 del numero 1243. Verifica:

$$1243 = 1 \cdot 6^0 + 3 \cdot 6^1 + 4 \cdot 6^2 + 5 \cdot 6^3 \tag{2.18}$$

Nota: possono essere espressi in base b non solo i numeri interi, ma più in generale tutti i numeri reali. Infatti le "cifre dopo la virgola" possono essere a loro volta espresse in base b. Se dopo la virgola abbiamo la sequenza di cifre $c_{-1}c_{-2}...c_{-M}$, questa individua un numero reale compreso tra 0 e 1:

$$0, c_{-1}c_{-2}c_{-3} \ ... \ c_{-M} = a_{-1}b^{-1} + a_{-2}b^{-2} + \cdots + a_{-M}b^{-M} \tag{2.19}$$

dove $a_{-1},\ \ldots, a_{-M}$ sono i numeri naturali $< b$ associati ai simboli $c_{-1},\ \ldots, c_{-M}$. Per esempio in base $b = 10$:

$$0,137 = 1 \cdot \frac{1}{10} + 3 \cdot \frac{1}{10^2} + 7 \cdot \frac{1}{10^3} \tag{2.20}$$

Pertanto ogni numero reale può rappresentarsi in base b come una somma pesata di potenze $\in \mathbb{Z}$ di b:

$$c_N c_{N-1} \ldots c_0,\ c_{-1} c_{-2} \ldots c_{-M} = a_N b^N + a_{N-1} b^{N-1} + \cdots a_0 b^0 + a_{-1} b^{-1} + a_{-2} b^{-2} + \cdots a_{-M} b^{-M} \tag{2.21}$$

3 Numeri complessi e matrici

3.1 Numeri complessi

Consideriamo l' equazione lineare a coefficienti interi $a, b \in \mathbb{Z}$

$$ax + b = 0 \tag{3.1}$$

Questa equazione ha per soluzione $x = -b/a$, soluzione che appartiene sempre a $\mathbb{Z}$ solo se b/a è un numero intero, altrimenti appartiene a $\mathbb{Q}$ (numeri razionali).

Similmente possiamo considerare l' equazione quadratica

$$x^2 = a \tag{3.2}$$

con $a \in \mathbb{R}$, che ha come soluzioni $x = \pm\sqrt{a}$. Questa soluzione è un numero reale solo se $a \geq 0$, altrimenti l' equazione non ha soluzioni reali. In particolare

$$x^2 = -1 \tag{3.3}$$

non ha soluzioni reali. Però, così come abbiamo dovuto ampliare i numeri da $\mathbb{Z}$ a $\mathbb{Q}$ per descrivere le soluzioni dell' equazione lineare, si può pensare a numeri più generali dei numeri reali, in cui esistono le soluzioni di equazioni quadratiche del tipo $x^2 = -1$. Questi numeri sono i *numeri complessi*, e il loro insieme viene denotato col simbolo $\mathbb{C}$.

Per costruire i numeri complessi, basta introdurre la quantità chiamata *unità immaginaria*, indicata col simbolo i. Questa è semplicemente la soluzione dell' equazione $x^2 = -1$, e cioè

$$i^2 = -1 \tag{3.4}$$

Questa equazione può essere vista come la definizione di i. Basta questa definizione, e l' uso delle solite regole per le quattro operazioni, per dedurre tutta la struttura dei numeri complessi.

Per esempio possiamo ora scrivere la soluzione di equazioni del tipo $x^2 = -4$. La soluzione è data da $x = 2i$ (infatti $(2i)^2 = 2^2 i^2 = -4$). In genere possiamo scrivere la soluzione di qualsiasi equazione quadratica del tipo $ax^2 + bx + c = 0$, anche quando il discriminante $b^2 - 4ac$ è minore di 0. Infatti ora siamo capaci di trattare radici quadrate di numeri negativi, avendo a disposizione i, che è la radice quadrata di -1. In realtà possiamo fare anche di più, e trattare radici ennesime di un qualunque numero reale, anzi più in generale di un qualunque numero complesso.

Introduciamo ora formalmente i numeri complessi. L' insieme $\mathbb{C}$ è dato da tutti gli elementi

$$z = x + iy \tag{3.5}$$

dove x e y sono numeri reali, chiamati rispettivamente *parte reale* e *parte immaginaria* del numero complesso z. Si usa la notazione

$$x = Re(z), \quad y = Im(z) \tag{3.6}$$

Quindi i numeri complessi sono individuati da una coppia ordinata di numeri reali (x, y). Dal punto di vista insiemistico si ha pertanto $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.

L' insieme $\mathbb{C}$ può essere dotato delle operazioni di somma, moltiplicazione e divisione in modo del tutto naturale.

Addizione: se $z = a + ib$ e $z' = a' + ib'$, si ha $z + z' = (a + a') + i(b + b')$, quindi la somma di due numeri complessi produce un numero complesso la cui parte reale è la somma delle parti reali e la parte immaginaria è la somma delle parti immaginarie di z e z'.

Moltiplicazione: $zz' = (a + ib)(a' + ib') = (aa' - bb') + i(ab' + a'b)$. Nella moltiplicazione di due numeri complessi si ottiene quindi un numero complesso con parte reale e parte immaginaria date dalle combinazioni $aa' - bb'$ e $ab' + a'b$ delle parti reali e immaginarie di z e z'. Nota: si dimostra immediatamente che $zz' = z'z$, cioè che la moltiplicazione tra numeri complessi è *commutativa*.

Prima di passare alla divisione, introduciamo l' operazione di **coniugazione** di un numero complesso, indicata da un asterisco, e definita da

$$z = x + iy \to z^* = x - iy \tag{3.7}$$

cioè per coniugare un numero complesso basta cambiare il segno della sua parte immaginaria. O altrimenti detto, basta cambiare i in $-i$, mentre x e y rimangono invariati. Se moltiplichiamo z per il suo complesso coniugato z^* otteniamo

$$zz^* = (x + iy)(x - iy) = x^2 + y^2 \tag{3.8}$$

cioè otteniamo una quantità reale ≥ 0. (zz^* non ha parte immaginaria, la i è scomparsa). Se prendiamo la radice quadrata di zz^*, si ottiene il **modulo** del numero complesso z, indicato come segue

$$|z| \equiv \sqrt{zz^*} = \sqrt{x^2 + y^2} \tag{3.9}$$

Divisione: dati i numeri complessi $z = a + ib$ e $z' = a' + ib'$, se a' e b' non sono entrambi nulli, si può eseguire la divisione:

$$\frac{z}{z'} = \frac{a + ib}{a' + ib'} \tag{3.10}$$

Per scrivere il risultato nella forma $z'' = a'' + ib''$ è sufficiente moltiplicare denominatore e numeratore per il complesso coniugato del denominatore:

$$\frac{z}{z'} = \frac{(a + ib)}{(a' + ib')} \frac{(a' - ib')}{(a' - ib')} = \frac{aa' + bb'}{a'^2 + b'^2} + i \, \frac{ba' - ab'}{a'^2 + b'^2} \tag{3.11}$$

3.2 Rappresentazione geometrica dei numeri complessi

Ogni numero complesso $z = a + ib$ è univocamente individuato dai due numeri reali a, b. Questi possono immaginarsi come le coordinate di un punto nel piano $\mathbb{R} \times \mathbb{R}$. Si ha quindi una corrispondenza biunivoca tra i punti del piano e i numeri complessi, e possiamo "visualizzare" i numeri complessi come punti del piano. Questo piano prende il nome di *piano di Gauss*.

Possiamo individuare i punti nel piano con le coordinate cartesiane a, b, oppure con altre coordinate, per esempio le coordinate *polari* ρ, φ, dove ρ è la lunghezza del segmento che congiunge il punto con l' origine, e θ l' angolo (orientato) che questo segmento forma con l' asse delle ascisse.

Dalle definizioni di seno e coseno si ha immediatamente

$$x = Re(z) = \rho \cos\theta, \quad y = Im(z) = \rho \sin\theta \tag{3.12}$$

e il numero complesso $z = x + iy$ può scriversi nella sua rappresentazione trigonometrica:

$$z = \rho(\cos\theta + i \sin\theta) \tag{3.13}$$

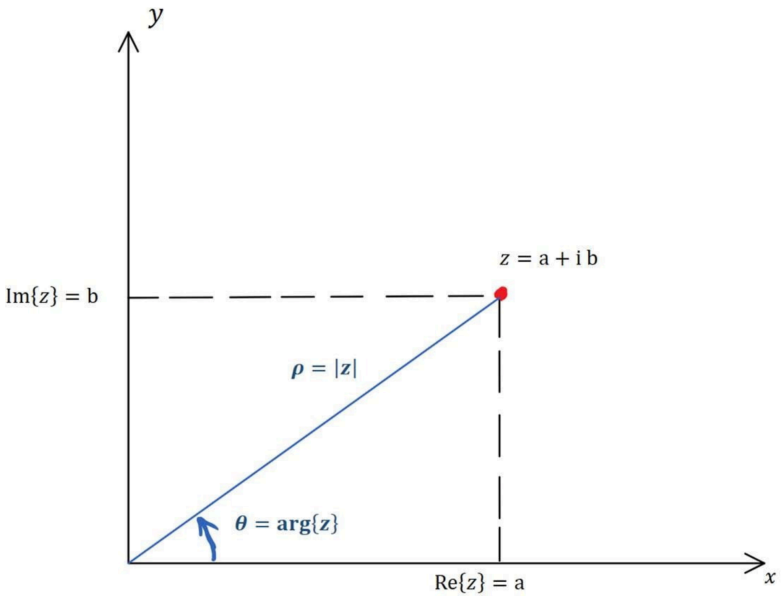


Fig. 2.1 Rappresentazione geometrica dei numeri complessi.

Dal teorema di Pitagora risulta che $\rho = \sqrt{a^2 + b^2}$, cioè $\rho = |z|$ è il modulo del numero complesso. L' angolo θ si chiama anche *argomento* del numero complesso, e si indica con $arg(z)$.

Riassumendo, un numero complesso z è individuato da due numeri reali :

- le sue coordinate cartesiane (a, b), ovvero la sua parte reale e parte immaginaria
- oppure dal suo modulo ρ e dal suo argomento $arg(z)$

E' conveniente esprimere il prodotto zz' nella rappresentazione trigonometrica. Se

z e z' sono dati da

$$z = \rho(\cos\theta + i\sin\theta), \quad z' = \rho'(\cos\theta' + i\sin\theta') \tag{3.14}$$

il loro prodotto si scrive

$$\begin{aligned} zz' = \rho\rho'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \\ \rho\rho'[(\cos\theta\cos\theta' - \sin\theta\sin\theta') + i(\cos\theta\sin\theta' + \sin\theta\cos\theta')] = \\ \rho\rho'[\cos(\theta+\theta') + i\sin(\theta+\theta')] \end{aligned} \tag{3.15}$$

da cui si ricava l' utile regola: *il prodotto di due numeri complessi ha per modulo il prodotto dei moduli e per argomento la somma degli argomenti.*

Applicando questa regola ripetutamente si arriva alla *formula di De Moivre* per la potenza n-esima di un numero complesso $z = \rho(\cos\theta + i\sin\theta)$

$$z^n = \rho^n(\cos n\theta + i\sin n\theta) \tag{3.16}$$

3.3 Radici n-esime dell' unità

La formula di De Moivre ci permette di risolvere facilmente l' equazione

$$z^n = 1 \tag{3.17}$$

($n \geq 1$). cioè di trovare le radici n-esime dell' unità. In notazione trigonometrica si ha

$$\rho^n(\cos n\theta + i\sin n\theta) = 1 \tag{3.18}$$

Per soddisfare questa equazione è necessario che sia:

$$\rho^n = 1, \quad n\theta = k\cdot 2\pi, \quad k \in \mathbb{N} \tag{3.19}$$

Quindi $z = \rho(\cos\theta + i\sin\theta)$ è soluzione se $\rho = 1$ e $\theta = \frac{2k\pi}{n}$ e le soluzioni hanno la forma:

$$z_k = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) \tag{3.20}$$

Ci sono n soluzioni diverse, poichè k può prendere n valori $k = 0, 1, ...n-1$ (per valori $\geq n$ le soluzioni si ripetono).

Esempio: le radici dell' unità per $n = 6$. Sono disposte sui vertici di un esagono nel piano di Gauss.

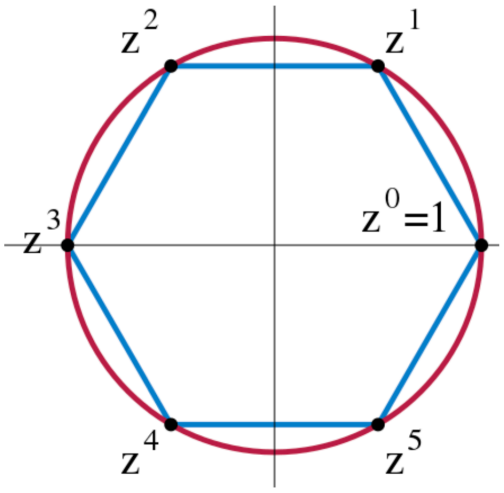


Fig. 2.2 Radici seste dell' unità. Sono disposte sui vertici di un esagono regolare iscritto nella circonferenza di centro in (0,0) e raggio 1, avente uno dei vertici in (1,0).

3.4 Esercizi sui numeri complessi

Esercizio 1: trovare modulo, argomento e rappresentazione trigonometrica di $z = 1 - i$, e di $1 - i\sqrt{3}$

Esercizio 2: dimostrare che se $zz' = 0$ allora almeno uno dei due numeri complessi z, z' è nullo.

Esercizio 3: disegnare nel piano di Gauss l' insieme dei numeri z tali che
i) $|z| \leq 1$
ii) $|z - 1| \leq 1$

Esercizio 4: se $z = \rho(\cos\theta + i \sin\theta)$, trovare la rappresentazione trigonomtrica di $-z$, $1/z$, iz, z^*.

Esercizio 5: dimostrare che
i) $(z^*)^* = z$
ii) $(z + z')^* = z^* + z'^*$
iii) $(zz')^* = z^* z'^*$
iv) $z + z^* = 2\ Re(z),\ \ z - z^* = 2i\ Im(z)$

3.5 Teorema fondamentale dell' algebra

L' equazione algebrica a coefficienti reali

$$a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 = 0 \tag{3.21}$$

ammette n soluzioni complesse. Se z è soluzione, lo è anche z^* (dimostrarlo usando l' Esercizio 5 di sopra).

Esempio : le soluzioni di

$$az^2 + bz + c = 0 \tag{3.22}$$

con $a, b, c \in \mathbb{R}$, sono date dalla nota formula

$$z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{3.23}$$

Sono soluzioni reali se $b^2 - 4ac \geq 0$, altrimenti sono complesse. In tal caso si possono scrivere come

$$z = \frac{-b \pm i\sqrt{4ac - b^2}}{2a} \tag{3.24}$$

3.6 Matrici

Nella Sezione precedente, abbiamo introdotto i numeri complessi $z \in \mathbb{C}$, caratterizzati da una *coppia* di numeri reali, e definito addizione, moltiplicazione e divisione in $\mathbb{C}$. Possiamo proseguire in questo tipo di generalizzazione, e introdurre *tabelle* di numeri reali, o anche complessi, che possono sommarsi e moltiplicarsi con opportune regole. Queste tabelle si chiamano *matrici*, e vengono organizzate in un certo numero di *righe* e di *colonne*. Per esempio la matrice

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} & ... & A_{1n} \\ A_{21} & A_{22} & A_{23} & ... & A_{2n} \\ A_{31} & A_{32} & A_{33} & ... & A_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1} & A_{m2} & A_{m3} & ... & A_{mn} \end{pmatrix} \tag{3.25}$$

ha m righe e n colonne. L' elemento della matrice corrispondente alla i-esima riga e j-esima colonna viene denotato con la coppia di indici ij. Per esempio l' elemento della matrice che si trova sulla seconda riga e sulla terza colonna viene indicato con A_{23}. Per indicare che la matrice A ha m righe e n colonne si usa la notazione $A_{m\times n}$, e si dice che A è una matrice $m \times n$. Se $n = m$ la matrice si dice *quadrata*.

Tra due matrici $A_{m\times n}$ e $B_{m\times n}$ (quindi che abbiano lo stesso numero di righe e lo stesso numero di colonne) viene definita l' addizione come segue:

Addizione: $(A + B)_{ij} = A_{ij} + B_{ij}$, cioè gli elementi ij della matrice somma (gli elementi che stanno sulla i-esima riga e j-esima colonna) si ottengono sommando tra loro gli elementi ij delle due matrici. Esempio:

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix} + \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \end{pmatrix} = \begin{pmatrix} A_{11} + B_{11} & A_{12} + B_{12} & A_{13} + B_{13} \\ A_{21} + B_{21} & A_{22} + B_{22} & A_{23} + B_{23} \end{pmatrix} \tag{3.26}$$

E' immediato verificare che l' addizione tra matrici è commutativa, $A + B = B + A$ e associativa, $(A + B) + C = A + (B + C)$. La *matrice zero* 0 ha tutti gli elementi uguali a 0, e $A + 0 = 0$ per ogni matrice A.

Moltiplicazione: Tra matrici $A_{m\times n}$ e $B_{n\times r}$ (quindi il numero di colonne di A deve essere uguale al numero di righe di B), si definisce una moltiplicazione AB come segue:

$$(AB)_{ij} = \sum_k A_{ik}B_{kj} \tag{3.27}$$

Questa regola di moltiplicazione matriciale viene anche detta "prodotto righe per colonne". Il risultato è una matrice $m \times r$. Per esempio:

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \\ B_{31} & B_{32} \end{pmatrix} =$$

$$= \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} + A_{13}B_{31} & A_{11}B_{12} + A_{12}B_{22} + A_{13}B_{32} \\ A_{21}B_{11} + A_{22}B_{21} + A_{23}B_{31} & A_{21}B_{12} + A_{22}B_{22} + A_{23}B_{32} \end{pmatrix} \tag{3.28}$$

Con tre matrici $A_{m\times n}$, $B_{n\times r}$, $C_{r\times s}$, la moltiplicazione è associativa: $(AB)C = A(BC)$. Per due matrici $A_{m\times n}, B_{n\times m}$ possiamo considerare entrambi i prodotti AB e BA. Se $n \neq m$ è ovvio che $AB \neq BA$, poichè i due prodotti sono matrici di dimensioni diverse (AB è una matrice $m \times n$ mentre BA è una matrice $n \times m$). Se $m = n$, cioè se A e B sono matrici quadrate, la moltiplicazione in genere non è commutativa. Per esempio

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.29}$$

Se A è una matrice quadrata $n \times n$, la *matrice unità* $I_{n\times n}$ è una matrice quadrata tale che $AI = IA = A$. I suoi elementi ij sono nulli se $i \neq j$ e uguali a 1 se $i = j$. In altre parole I è una matrice diagonale, con tutti gli elementi sulla diagonale uguali a 1. Gli elementi di I vengono anche indicati col *simbolo di Kronecker*: δ_{ij}, che vale 1 se $i = j$ e 0 altrimenti. E' anche detto "delta di Kronecker".

Moltiplicazione per un numero: se λ è un numero reale (o complesso) e A una matrice, si definisce il prodotto λA semplicemente moltiplicando ogni elemento di A per il numero λ. Per esempio

$$\lambda \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix} = \begin{pmatrix} \lambda A_{11} & \lambda A_{12} & \lambda A_{13} \\ \lambda A_{21} & \lambda A_{22} & \lambda A_{23} \end{pmatrix} \tag{3.30}$$

Nota: $A\lambda$ è definito uguale a λA.

Trasposizione: definita tramite scambio di righe e colonne. Gli elementi della matrice trasposta di A, indicata con A^T, sono definiti da

$$(A^T)_{ij} = A_{ji} \tag{3.31}$$

La trasposta di una matrice $m \times n$ è una matrice $n \times m$. Esempio:

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix}^T = \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \\ A_{13} & A_{23} \end{pmatrix}$$

Una matrice quadrata tale che $A^T = A$ si dice *simmetrica*.

Matrice inversa: per una matrice quadrata A, l' inversa A^{-1} è definita da

$$A^{-1}A = AA^{-1} = I \tag{3.32}$$

Esempio: se A è una generica matrice 2×2:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{3.33}$$

la sua inversa A^{-1} è data dalla matrice

$$A^{-1} = \frac{1}{(ad - bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tag{3.34}$$

come si può facilmente verificare eseguendo le moltiplicazioni $A^{-1}A$, AA^{-1}. Nota: l' inversa di A esiste solo se $ad - bc \neq 0$.

Esercizio: dimostrare che $(A^{-1})^{-1} = A$.

Esercizi: dimostrare le seguenti proprietà, con A, B, C matrici e λ, μ numeri

1) $A(B + C) = AB + BC$ (proprietà distributiva)
2) $(AB)C = A(BC)$ (proprietà associativa del prodotto)
3) $\lambda(\mu A) = (\lambda\mu)A$
4) $(\lambda + \mu)A = \lambda A + \mu A$
5) $\lambda(A + B) = \lambda A + \lambda B$
6) $(\lambda A)B = \lambda(AB) = A(\lambda B)$

4 Relazioni

Se a e b sono elementi di uno stesso insieme A, a può essere *in relazione* ρ con b, e si scrive $a\ \rho\ b$. Esempio: se la relazione ρ è l' uguaglianza $=$, $a\ \rho\ b$ significa $a = b$, e quindi a è in relazione ρ con b se a e b sono uguali. Se $a, b \in \mathbb{N}$ e ρ è la relazione "minore di", allora $a\ \rho\ b$ può scriversi $a < b$, e a è in relazione ρ con b se è minore di b. Se a non è in relazione ρ con b, si scrive $a \not\rho\ b$. Altri esempi di relazioni:

i) in $\mathbb{C}$, z è in relazione con z' se $|z| = |z'|$.
ii) in $P(A)$, X è in relazione con Y se $X \subset Y$.
iii) nel piano $\mathbb{R} \times \mathbb{R}$, il punto P è in relazione con il punto Q se la loro distanza è inferiore a 1.
iv) nell' insieme delle radici ottave dell' unità, $a\ \rho\ b$ se $a^2 = b$
v) nel piano $\mathbb{R} \times \mathbb{R}$, il punto (x, y) è in relazione con (x', y') se $y = y'$.

Grafo della relazione: è un modo per visualizzare una relazione in un insieme A (con un numero finito di elementi). Si rappresenta ogni elemento con un punto, e se a è in relazione con b, si collega il punto rappresentativo di a col punto rappresentativo di b tramite una linea orientata da a a b.

Esercizio: disegnare il grafo rappresentativo della relazione iv).

Una relazione ρ si dice *riflessiva* se $a\ \rho\ a$, per ogni $a \in A$; si dice *simmetrica* se $a\ \rho\ b\ \Rightarrow\ b\ \rho\ a$, per ogni $a, b \in A$; si dice *transitiva* se $a\ \rho\ b$ e $b\ \rho\ c$ implica $a\ \rho\ c$, per ogni $a, b, c \in A$.

Esempi con $A = \mathbb{R}$:
la relazione $<$ è transitiva, ma non riflessiva e non simmetrica
la relazione $\leq$ è riflessiva e transitiva, ma non simmetrica
la relazione ρ definita da $x\ \rho\ y$ se $x = 2y$, non ha nessuna delle tre proprietà.

4.1 Relazioni di equivalenza

Se una relazione è riflessiva, simmetrica e transitiva, viene chiamata *relazione di equivalenza*. Per esempio sono relazioni di equivalenza l' uguaglianza $=$, oppure le relazioni i) , v) (vedi sopra).
Una relazione di equivalenza viene indicata col simbolo $\sim$.

4.2 Classi di equivalenza

Sia $\sim$ un' equivalenza su un insieme A. Per ogni $a \in A$ si definisce un insieme:

$$[a]_\sim = \{x | x \in A, x \sim a\} \tag{4.1}$$

cioè l' insieme di tutti gli elementi equivalenti a a. Questo insieme si chiama **classe di equivalenza**.

L' insieme di tutte le classi di equivalenza viene chiamato **insieme quoziente** e si indica col simbolo $A/_\sim$:

$$A/_\sim \;=\; \{[a]_\sim \,|a \in A\} \tag{4.2}$$

Infine si definisce l' applicazione $\pi : A \longrightarrow A/_\sim$

$$\pi(a) = [a]_\sim, \quad a \in A \tag{4.3}$$

chiamata *applicazione canonica* o *proiezione canonica*.

Esempi

i) se la relazione di equivalenza è la i), cioè $z \sim z'$ se $|z| = |z'|$, le classi di equivalenza (insiemi dei numeri complessi con stesso modulo) sono i cerchi nel piano di Gauss con centro nell' origine. Possiamo individuare ogni classe di equivalenza con il raggio del cerchio. L' insieme quoziente è l' insieme di tutti i cerchi concentrici.

ii) se la relazione di equivalenza è la v), cioè due punti nel piano sono equivalenti se hanno stessa ordinata, le classi di equivalenza (insiemi dei punti con stessa ordinata) sono le rette parallele all' asse delle ascisse. Possiamo individuare ogni classe di equivalenza con il valore y dell' ordinata dei punti della retta. L' insieme quoziente è l' insieme di tutte le rette parallele all' asse delle ascisse.

In entrambi gli esempi, l' equivalenza ha determinato una famiglia di sottoinsiemi del piano: cerchi concentrici nel primo esempio, rette parallele all' asse x nel secondo esempio. I sottoinsiemi corrispondenti a classi di equivalenza diverse (per esempio cerchi di raggio diverso) non hanno elementi in comune, altrimenti le classi di equivalenza dovrebbero coincidere (stesso raggio). Lo stesso vale per il secondo esempio. Quindi le classi di equivalenza sono sottoinsiemi disgiunti. Infine l' unione di tutti i cerchi concentrici, oppure l' unione di tutte le rette parallele, ricostruisce tutto il piano. Infatti qualunque punto del piano appartiene a una precisa classe di equivalenza (un cerchio o una retta parallela).

Riassumiamo le tre proprietà delle classi di equivalenza in un insieme A:

1) non sono vuote: ogni elemento di A è equivalente a se stesso, pertanto $[a]_\sim$ contiene almeno l' elemento a.
2) sono disgiunte
3) la loro unione coincide con A.

4.3 Partizioni

Una *partizione di un insieme* A è una famiglia $\mathcal{F}$ di sottoinsiemi di A che soddisfa le tre proprietà appena menzionate:

1) ogni sottoinsieme $X \in \mathcal{F}$ non è vuoto
2) se $X, Y \in \mathcal{F}$, allora $X \cap Y = \varnothing$.
3) $\bigcup_{X \in \mathcal{F}} X = A$

Quindi, data una relazione $\sim$ nell' insieme A, l' insieme delle classi di equivalenza (cioè $A/_\sim$) costituisce una partizione di A.

Viceversa, data una partizione $\mathcal{F}$ di A, si può definire una relazione di equivalenza $\sim_{\mathcal{F}}$ semplicemente dichiarando equivalenti due elementi di A che facciano parte di uno stesso sottoinsieme X nella famiglia $\mathcal{F}$. Dimostrazione: immediata.

4.4 Insieme delle classi resto: aritmetica modulare

Sia $n \in \mathbb{N}$ con $n \geq 1$. Si definisce una relazione tra numeri interi $a, b \in \mathbb{Z}$, chiamata *uguaglianza modulare* (oppure *congruenza*): a è congruente a b modulo n, e si scrive

$$a \equiv b \ (mod\ n) \quad \text{oppure} \quad a \equiv_n b \tag{4.4}$$

se n divide $a - b$, cioè se

$$a = b + kn, \quad k \in \mathbb{Z} \tag{4.5}$$

Quindi due interi sono congrui modulo n se differiscono per un multiplo intero di n.

La congruenza modulo n è una relazione di equivalenza: infatti è riflessiva (ogni intero è congruo a se stesso), simmetrica (se $a \equiv_n b$, allora si ha anche $b \equiv_n a$) e transitiva (se $a \equiv_n b$ e $b \equiv_n c$, allora $a \equiv_n c$).

Esercizio: dimostrarlo.

Si possono allora definire le classi di equivalenza

$$[a]_n = \{x \mid x \in \mathbb{Z},\ x \equiv_n a\} \tag{4.6}$$

Questi insiemi possono anche indicarsi come

$$[a]_n = \{a + kn,\ a, k \in \mathbb{Z}\} \tag{4.7}$$

L' insieme di queste classi di equivalenza è l' insieme quoziente

$$\mathbb{Z}/\equiv_n \ = \{[a]_n,\ \mid a \in \mathbb{Z}\} \tag{4.8}$$

Questo insieme è costituito dalle n classi disgiunte:

$$[0]_n,\ [1]_n,\ [2]_n, ...,\ [n-1]_n \tag{4.9}$$

Infatti la classe $[n]_n$ coincide con la classe $[0]_n$, e in generale $[a+n]_n = [a]_n$.

Per esempio:

$$\begin{aligned} [0]_3 &= \{..., -9, -6, -3, 0, 3, 6, 9, ...\} \\ [1]_3 &= \{..., -8, -5, -2, 1, 4, 7, 10, ...\} \\ [2]_3 &= \{..., -7, -4, -1, 2, 5, 8, 11, ...\} \end{aligned} \tag{4.10}$$

L' insieme delle classi di equivalenza $[a]_n$ determina una partizione di $\mathbb{Z}$, come è facile verificare nell' esempio di sopra.

La congruenza è compatibile con l' addizione e la moltiplicazione, nel senso che se $a \equiv_n b,\ c \equiv_n d$, si ha

$$a + c \equiv_n b + d, \quad ac \equiv_n bd \tag{4.11}$$

In particolare

$$a + k \equiv_n b + k \quad \Leftrightarrow \quad a \equiv_n b \tag{4.12}$$

Tuttavia se

$$ak \equiv_n bk \tag{4.13}$$

non possiamo in generale dedurre che $a \equiv_n b$. Infatti vale il seguente

Teorema di divisione modulare: $ak \equiv_n bk$ implica $a \equiv_n b$ solo se k è coprimo con n.

Dimostrazione: da $ka \equiv_n kb$ si ha $k(a-b) \equiv_n 0$, cioè $k(a-b) = jn,\ j \in \mathbb{Z}$. Quindi n divide $k(a-b)$. Se n è coprimo con k, per il Lemma esteso di Euclide n deve dividere $a-b$, e cioè $a \equiv_n b$. □

Esempio: si ha $10 \cdot 6 \equiv_{15} 10 \cdot 9$, ma non vale la congruenza modulo 15 degli interi 6 e 10, e infatti 10 e 15 hanno un fattore comune.

Esercizi:

1) dimostrare che $7^n \equiv_8 1$ se n è pari e $7^n \equiv_8 7$ se n è dispari. Suggerimento: per induzione.
2) siano $x, y, n \in \mathbb{Z}$ e $n > 0$. Dimostrare che $x \equiv_n y \ \Leftrightarrow$ i resti delle divisioni x/n, y/n sono uguali.

Da 2) segue che tutti gli elementi di una classe di equivalenza modulo n hanno lo stesso resto dopo una divisione per n. Per questa ragione le classi di equivalenza modulo n si chiamano *classi resto*.

5 Cardinalità di insiemi

• La *cardinalità* di un insieme finito A è il numero dei suoi elementi, e si indica con $|A|$. La cardinalità dell' insieme vuoto è zero.

• Due insiemi (non necessariamente finiti) si dicono *equipotenti* se esiste una biiezione $\varphi : A \leftrightarrow B$. In tal caso si dice anche che hanno la stessa cardinalità. Per esempio l' insieme dei numeri naturali $\mathbb{N}$ e l' insieme dei numeri naturali pari $\mathbb{N}_{pari}$ sono equipotenti: esiste una biiezione $\varphi : \mathbb{N} \leftrightarrow \mathbb{N}_{pari}$ data da $\varphi(n) = 2n, n \in \mathbb{N}$.

• Se A è finito e $B \subseteq A$, si ha $|B| \leq |A|$.

• Se A è finito:
i) ogni applicazione iniettiva $f : A \to A$ è anche suriettiva, e quindi biiettiva.
ii) ogni applicazione suriettiva $f : A \to A$ è anche iniettiva, e quindi biiettiva.
Questi asserti non valgono necessariamente se A è un insieme infinito. Esempio: l' applicazione $\varphi : \mathbb{N} \to \mathbb{N}$ definita da $\varphi(0) = 0,\ \varphi(x) = x - 1$ per x intero > 1, è suriettiva ma non iniettiva. L' applicazione $\psi : \mathbb{N} \to \mathbb{N}$ definita da $\psi(x) = x + 1$ per $x \in \mathbb{N}$, è iniettiva ma non suriettiva.

• Se A e B sono insiemi finiti disgiunti si ha $|A \cup B| = |A| + |B|$.
Se A e B sono insiemi finiti si ha $|A \cup B| = |A| + |B| - |A \cap B|$.
Se A e B sono insiemi finiti si ha $|A \times B| = |A| \cdot |B|$, da cui segue che $|A^n| = |A|^n$.

• Se A e B sono insiemi finiti, si indica con B^A l' insieme di tutte le applcazioni f da A da B. Si ha allora $|B^A| = |B|^{|A|}$.

Dimostrazione: sia $|A| = m$ e $|B| = n$. Una applicazione f è definita dalla sua immagine su tutti gli elementi di A, cioè dagli elementi di B: $f(a_1), f(a_2), ..., f(a_m)$. Per ogni immagine $f(a_i)$ possiamo scegliere un elemento di B in n modi, e quindi le scelte possibili per la sequenza $f(a_1), f(a_2), ..., f(a_m)$ sono n^m. □

• Se $|A| = m$ e $|B| = n$, il numero delle applicazioni iniettive $A \to B$ è 0 se $m > n$, e $n!/(n - m)!$ se $m \leq n$.

Dimostrazione: è chiaro che se gli elementi di B sono in numero minore degli elementi di A, non possono esserci applicazioni f iniettive da A a B (necessariamente si dovrà avere $f(a_i) = f(a_j)$ per almeno due elementi distinti a_i, a_j di A). Se invece $m \leq n$, quanti modi ci sono per distribuire n elementi di B in queste m immagini ? Per $f(a_1)$ abbiamo n scelte possibili (cioè $f(a_1)$ può essere uguale a uno degli n elementi di B), per $f(a_2)$ rimangono $n-1$ scelte possibili, e così via. Quindi ci sono $n(n-1)(n-2)\cdots(n-m+1) = n!/(n-m)!$ modi di scegliere gli elementi di B da assegnare alla sequenza $f(a_1), f(a_2), ..., f(a_m)$. □

• In modo equivalente, possiamo dire che il numero di disposizioni di n oggetti in m posti è $n!/(n - m)!$.

• Se$|A| = n$, le biiezioni $A \leftrightarrow A$ si chiamano anche *permutazioni*. Il loro numero si ricava dalla formula di sopra per $n = m$, e cioè $n!$. Una permutazione f è individuata da $f(a_1), ..., f(a_n)$, e viene denotata come segue

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix} \tag{5.1}$$

dove per semplicità gli oggetti $a_1, ...a_n \in A$ vengono denotati con $1, ...n$. Esempio: le permutazioni f dell' insieme $\{1, 2, 3\}$ sono le 3! biiezioni

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

La permutazione inversa f^{-1} di f si ottiene scambiando le due righe e riordinando le colonne in modo che la prima riga diventi $1, 2, ...n$. La composizione di due permutazioni è una permutazione (la composizione di applicazioni biiettive è ancora un' applicazione biiettiva).

Esercizio: trovare la permutazione risultante dalla composizione $f \circ g$ delle due permutazioni

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}, \; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix} \tag{5.2}$$

5.1 Coefficienti binomiali

Sono definiti come segue[3], con $n, k \in \mathbb{N}$ e $k \leq n$:

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k! \; (n-k)!} \tag{5.3}$$

Nascono dalla formula del binomio:

$$(x+y)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} x^{n-k} y^k, \quad \forall x, y \in \mathbb{R}, \; \forall n \in \mathbb{N} \tag{5.4}$$

Per esempio, se $n = 3$:

$$(x+y)^3 = \begin{pmatrix} 3 \\ 0 \end{pmatrix} x + \begin{pmatrix} 3 \\ 1 \end{pmatrix} x^2 y + \begin{pmatrix} 3 \\ 2 \end{pmatrix} x y^2 + \begin{pmatrix} 3 \\ 3 \end{pmatrix} y^3 = x^3 + 3x^2 y + 3xy^2 + y^3 \tag{5.5}$$

Esercizio: dimostrare per induzione su n la formula del binomio usando l' identità:

$$\begin{pmatrix} n-1 \\ k-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} \tag{5.6}$$

[3]Si ricorda che per $n \in \mathbb{N}^*$ il *fattoriale* di n è definito da $n! = n(n-1)(n-2)\cdots 1$. Inoltre si pone $0! = 1$.

Esercizio: verificare la formula di sopra, e derivarne il metodo grafico per determinare i coefficienti binomiali, detto triangolo di Tartaglia:

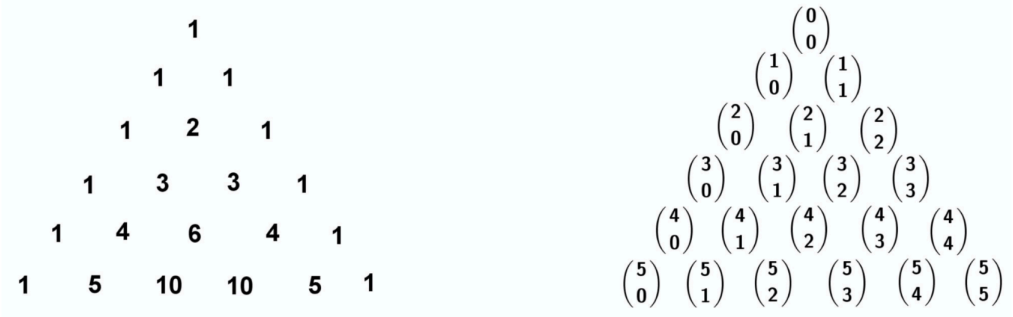


Fig. 5.1 Triangolo di Tartaglia per i coefficienti binomiali

Teorema: siano $n, k \in \mathbb{N}$ e $n \geq k$. Un insieme di cardinalità n ha $\left(\begin{array}{c} n \\ k \end{array} \right)$ sottoinsiemi di cardinalità k.

Dimostrazione: abbiamo visto nella Sezione precedente che il numero di disposizioni di n oggetti in k posti è dato da $n!/(n-k)!$. Quindi ci sono $n!/(n-k)!$ modi di scegliere k elementi, in un certo ordine, da un insieme di n elementi. Ma nel formare un sottoinsieme, l' ordine con cui i suoi elementi compaiono nella lista degli elementi è irrilevante (per esempio i due sottoinsiemi $\{1,2\}$ e $\{2,1\}$ sono uguali). Bisogna quindi dividere $n!/(n-k)!$ per il numero delle permutazioni di k oggetti, cioè per $k!$, ottenendo $\left(\begin{array}{c} n \\ k \end{array} \right)$. $\square$

Esercizio: in quanti modi una commissione di 10 persone può formare una sottocommissione di tre persone ?

Esercizio: quante partite ci sono in un girone all' italiana con 9 squadre ?

Esercizio: dimostrare le seguenti identità

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right) \tag{5.7}$$

$$\left(\begin{array}{c} n \\ 0 \end{array} \right) + \left(\begin{array}{c} n \\ 1 \end{array} \right) + \cdots + \left(\begin{array}{c} n \\ n \end{array} \right) = 2^n \tag{5.8}$$

$$\left(\begin{array}{c} n \\ 0 \end{array} \right) - \left(\begin{array}{c} n \\ 1 \end{array} \right) + \cdots + (-1)^n \left(\begin{array}{c} n \\ n \end{array} \right) = 0 \tag{5.9}$$

5.2 Insiemi infiniti

Esempi di insiemi infiniti: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, ...$

• Un insieme A si dice *numerabile* se è equipotente a $\mathbb{N}$, cioè se esiste una biiezione tra A e $\mathbb{N}$. In tal caso la cardinalità di A è la cardinalità di $\mathbb{N}$, e quest' ultima si indica convenzionalmente con $\aleph_0$, dove $\aleph$ (aleph) è la prima lettera dell' alfabeto ebraico:

$$|A| = |\mathbb{N}| = \aleph_0 \tag{5.10}$$

Teorema: $\mathbb{Z}$ è numerabile. Dimostrazione: immediata.

Teorema: $\mathbb{Q}$ è numerabile. Dimostrazione: basta enumerare (e quindi mettere in relazione biunivoca con $\mathbb{N}$) tutte le frazioni. Per esempio:

$$\begin{array}{l} 1/1 \\ 1/2 \;\; 2/1 \\ 1/3 \;\; \cancel{2/2} \;\; 3/1 \\ 1/4 \;\; 2/3 \;\; 3/2 \;\; 4/1 \\ 1/5 \;\; \cancel{2/4} \;\; \cancel{3/3} \;\; \cancel{4/2} \;\; 5/1 \\ \ldots\ldots \end{array} \tag{5.11}$$

dove la j-esima riga contiene le frazioni per le quali numeratore e denominatore si sommano a j, e si cancellano quelle frazioni che sono già contenute nelle righe precedenti.

Teorema (Cantor): $\mathbb{R}$ non è numerabile. Dimostrazione: per assurdo, con il metodo diagonale di Georg Cantor. Nota preliminare: basta dimostrare che l' insieme dei numeri reali compresi tra 0 e 1 non è numerabile. Supponiamo che questo insieme sia numerabile, e che quindi esista una biiezione φ tra $\mathbb{N}$ e $\mathbb{R}$:

$$\begin{array}{l} \varphi(1) = 0, a_{-1}a_{-2}a_{-3}...a_{-N}... \\ \varphi(2) = 0, a'_{-1}a'_{-2}a'_{-3}...a'_{-N}... \\ \varphi(3) = 0, a''_{-1}a''_{-2}a''_{-3}...a''_{-N}... \\ \quad \vdots \qquad\qquad\qquad \vdots \end{array} \tag{5.12}$$

dove a destra scriviamo in notazione decimale tutti i numeri reali compresi tra 0 e 1 (e a_{-j} è la j-esima cifra decimale dopo la virgola). Dimostriamo ora che esiste un numero reale r non presente in questo elenco. Infatti consideriamo il numero reale

$$r = 0, b_{-1}b_{-2}b_{-3}...b_{-N}... \tag{5.13}$$

con $b_{-j} = 0$ se la j-esima cifra decimale di $\varphi(j)$ è diversa da 0, e $b_{-j} = 1$ altrimenti. Questo numero r deve essere diverso da ogni numero della lista infinita di sopra. Infatti è diverso da $\varphi(1)$ poichè la sua prima cifra decimale è diversa da a_{-1}, è

diverso da $\varphi(2)$ poichè la sua seconda cifra decimale è diversa da a'_{-2}, è diverso da $\varphi(3)$ poichè la sua terza cifra decimale è diversa da a''_{-3} e così via. Quindi l' applicazione φ non è suriettiva, e non può essere una biiezione tra $\mathbb{N}$ e $\mathbb{R}$. $\square$

Esercizi: dimostrare che

i) $\mathbb{R}$ è equipotente al suo sottoinsieme formato dai numeri reali compresi tra 0 e 1. Suggerimento: usare un metodo grafico, con un cerchio e una retta tangente al cerchio.

ii) $\mathbb{R}$ è equipotente a $\mathbb{R} \times \mathbb{R}$, e quindi anche a $\mathbb{R}^n$. Suggerimento: ogni numero reale r può essere posto in corrispondenza biunivoca con due numeri reali compresi tra 0 e 1, dati dalle due sequenze numeriche di cifre che individuano la parte intera ("prima della virgola") e la parte frazionaria ("dopo la virgola") di r.

iii) l' insieme delle parti di $\mathbb{N}$ è equipotente a $\mathbb{R}$. Suggerimento: usare il metodo diagonale di Cantor.

Nota: dalla ii) segue che $\mathbb{R}$ è equipotente a $\mathbb{R}^n$.

5.3 Ordinamenti

• Una relazione ρ in un insieme A si dice *antisimmetrica* se $\forall a, b \in A$, $a \ \rho \ b$ e $b \ \rho \ a$ implicano che $a = b$.

• **Ordinamento parziale:** relazione ρ riflessiva, antisimmetrica e transitiva.

Esempi:

1) la relazione $\leq$ in $\mathbb{N}$
2) la relazione "divide" in $\mathbb{N} - \{0\}$: se a e b sono due numeri naturali diversi da 0, $a \ \rho \ b$ se $a \mid b$ (a divide b).
3) la relazione in $\mathbb{N} - \{0\}$ definita da $a \ \rho \ b$ se $\frac{1}{a} \leq \frac{1}{b}$.

Esercizio: dimostrare che queste tre relazioni sono degli ordinamenti parziali.

Nota: in generale non tutti gli elementi dell' insieme A risultano necessariamente in relazione tra loro. Per esempio nel caso della relazione 2) , i numeri 3 e 5 non sono in relazione tra loro: infatti 3 non divide 5 e viceversa. Quando invece $\forall a, b \in A$ si ha $a \ \rho \ b$ oppure $b \ \rho \ a$, allora l' ordinamento si dice *totale*.

Si usa indicare un insieme A dotato di un ordinamento parziale con il simbolo $(A, \leq)$, dove la grafia $\leq$ indica appunto un ordinamento parziale. Dato un ordinamento parziale $\leq$ si può definire l' ordinamento parziale inverso $\geq$: per ogni $a, b \in A$ si ha $a \geq b$ se e solo se $b \leq a$.

Esercizio: verificare che $\geq$ è un ordinamento parziale.

In un insieme parzialmente ordinato $(A, \leq)$ un elemento $a \in A$ si dice:

- il *minimo* di A se $a \leq x$ per ogni $x \in A$.
- il *massimo* di A se $x \leq a$ per ogni $x \in A$.
- un *elemento minimale* di A se per ogni $x \in A$ si ha che $x \leq a$ implica $x = a$.
- un *elemento massimale* di A se per ogni $x \in A$ si ha che $a \leq x$ implica $x = a$.

Se $B \subseteq A$, un elemento $a \in A$ si dice:

- un *minorante* di B in A se $a \leq b$ per ogni $b \in B$.
- un *maggiorante* di B in A se $b \leq a$ per ogni $b \in B$.
- *estremo inferiore* di B (in A) se a è il massimo dei minoranti di B in A.
- *estremo superiore* di B (in A) se a è il minimo dei maggioranti di B in A.

Pertanto a è l' estremo inferiore di B se e solo se
i) $a \leq b$ per ogni $b \in B$ e
ii) per ogni $a' \in A$ con la proprietà che $a' \leq b$ per tutti i $b \in B$ si ha $a' \leq a$.
Analogamente a è l' estremo superiore di B se e solo se
i) $b \leq a$ per ogni $b \in B$ e
ii) per ogni $a' \in A$ con la proprietà che $b \leq a'$ per tutti i $b \in B$ si ha $a \leq a'$.

Nota: non è detto che per ogni $(A, \leq)$ e per ogni suo sottoinsieme B esistano sempre massimo, minimo, elementi massimali o minimali, maggioranti o minoranti etc. Per esempio $\mathbb{N}$ con il suo ordinamento naturale non ha massimo e ha 0 come minimo.

Esempio:
1) $\mathbb{N}^* = \mathbb{N} - \{0\}$ con l' ordinamento "divide" (vedi sopra). Questo insieme parzialmente ordinato ha un minimo, il numero 1, in quanto $1 \mid n$ per ogni $n \in \mathbb{N}^*$ e non ha nessun massimo (non esiste nessun $n_0 \in \mathbb{N}^*$ tale che $n \mid n_0$ per ogni $n \in \mathbb{N}^*$). Inoltre 1 è un elemento minimale di $\mathbb{N}^*$, poichè se $n \in \mathbb{N}^*$ e $n \mid 1$, allora $n = 1$. Non esistono invece elementi massimali, poichè per ogni $n_0 \in \mathbb{N}^*$ esiste $n_1 \in \mathbb{N}^*$ tale che $n_0 \mid n_1$ e $n_0 \neq n_1$.
2) Consideriamo ora il sottoinsieme $P^+ \subseteq \mathbb{N}^*$ dei numeri pari positivi. I minoranti di P^+ in $\mathbb{N}^*$ sono i numeri $n \in \mathbb{N}^*$ che dividono tutti i numeri pari, e quindi sono 1 e 2. Nell' insieme $\{1, 2\}$ il numero 2 è il massimo perchè $1 \mid 2$. Ne consegue che 2 è l' estremo inferiore di P^+ in $\mathbb{N}^*$. Invece non esistono $n \in \mathbb{N}^*$ che sono divisibili per tutti gli elementi di P^+, e quindi P^+ non ha maggioranti in $\mathbb{N}^*$, e a maggior ragione, non ha un estremo superiore in $\mathbb{N}^*$.

Esercizio: Sia $D_{>1}$ l' insieme dei numeri dispari maggiori di 1. Definiamo $A = D_{>1} \cup \{2\}$, e supponiamo che l' ordinamento di A sia il "divide". Dimostrare che:
- A ha un solo elemento massimale ma non ha massimo.
- l' estremo inferiore di A in $\mathbb{N}^*$ è il numero 1.

Esercizio: dimostrare che se un insieme parzialmente ordinato A ha un minimo a, allora a è anche l' unico minimo. Analogamente per il massimo.

Esercizio: dimostrare che
- il minimo di A è anche elemento minimale di A. Analogamente il massimo è elemento massimale.
- non vale il viceversa.

6 Grafi

• Un *grafo* è un insieme $V \neq \varnothing$ con relazione simmetrica ρ tale che $v \not\rho\, v$, $\forall v \in V$.

Possiamo rappresentare gli elementi dell' insieme V come punti, e tracciare un arco di curva dal punto che rappresenta v a quello che rappresenta w se $v\ \rho\ w$. Nel caso di un grafo la relazione ρ è simmetrica, e quindi l' arco che congiunge v e w non è orientato. Il diagramma che si ottiene contiene tutta l' informazione del grafo, cioè l' insieme degli elementi di V, chiamati *vertici*, e delle linee $\{v, w\}$, chiamate *lati* del grafo.

Un grafo G è quindi individuato da l' insieme V dei vertici e l' insieme L dei suoi lati:

$$L = \{\{v, w\} \mid v, w \in V, v\ \rho\ w\} \tag{6.1}$$

Si può denotare il grafo G col simbolo (V, L).

Esempio: consideriamo il grafo $G = (V, L)$ per il quale si ha:

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6\}, \quad L = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7\} \tag{6.2}$$

con

$$\begin{aligned} &l_1 = \{v_1, v_5\}, l_2 = \{v_4, v_6\}, l_3 = \{v_3, v_2\}, l_4 = \{v_1, v_2\}, \\ &l_5 = \{v_5, v_4\}, l_6 = \{v_3, v_4\}, l_7 = \{v_5, v_2\} \end{aligned} \tag{6.3}$$

Il diagramma che lo rappresenta può essere disegnato con vari stili:

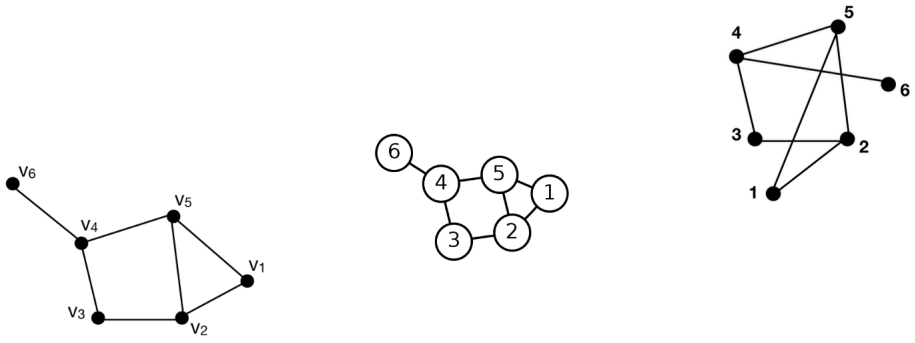


Fig. 6.1 diversi modi per rappresentare lo stesso grafo

Il modo di disporre i vertici sul piano è del tutto arbitrario, basta che vengano collegati con una linea a due a due i vertici indicati nella lista dei lati. Le etichette $v_1, v_2, ...$ dei vertici sono utili quando si definisce il grafo tramite la lista L dei suoi lati, ma possono essere superflue se il grafo viene rappresentato col diagramma corrispondente.

• Due vertici si dicono *adiacenti* se sono estremi dello stesso lato

• Se due lati hanno un vertice in comune, si dicono *incidenti*.

• Se $G = (V, L)$ e $G' = (V', L')$ sono due grafi, un *isomorfismo* di G in G' è una biiezione $\varphi : V \to V'$ tale che $\{v, w\} \in L$ implica $\{\varphi(v), \varphi(w)\} \in L'$ e viceversa. Due grafi G e G' si dicono isomorfi se esiste un isomorfismo tra G e G'. Per esempio i grafi in Fig. 6.2 sono tra loro isomorfi.

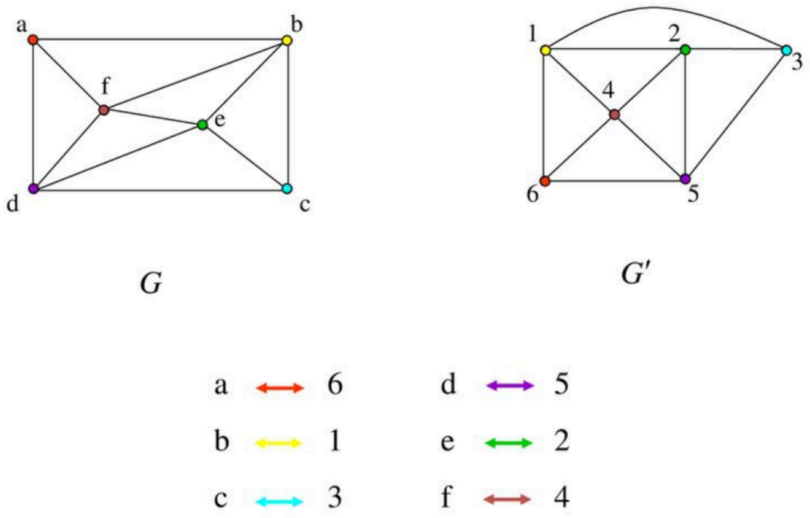


Fig. 6.2 Grafi isomorfi

• Un *automorfismo* di G è un isomorfismo da G in G.

• Se $G = (V, L)$ è un grafo, V' è un sottoinsieme di V e L' è un sottoinsieme di L tale che ogni lato in L' unisca vertici contenuti in V', allora $G' = (V', L')$ è un grafo, detto *sottografo* di G.

• Un grafo $G = (V, L)$ è un grafo *finito* se V è un insieme finito (e allora anche L è finito).

• Se $G = (V, L)$ è un grafo finito, il *grado* di un vertice $v \in V$ è il numero di lati incidenti su v, e si indica con $d(v)$. Se questo numero è pari (dispari) il vertice si dice pari (dispari). Un vertice con $d(v) = 0$ si dice *isolato*.

Osservazione: il numero di lati di un grafo finito, cioè $|L|$ (numero di elementi dell' insieme L) è uguale alla semisomma dei gradi di tutti i vertici del grafo:

$$|L| = \frac{1}{2} \sum_{v \in V} d(v) \tag{6.4}$$

Dimostrazione: immediata notando che ogni lato incide su due vertici. Corollario: ogni grafo finito ha un numero pari di vertici dispari, poichè dalla formula di sopra risulta che la somma dei gradi è sempre pari.

Nota: un isomorfismo φ tra grafi $G = (V, L)$ e $G' = (V', L')$ conserva i gradi dei vertici, cioè per ogni vertice $v \in V$ si ha $d(v) = d(\varphi(v))$. Dimostrazione: immediata dalla definizione di isomorfismo.

• Se in un grafo tutti i vertici hanno stesso grado, il grafo si dice *regolare*.
Esercizio: disegnare tutti i grafi regolari con un numero n di vertici fino a $n = 6$.

Un grafo *orientato* è un insieme V su cui è definita una relazione (non necessariamente simmetrica). Le linee che congiungono i vertici sono allora linee orientate.

• Un *multigrafo* è un grafo in cui due vertici possano essere uniti da più di un lato. In un *multigrafo orientato* il lati del multigrafo sono orientati, e si ammettono anche lati che escono e entrano nello stesso vertice (formando un *cappio*), vedi la Fig. 6.3.

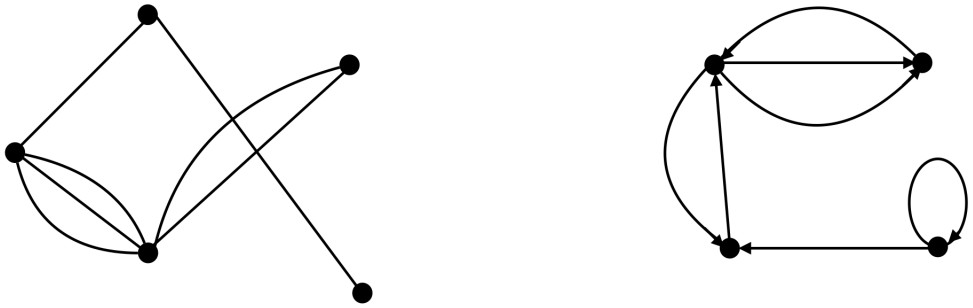


Fig. 6.3 Multigrafo e multigrafo orientato

• Un *cammino* da v a w in un grafo G è una successione finita $l_1 = \{v_1, v_2\}, l_2 = \{v_2, v_3\}, l_m = \{v_m, v_{m+1}\}$ di lati *distinti* di G con $v = v_1$ e $w = v_{m+1}$. Quindi un cammino si percorre sul grafo con una penna senza mai staccarla dal foglio, e se si percorrono m lati il cammino si dice di lunghezza m. Un cammino di lunghezza > 0 da v a v si chiama *cammino chiuso* o *circuito*.

• Un grafo $G = (V, L)$ si dice *connesso* se per ogni $v, w \in V$ esiste un cammino da v a w.

• Un grafo si dice *completo* se tutti i suoi vertici sono a due a due adiacenti (ogni vertice è collegato da un lato a tutti gli altri). I grafici completi fino a 7 vertici, sono riportati in Fig. 6.4, e quello con 28 vertici nella pagina di copertina.

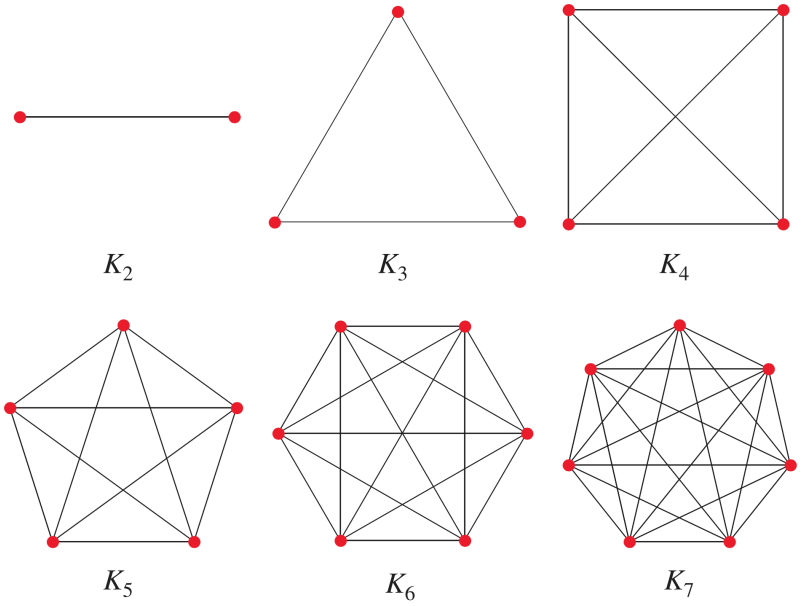


Fig. 6.4 Grafi completi fino a 7 vertici.

6.1 Cammini e circuiti euleriani

Un *cammino o circuito euleriano* è un cammino o un circuito che percorre tutti i lati di un multigrafo una sola volta.

Teorema (Eulero, 1736): un multigrafo finito G privo di vertici isolati ammette un circuito euleriano se e solo se G è connesso e tutti i suoi vertici sono pari.

Dimostrazione:

1) Sia $G = (V, L)$ un multigrafo finito privo di vertici isolati, con circuito euleriani. Dimostriamo che G è connesso. Infatti essendo G privo di vertici isolati, ogni suo vertice appartiene sempre almeno a un lato di G, e quindi il circuito euleriano (che percorre tutti i lati) tocca tutti i vertici di G. Ne consegue che G è connesso.

2) Fissiamo ora un vertice v_0 e percorriamo tutto il circuito euleriano partendo da v_0. Ogni volta che si incontra un vertice, si entra e si esce dal vertice per due lati che non erano stati percorsi in precedenza. Ne discende che tutti i vertici (eccetto al più v_0) sono di grado pari. Lo stesso ragionamento vale per v_0: il percorso euleriano può attraversarlo più di una volta, ogni attraversamento necessita due lati non precedentemente percorsi, e questi lati va aggiunto il lato di partenza e il lato di arrivo finale su v_0. Anche v_0 deve allora avere grado pari. Abbiamo quindi dimostrato la parte "solo se" del Teorema di Eulero.

3) Viceversa supponiamo ora che G sia un multigrafo finito, senza vertici isolati, connesso, e con tutti i vertici pari. Dobbiamo dimostrare che allora esiste un circuito euleriano in G. Fissiamo un qualsiasi vertice v_0. Dato che v_0 non è isolato, esiste almeno un lato a cui questo vertice appartiene. Si parte da v_0 e si percorre questo lato. Ogni volta che si arriva a un nuovo vertice, questo appartiene a un numero

pari di lati (per ipotesi) e quindi si può sempre scegliere un lato di uscita che non sia stato ancora percorso. In questo modo ogni volta che si passa per un vertice si usano due lati incidenti nel vertice, e quindi il numero dei lati incidenti nel vertice e non ancora percorsi rimane pari. Il processo può finire solamente quando si raggiungerà l' unico vertice lasciato momentaneamente con un numero dispari di lati non ancora percorsi, e cioè v_0. D' altra parte il processo deve necessariamente avere termine, essendo G un multigrafo finito. Si conclude che esiste un cammino da v_0 a v_0, cioè un circuito C_1. Naturalmente non è detto che C_1 percorra tutti i lati di G e che quindi sia un circuito euleriano.

4) Consideriamo allora il sottomultigrafo ottenuto da G togliendo tutti i lati di C_1. Si ottiene un multigrafo, non necessariamente connesso, ma sempre con tutti i vertici pari. Si ripete quindi il procedimento, costruendo un circuito C_2. Continuando, si trova una sequenza finita $C_1, C_2, ...C_k$ di circuiti aventi a due a due nessun lato in comune, e tale che tutti i lati del multigrafo G appartengono a uno di questi circuiti. (i circuiti individuano una partizione dell' insieme L dei lati di G). Almeno due di questi circuiti devono incontrarsi in qualche vertice, altrimenti G non sarebbe connesso. Se C_i e C_j passano entrambi per il vertice w, percorrendo prima C_i da w a w e poi C_j da w a w si ottiene un circuito $C_{i,j}$ da w a w. Sostituendo nella lista dei circuiti il circuito $C_{i,j}$ alla coppia di circuiti C_i e C_j si ottiene una partizione di L in $k-1$ circuiti. Iterando si ottiene un unico cammino C, che è un circuito euleriano per G. □

Corollario: un multigrafo finito G privo di vertici isolati ha un cammino euleriano se e solo se è connesso e ha zero o due vertici dispari.

Dimostrazione: supponiamo che G abbia un cammino euleriano da un vertice v a un vertice w. Se questo cammino è un circuito, per il Teorema precedente si conclude che G è connesso e ha zero vertici dispari. Se il cammino non è un circuito, ragionando come nel teorema precedente, si conclude che tutti i vertici sono pari, eccetto al più il vertice di partenza v e il vertice di arrivo w. Da v si esce una volta in più (quando si è partiti), e quindi v deve essere dispari. In w si arriva una volta in più (a conclusione del cammino) e quindi deve essere dispari. Pertanto v e w sono i due soli vertici dispari.

Viceversa, se G ha zero vertici dispari, G ha un circuito euleriano per il Teorema precedente. Se invece G ha due vertici dispari v e w, possiamo considerare il multigrafo G' ottenuto aggiungendo un vertice v_0 e collegandolo con un lato l a v e con un altro lato l' a w. In G' tutti i vertici sono pari, e quindi per il teorema di Eulero G' ha un circuito euleriano. Sopprimendo ora in questo circuito i due lati l, l' si ottiene un cammino euleriano da v a w. □

Nota: si osservi che le dimostrazioni del Teorema di Eulero e del Corollario contengono dei procedimenti effettivi per costruire il circuito (o il cammino) euleriano cercato. In particolare si è visto che se vi sono due vertici dispari, questi devono essere necessariamente gli estremi del cammino euleriano.

6.2 Cammini e circuiti hamiltoniani

Un *cammino hamiltoniano* in un multigrafo finito è un cammino che passa una sola volta per ogni vertice del multigrafo.

Esempio: nella Fig. 6.5 i multigrafi G_1 e G_2 hanno un cammino euleriano, mentre i multigrafi G_3 e G_4 non hanno un cammino euleriano. I multigrafi G_1 e G_3 hanno un cammino hamiltoniano, mentre i multigrafi G_2 e G_4 non hanno un cammino hamiltoniano. Si vede da questi esempi che non sembra esserci alcun rapporto tra esistenza di un cammino euleriano e esistenza di un cammino hamiltoniano.

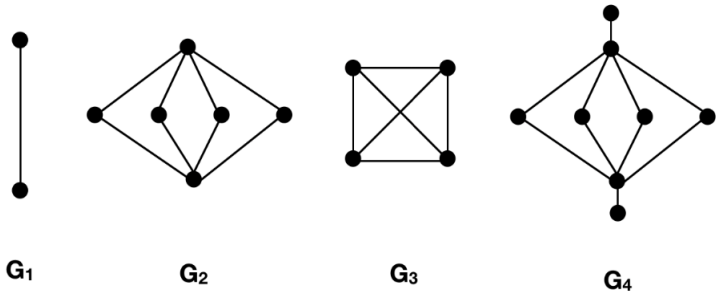


Fig. 6.5 Cammini euleriani e cammini hamiltoniani

• Le definizioni di cammini euleriani e hamiltoniani possono essere adattate ai multigrafi finiti orientati.

Teorema: ogni multigrafo finito orientato completo ha un cammino orientato hamiltoniano. Per la (semplice) dimostrazione cf. [1], p. 119.
Nota: questo teorema non può essere esteso ai *circuiti* orientati hamiltoniani. Infatti il multigrafo orientato con due soli vertici ha un cammino hamiltoniano ma non un circuito hamiltoniano.

6.3 Altre caratteristiche dei grafi

• La *distanza* tra due vertici v e w in un multigrafo connesso $G = (V, L)$ è il minimo delle lunghezze di tutti i cammini da v a w, e si indica con $d(v, w)$. Si ha, per ogni $u, v, w \in V$:

$$\begin{aligned} &d(v,w) = 0 \quad \Leftrightarrow \quad v = w \\ &d(v,w) = d(w,v) \\ &d(u,v) + d(v,w) \geq d(u,w) \end{aligned} \tag{6.5}$$

• Il *diametro* di $G = (V, L)$ è dato dal massimo dell' insieme $\{d(u, v) \mid u, v \in V\}$. Per esempio il diametro del grafo in Fig. 6.1. è 3.

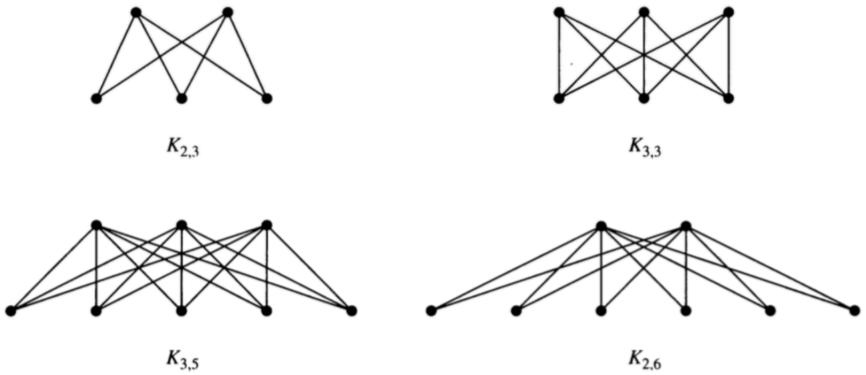


Fig. 6.6 Esempi di grafi bipartiti completi

• Un grafo $G = (V, L)$ si dice *bipartito* se esiste una partizione $\{V_1, V_2\}$ di V tale che ogni lato di G abbia un estremo in V_1 e l' altro in V_2. Un *grafo bipartito completo* è definito da

$$\begin{aligned} V &= \{v_1, ...v_m, w_1, ...w_n\} \\ L &= \{\{v_i, w_j\} \mid i = 1, ...m \ , \ j = 1, ...n\} \end{aligned} \tag{6.6}$$

e viene denotato con $K_{i,j}$. Alcuni esempi di grafi bipartiti completi sono riportati in Fig. 6.6.

• Per un grafo finito G si definisce la matrice di adiacenza A come segue: $A_{ij} = 1$ se i vertici v_i e v_j sono adiacenti, altrimenti $A_{ij} = 0$. Evidentemente A è simmetrica. La matrice di adiacenza contiene tutta l' informazione del grafo, ed è un modo alternativo per codificare questa informazione. Un esempio della sua utilità è dato dal teorema: se $l > 0$, $(A^l)_{ij}$ è il numero di catene di lunghezza l da v_i a v_j, dove una *catena* è una sequenza finita di lati non necessariamenti distinti tra loro (come sarebbe per un cammino). Per la dimostrazione vedi [1], p. 121.

Esercizio: modellare il problema dei sette ponti di Königsberg (vedi Fig. 6.10) con un multigrafo G, e dimostrare che non esiste un circuito euleriano in G.

6.4 Alberi e grafi piani

• Un *albero* è un grafo connesso privo di circuiti.

• Una *foresta* è un grafo privo di circuiti. Può essere quindi formato da più alberi sconnessi fra loro.

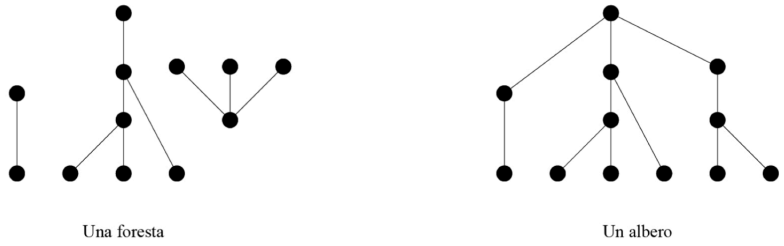


Fig. 6.7 Alberi e foreste

• In un albero esiste un solo cammino tra due vertici qualunque v e w. Pertanto $d(v, w) = t$ se $l_1, ...l_t$ è l' unico cammino da v a w.

• Un modo standard per disegnare un albero è quello di scegliere un vertice e disporre su righe successive i vertici a distanze crescenti.

Osservazioni:

- se si toglie un lato a un albero, si ottiene un grafo sconnesso.
- un albero con n vertici ha $n - 1$ lati (si dimostra per induzione).
- un grafo connesso con n vertici e $n - 1$ lati è un albero.

Multigrafo piano: è un multigrafo $G = (V, L)$ dove V è un insieme di punti in un piano, L è un insieme di archi di curve (i "lati") nel piano, e due lati distinti si intersecano al più nei loro estremi. Per esempio i grafi G_1, G_2, G_4 della Fig. 6.5. sono grafi piani.

• Un multigrafo si dice *planare* se è isomorfo a un multigrafo piano. Per esempio il grafo G_3 della Fig. 6.5 è isomorfo al primo grafo piano della Fig. 6.8, e quindi è planare.

• Un multigrafo piano finito suddivide il piano in *regioni*, vedi ad esempio la Fig. 6.8. Le regioni si chiamano *facce* del multigrafo. Nota: la regione 4 del primo grafo e la regione 6 del secondo grafo sono illimitate.

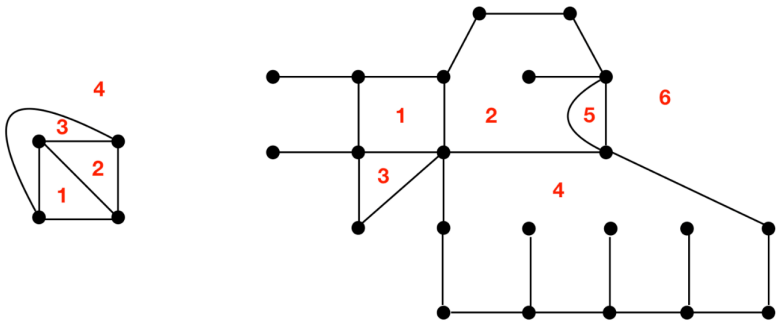


Fig. 6.8 Grafi piani: suddividono il piano in regioni

Teorema (Eulero): se G è un multigrafo piano finito connesso con $|V|$ vertici, $|L|$ lati e F facce, si ha:

$$|V| - |L| + |F| = 2 \tag{6.7}$$

Dimostrazione: per induzione sul numero dei lati. Se $|L| = 0$, necessariamente $|V| = 1$, $|F| = 1$ e il teorema è verificato. Consideriamo ora un multigrafo $G = (V, L)$ con $|L| \geq 1$ lati e distinguiamo due casi:

i) G non ha un circuito
ii) G ha un circuito

Se vale i), G ha tutti lati semplici (cioè due vertici adiacenti sono collegati da un solo lato) e quindi G è un grafo. Essendo connesso e privo di circuiti è un albero, il che implica $|L| = |V| - 1$ e $|F| = 1$. Pertanto $|V| - |L| + |F| = 2$.

Se vale ii), sia G' il sottomultigrafo di G ottenuto togliendo un lato del circuito. Allora G' è piano, connesso, ha $|V|$ vertici, $|L| - 1$ lati e $|F| - 1$ facce, in quanto due facce di G sono state riunite in un' unica faccia di G' rimuovendo un lato del circuito. Per l' ipotesi induttiva applicata a G' (cioè si assume valido il teorema per multigrafi piani connessi con $|L| - 1$ lati) si ha

$$|V| - (|L| - 1) + (|F| - 1) = 2 \quad \Leftrightarrow \quad |V| - |L| + |F| = 2 \tag{6.8}$$

e quindi il teorema è dimostrato per ogni multigrafo piano finito connesso. □

Corollario: Se $G = (V, L)$ è un grafo planare finito si ha

$$|L| \leq 3|V| - 6 \tag{6.9}$$

Dimostrazione: siano $G_i = (V_i, L_i)$ le componenti connesse di G. Basta dimostrare il corollario per ogni componente connessa. Ogni faccia di G_i ha per bordo un circuito di lunghezza ≥ 3. Ogni linea fa parte del bordo comune a due facce, e allora si ha $|L| \geq \frac{3}{2}|F|$ (bisogna dividere per 2 altrimenti ogni linea viene contata due volte). Applicando la formula di Eulero a G_i si trova

$$|V_i| = |L_i| - |F_i| + 2 \geq |L_i| - \frac{2}{3}|L_i| + 2 = \frac{1}{3}|L_i| + 2 \quad \Rightarrow \quad |L_i| \leq 3|V_i| - 6 \tag{6.10}$$

e sommando membro a membro le disuguaglianze $|L_i| \leq 3|V_i| - 6$ il Corollario è dimostrato. □

Corollario: il grafo completo K_5 non è planare. Dimostrazione: per K_5 si ha $|V| = 5$ e $|L| = 10$, e non vale la disuguaglianza $|L| \leq 3|V| - 6$ valida per tutti i grafi planari finiti. □

Teorema di Kuratowski: Un grafo finito è planare se e solo se non contiene sottografi isomorfi a K_5 o a $K_{3,3}$. Il teorema, di dimostrazione non elementare, è molto utile per determinare se un grafico è planare o non planare.

Teorema dei quattro colori. Ogni multigrafo planare finito ha una 4-colorazione. Per k-colorazione di un multigrafo $G = (V, L)$ si intende un' applicazione $\chi : V \to \{1, 2, ...k\}$ tale che $\chi(v) \neq \chi(w)$ per ogni coppia v, w di vertici adiacenti.

E' un teorema molto famoso della teoria dei grafi. La sua dimostrazione (Appel e Hakern, 1977) è estremamente lunga e difficile, e alcune sue parti sono trattate al calcolatore. E' invece abbastanza semplice dimostrare l' esistenza di una 5-colorazione (vedi [1] p. 133). Il teorema dei quattro colori implica immediatamente che ogni carta geografica politica può essere colorata con quattro colori, in modo che nessuna coppia di nazioni confinanti abbia lo stesso colore (dimostrarlo).

Solidi platonici. Sono poliedri regolari: le facce sono poligoni regolari congruenti tra loro, i vertici hanno tutti lo stesso grado. Proiettando da un punto opportuno i lati di un poliedro regolare su un piano si ottiene un grafo piano.

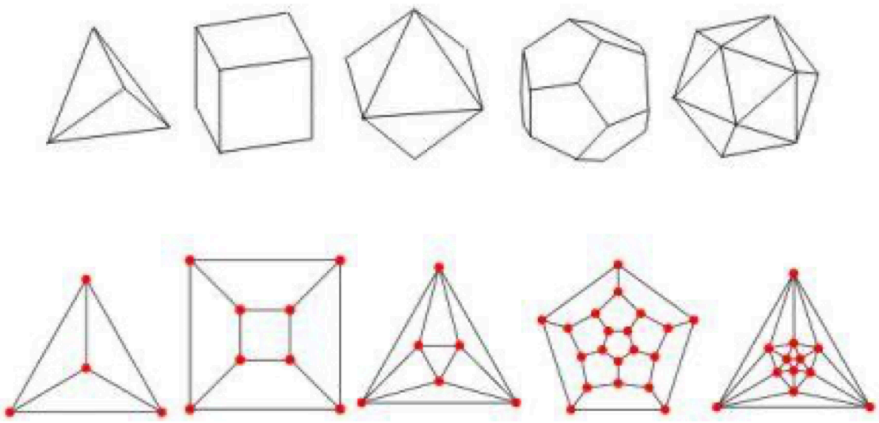


Fig. 6.9 Le proiezioni sul piano dei solidi platonici

Supponiamo di voler determinare i solidi platonici le cui facce sono poligoni con p angoli e con vertici di grado q. Nel grafo piano corrispondente si ha

$$|L| = \frac{q}{2}|V| \tag{6.11}$$

vedi l' equazione (6.4). Ogni faccia ha p lati, e quindi le facce sono delimitate complessivamente da $p|F|$ lati. Però in questo conteggio ogni lato è contato due volte (perchè separa due facce) e allora

$$|L| = \frac{p}{2}|F| \tag{6.12}$$

Dalla formula di Eulero si ha:

$$\frac{2}{q}|L| - |L| + \frac{2}{p}|L| = 2 \quad \Rightarrow \quad \frac{2p - pq + 2q}{pq}\,|L| = 2 \tag{6.13}$$

In particolare bisogna avere $2p-pq+2q > 0$ che implica anche $4 > 4-(2p-pq+2q) = (p-2)(q-2)$. Quindi deve valere la disuguaglianza:

$$(p-2)(q-2) < 4 \tag{6.14}$$

Ricordando ora che un poligono ha almeno tre angoli si deve avere $p \geq 3$. Su un vertice devono incidere almeno tre lati, e quindi si ha $q \geq 3$. Con questi vincoli la disuguaglianza (6.14) ha solo 5 soluzioni :

p=3, q=3 $\rightarrow$ tetraedro
p=3, q=4 $\rightarrow$ ottaedro
p=3, q=5, $\rightarrow$ icosaedro
p=4, q=3, $\rightarrow$ cubo
p=5, q=3, $\rightarrow$ dodecaedro

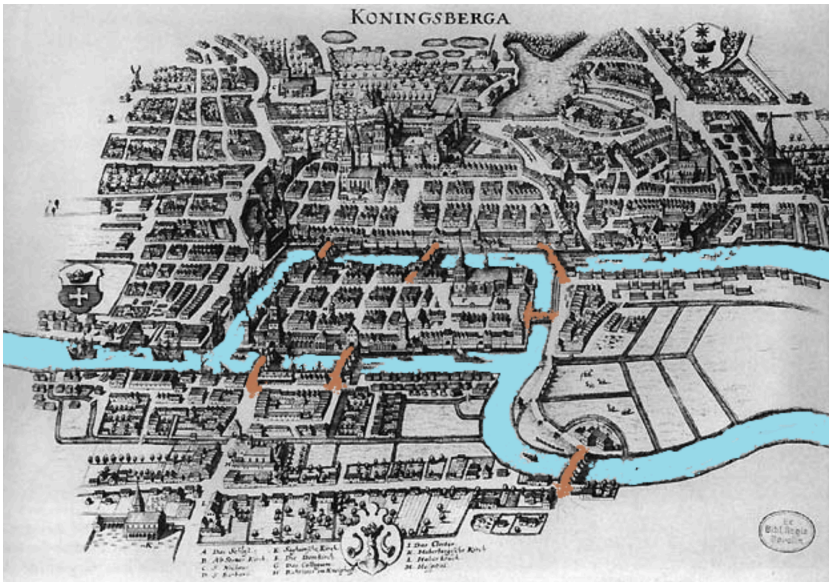


Fig. 6.10 I sette ponti di Königsberg

7 Insiemi dotati di un' operazione

7.1 Operazioni

Se A è un insieme, una *operazione* (detta anche operazione binaria o *legge di composizione*) su A è un' applicazione $\omega : A \times A \to A$. Più in generale una operazione n-aria su A è un' applicazione $A^n = \underbrace{A \times A \times \cdots \times A}_{n} \to A$.

Esempi:

1) addizione, sottrazione, moltiplicazione sono operazioni su $\mathbb{R}$, mentre la divisione è un' operazione su R^*.

2) Se A è un insieme, l' intersezione e l' unione tra sottoinsiemi di A sono operazioni su $P(A)$.

3) Se A^A è l' insieme di tutte le applicazioni di A in A, la composizione di due applicazioni è un' operazione su A^A.

Le operazioni tra due elementi a e b si denotano con simboli del tipo $+, \cdot, \star, \circ$ etc., oppure scrivendo ab senza alcun simbolo. Un insieme A su cui è definita una operazione $\star$ è anche detto *struttura algebrica* e viene indicato con $(A, \star)$.

7.2 Semigruppi

• Un *semigruppo* $(S, \star)$ è un insieme S dotato di un' operazione $\star$ **associativa**:

$$(a \star b) \star c = a \star (b \star c), \quad \forall a, b, c \in S \tag{7.1}$$

Quindi le parentesi non sono necessarie, e si può scrivere semplicemente $a \star b \star c$.

Esempi: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$ sono semigruppi, mentre $(\mathbb{Z}, -)$ non è un semigruppo poichè $(a - b) - c \neq a - (b - c)$. $(A^A, \circ)$ è un semigruppo, con operazione data dalla composizione di applicazioni, poichè la composizione è associativa.

• Un semigruppo $(S, \star)$ si dice *commutativo* se per ogni $a, b \in S$ si ha $a \star b = b \star a$. Esempi: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$ sono semigruppi commutativi. Se A è un insieme, $(P(A), \cup)$ e $(P(A), \cap)$ sono semigruppi commutativi.

• Se $(A, \star)$ è un insieme con un' operazione, un sottoinsieme $B \subseteq A$ si dice *sottoinsieme chiuso* sotto l' operazione $\star$ se $\forall x, y \in B$ si ha $x \star y \in B$. In tal caso $\star$ è un' operazione su B (operazione *indotta*). Per esempio $\mathbb{N}$ è un sottoinsieme di $\mathbb{R}$ chiuso sotto l' addizione e la moltiplicazione.

• Se S è un semigruppo e T un suo sottoinsieme chiuso, allora T con l' operazione indotta dall' operazione su S è un semigruppo: infatti la proprietà associativa vale per ogni $a, b, c \in S$ e quindi per ogni $a, b, c \in T$. In questo caso T si dice sottosemigruppo di S. Per esempio $(\mathbb{N}, +)$ è un sottosemigruppo di $(\mathbb{R}, +)$.

Esercizio: dimostrare che se $B \subseteq A$, allora $(P(B), \cup)$ è un sottosemigruppo di $(P(A), \cup)$, e $(P(B), \cap)$ è un sottosemigruppo di $(P(A), \cap)$.

• Se $(A, \cdot)$ è un semigruppo, si possono definire le potenze n-esime (con $n \in \mathbb{N}^*$) di un elemento $a \in A$ per induzione su n:

$$a^1 = a, \quad a^n = a^{n-1} \cdot a \tag{7.2}$$

da cui si ricavano le relazioni

$$a^n \cdot a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad n, m \in \mathbb{N}^* \tag{7.3}$$

7.3 Monoidi

• Una *identità sinistra* in un semigruppo $(S, \cdot)$ è un elemento $e \in S$ tale che $e \cdot a = a, \ \forall a \in S$. Analogamente una *identità destra* è un elemento $e' \in S$ tale che $a \cdot e' = a, \ \forall a \in S$. Se in S esistono sia una identità sinistra e che una identità destra e', si ha $e = e \cdot e' = e'$, e pertanto identità sinistra e identità destra coincidono.

• Un *monoide* è un semigruppo S nel quale esiste un elemento e chiamato identità, definito da

$$a \cdot e = e \cdot a = a, \quad \forall a \in S \tag{7.4}$$

Osservazione: in un semigruppo, se esiste una identità, è unica. Infatti se ci fossero due identità e, e', in particolare e sarebbe identità sinistra e e' sarebbe identità destra, e quindi $e = e'$.

Esempi:
1) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono monoidi con identità $= 0$.
2) $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ sono monoidi con identità $= 1$.
3) L' insieme delle matrici $n \times n$, con operazione data dalla moltiplicazione matriciale righe per colonne, è un monoide con identità = matrice unità $I_{n \times n}$.
4) $(A^A, \circ)$ è un monoide con identità $= i_A : A \to A$ (applicazione identità sull' insieme A).
5) $(P(A), \cap)$ è un monoide, con identità $= A$

• per un monoide $(M, \cdot)$, le potenze n-esime di un elemento $a \in M$ possono essere definite per $n \geq 0$, ponendo $a^0 =$ identità di M. Valgono allora le stesse formule date in (7.3), con $n, m \in \mathbb{N}$.

• Un sottoinsieme $N \subseteq M$ di un monoide $(M, \cdot)$, che sia lui stesso un monoide $(N, \cdot)$, si dice *sottomonoide* di M.

Esempio: $(\mathbb{N}, +)$ è un sottomonoide di $(\mathbb{R}, +)$.

Esercizio: dimostrare che l' insieme delle matrici 2×2 della forma:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a, b \in \mathbb{R} \tag{7.5}$$

è un sottomonoide del monoide $M_2(\mathbb{R})$ delle matrici 2×2 a elementi in $\mathbb{R}$, con operazione data dalla moltiplicazione matriciale.

7.4 Omomorfismi

Siano $(S, \star)$ e $(S', \circ)$ due semigruppi. Un *omomorfismo di semigruppi* φ di S in S' è un' applicazione $\varphi : S \to S'$ tale che

$$\varphi(x \star y) = \varphi(x) \circ \varphi(y), \quad \forall x, y \in S \tag{7.6}$$

Se $(S, \star)$ e $(S', \circ)$ sono due monoidi con identità 1_S e $1_{S'}$ rispettivamente, un *omomorfismo di monoidi* $\varphi : S \to S'$ è un omomorfismo di semigruppi tale che

$$\varphi(1_S) = 1_{S'} \tag{7.7}$$

Nota: usando la definizione (7.6) si trova $\varphi(x) = \varphi(1_S \star x) = \varphi(1_S) \circ \varphi(x)$ e anche $\varphi(x) = \varphi(x \star 1_S) = \varphi(x) \circ \varphi(1_S)$ per ogni $x \in S$, il che dimostra che $\varphi(1_S)$ funge da identità per l' immagine di φ in S'. Se l' immagine di φ coincide con S' (cioè se φ è suriettiva), allora $\varphi(1_S) = 1_{S'}$. Quindi un omomorfismo di semigruppi è anche omomorfismo di monoidi solo se è un omomorfismo suriettivo.

Esempio: consideriamo i monoidi $(\mathbb{N}, \cdot)$ e $(\mathbb{N} \times \mathbb{N}, \circ)$, dove l' operazione $\circ$ è definita da $(a, b) \circ (c, d) = (ac, bd)$. Si ha $1_{\mathbb{N}} = 1$ e $1_{\mathbb{N}\times\mathbb{N}} = (1, 1)$. L' applicazione $\varphi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita da $\varphi(a) = (a, 0)$ è un omomorfismo di semigruppi ma non di monoidi, infatti $\varphi(1_{\mathbb{N}}) = (1, 0) \neq 1_{\mathbb{N}\times\mathbb{N}}$.

Definizioni: Un *isomorfismo* (di semigruppi o di monoidi) è un omomorfismo che è anche una biiezione.
Un *endomorfismo* di S è un omomorfismo da S in S.
Un *automorfismo* è un isomorfismo da S in S.
Due semigruppi S, S' si dicono *isomorfi* se esiste un isomorfismo tra loro, e si indica con $S \cong S'$.

Esempi:
1) sia $\pi : \mathbb{Z} \to \{1, -1\}$ l' applicazione definita da $\pi(z) = (-1)^z, \quad \forall z \in \mathbb{Z}$. Allora π è un omomorfismo di monoidi di $(\mathbb{Z}, +)$ in $(\{1, -1\}, \cdot)$. (verificarlo)
2) sia $\mu : \mathbb{C} \to \mathbb{R}$ l' applicazione definita da $\mu(z) = |z|, \quad \forall z \in \mathbb{C}$. Allora μ è un omomorfismo di monoidi di $(\mathbb{C}, \cdot)$ in $(\mathbb{R}, \cdot)$. (verificarlo)

Esercizio: si consideri l' applicazione $\varphi : \mathbb{C} \to M_2(\mathbb{R})$, dove $M_2(\mathbb{R})$ è il monoide delle matrici 2×2 con elementi $\in \mathbb{R}$, definita da

$$\varphi(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a, b \in \mathbb{R} \tag{7.8}$$

Dimostrare: 1) che φ è iniettiva, 2) che φ è un omomorfismo tra i monoidi $(\mathbb{C}, +)$ e $(M_2(\mathbb{R}), +)$, e tra i monoidi $(\mathbb{C}^*, \cdot)$ e $(M_2(\mathbb{R}), \cdot)$.

7.5 Quozienti

Sia $(S, \cdot)$ un semigruppo e $\sim$ una relazione di equivalenza sull' insieme S. Si dice che l' operazione $\cdot$ e l' equivalenza $\sim$ sono *compatibili* se

$$a \sim b,\ c \sim d \quad \Rightarrow\ a \cdot c \sim b \cdot d, \quad \forall a, b, c, d \in S \tag{7.9}$$

Esempio: la congruenza modulare $\equiv_n$ è compatibile sia con l' addizione che con la moltiplicazione in $\mathbb{Z}$.

• Sia $(S, \cdot)$ un semigruppo e $\sim$ una relazione di equivalenza su S compatibile con l' operazione $\cdot$. E' allora possibile definire sull' insieme quoziente $S/\equiv$ un' operazione $\circ$ tra classi di equivalenza come segue

$$[a] \circ [b] = [a \cdot b], \quad \forall [a], [b] \in S/\sim \tag{7.10}$$

Ci si può chiedere se questa è una buona definizione, nel senso che individua univocamente il prodotto di due classi di equivalenza. Consideriamo la classe $[a]$, con $a \in S$. Questa per definizione è uguale alla classe $[b]$ se $a \sim b$. Analogamente $[c] = [d]$ se $c \sim d$. Allora una operazione su $G/\sim$ deve essere tale che $[a] \circ [b] = [c] \circ [d]$, cioè $[a \cdot b] = [c \cdot d]$, e questo è vero grazie alla compatibilità (7.9). Inoltre l' operazione $\circ$ è associativa: infatti

$$([a] \circ [b]) \circ [c] = [a \cdot b] \circ [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \circ [b \cdot c] = [a] \circ ([b] \circ [c]) \tag{7.11}$$

per ogni $[a], [b], [c] \in S/\sim$. Di conseguenza $(S/\sim, \circ)$ è un semigruppo. Se inoltre $(S, \cdot)$ è un monoide con identità 1_S, allora anche $(S/\sim, \circ)$ è un monoide con identità $1_{S/\sim} = [1_S]$ (dimostrazione immediata).

Esercizio: applicare la discussione di sopra ai monoidi $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \cdot)$, con relazione di equivalenza data dalla congruenza modulare $\equiv_n$.

7.6 Il monoide delle parole

Se A è un insieme, una *parola* di lunghezza n nell' *alfabeto* A è una qualunque sequenza $a_1 a_2 \cdots a_n$ di n elementi di A. L' insieme delle parole di lunghezza n si denota con W_n. Per convenzione si definisce la *parola vuota* w_0 come la sequenza di

zero elementi di A, e allora $W_0 = \{w_0\}$. L' insieme di tutte le parole nell' alfabeto A è denotato W_A:

$$W_A = \bigcup_{n\in\mathbb{N}} W_n \tag{7.12}$$

Nell' insieme W_A si può definire una operazione $\circ$, tramite concatenazione delle parole. Se $w = a_1 \cdots a_n$ e $w' = b_1 \cdots b_m$ si definisce

$$w \circ w' = a_1 \cdots a_n b_1 \cdots b_m \tag{7.13}$$

Con questa operazione, $(W_A, \circ)$ diventa un monoide con identità w_0, detto *monoide delle parole* nell' alfabeto A.

• Consideriamo l' applicazione $\lambda : W_A \to \mathbb{N}$ che associa a ogni parola di lunghezza n il numero n. Si verifica immediatamente che λ è un omomorfismo del monoide $(W_A, \circ)$ nel monoide $(\mathbb{N}, +)$.

7.7 Gruppi

In un monoide $(M, \cdot)$ con identità 1_M si dice che $a \in M$ è *invertibile a sinistra* se esiste un elemento $b \in M$, chiamato *inverso sinistro* di a, tale che $b \cdot a = 1_M$, e si dice che a è *invertibile a destra* se esiste un elemento $c \in M$, chiamato *inverso destro* di a, tale che $a \cdot c = 1_M$. L' elemento a si dice *invertibile* se è invertibile sia a sinistra che a destra. In tal caso inverso sinistro b e inverso destro c di a coincidono: infatti $b = b \cdot 1_M = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1_M \cdot c = c$.

• Un *gruppo* è un monoide in cui ogni elemento a è invertibile. L' inverso di a viene denotato con a^{-1}, e quindi si ha $a \cdot a^{-1} = a^{-1} \cdot a = 1_M,\ \forall a \in M$.

Osservazione: in un gruppo l' inverso è unico: se $a \cdot b = a \cdot c = 1_M$, moltiplicando a sinistra per un inverso di a si trova $b = c$.

Osservazione: valgono le seguenti relazioni (di immediata dimostrazione):

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}, \quad (a^{-1})^{-1} = a \tag{7.14}$$

• Un gruppo $(G, \cdot)$ in cui $a \cdot b = b \cdot a$ per ogni $a, b \in G$ si dice *commutativo* o *abeliano*.

Riassumiamo le proprietà che caratterizzano un gruppo nella seguente

Definizione: un *gruppo* $(G, \cdot)$ è un insieme G dotato di un' operazione $\cdot$ che soddisfa alle proprietà

1) associatività
2) esistenza dell' identità 1_G
3) esistenza dell' inverso di ogni elemento di G

Esempi: i monoidi $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ sono gruppi abeliani. I monoidi $(\mathbb{N},+),(\mathbb{N},\cdot),(\mathbb{Z},\cdot),(\mathbb{Q},\cdot),(\mathbb{R},\cdot),(\mathbb{C},\cdot)$ non sono gruppi. I monoidi $(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot),(\mathbb{C}^*,\cdot)$ sono gruppi abeliani.

• In un gruppo G si possono definire le potenze n-esime di un elemento $g \in G$, con $n \in \mathbb{Z}$. Le potenze negative vengono definite da $g^{-n} = \underbrace{g^{-1}\cdots g^{-1}}_{n} = (g^{-1})^n$.

Valgono allora le relazioni (7.3) con $n, m \in \mathbb{Z}$.

• Se H è un sottoinsieme di un gruppo G , tale che
1) H è chiuso rispetto all' operazione di $(G,\cdot)$, cioè $a \cdot b \in H, \quad \forall, b \in H$.
2) l' identità 1_G di G è contenuta in H.
3) per ogni $a \in H$ esiste l' inverso $a^{-1} \in H$

allora H è esso stesso un gruppo. In questo caso H si dice *sottogruppo* di G, e si scrive $H \leq G$. Per ogni gruppo G, G stesso e $\{1_G\}$ sono sottogruppi banali di G detti sottogruppi *impropri*. Gli altri sottogruppi si dicono *propri*.

Esempi:
1) L' insieme C_n delle radici n-esime di 1 è un gruppo (con operazione data dalla moltiplicazione tra numeri complessi): $C_n = \{z \mid z \in \mathbb{C},\ z^n = 1\}$.
2) $(\mathbb{C}^*,\cdot)$ è un gruppo. Il sottoinsieme $\Pi = \{z \mid z \in \mathbb{C}, |z| = 1\}$ è un suo sottogruppo.

Teorema: un insieme non vuoto H è un sottogruppo di G se e solo se $\forall a, b \in H$, si ha $ab^{-1} \in H$

Dimostrazione: se H è un sottogruppo di G, e $a, b \in H$, allora $b^{-1} \in H$ e di conseguenza $ab^{-1} \in H$.
Viceversa, se per ogni a, b contenuti nel sottoinsieme H si ha $ab^{-1} \in H$, in particolare si ha $aa^{-1} = 1_G \in H$. Allora si ha anche che $1_G a^{-1} \in H$ e quindi $a^{-1} \in H$. Finalmente H è chiuso poichè $ab = a(b^{-1})^{-1} \in H$. Sono quindi soddisfatte le tre condizioni di sopra perchè H sia un sottogruppo di G.□

• Omomorfismi e isomorfismi φ tra gruppi G, G' sono definiti come per i monoidi, e quindi devono valere le relazioni (7.6), (7.7), con la richiesta aggiuntiva:

$$\varphi(g^{-1}) = (\varphi(g))^{-1} \quad \forall g \in G \tag{7.15}$$

Questa relazione discende dalle prime due solo se φ è suriettiva, altrimenti viene imposta come parte della definizione di omomorfismo tra gruppi.

• La cardinalità di un gruppo G si dice *ordine* di G.

• La **tavola di moltiplicazione** di un gruppo G, cioè una tabella che contiene tutti i possibili prodotti di due elementi di G, caratterizza completamente G. Due gruppi isomorfi hanno la stessa tavola di moltiplicazione, e quindi sono lo stesso gruppo, anche se possono avere definizioni diverse, come ad esempio C_n e il gruppo delle rotazioni che lasciano invariato un poligono regolare di n lati.

• Il *prodotto diretto* di due gruppi $(G,\cdot),(G',\circ)$, indicato con $G\times G'$ viene definito come l' insieme delle coppie (g,g') con $g\in G$ e $g'\in G'$, dove è data una operazione (associativa) $\star$:

$$(a,b)\star(c,d)=(a\cdot c, b\circ d) \tag{7.16}$$

Questa definizione assicura l' esistenza dell' identità $(1_G,1_{G'})$ e dell' inverso $(a,b)^{-1}=(a^{-1},b^{-1})$ nell' insieme $G\times G'$, e quindi $(G\times G',\star)$ è un gruppo.

Spesso si indicano le operazioni sui vari gruppi $G,G',G\times G'$ con lo stesso simbolo (o senza simbolo).

7.8 Permutazioni

Le permutazioni di n oggetti formano un gruppo, chiamato *gruppo simmetrico* S_n, con operazione data dalla composizione di permutazioni, e con unità data dalla permutazione identica, cioè la permutazione che lascia tutti gli oggetti al loro posto. Ogni permutazione ha il suo inverso, che riordina gli elementi nella loro posizione iniziale.

Gli elementi f di S_n sono permutazioni individuate dalla tabella:

$$f=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n)\end{pmatrix} \tag{7.17}$$

che indica in modo esplicito come vengono riordinati gli elementi $1,2,...n$. Un altro modo di descrivere una permutazione fa uso di un grafo orientato. Per esempio la permutazione

$$f=\begin{pmatrix} 1&2&3&4&5&6&7&8&9\\ 6&4&3&7&1&5&8&2&9\end{pmatrix} \tag{7.18}$$

può rappresentarsi col grafo orientato

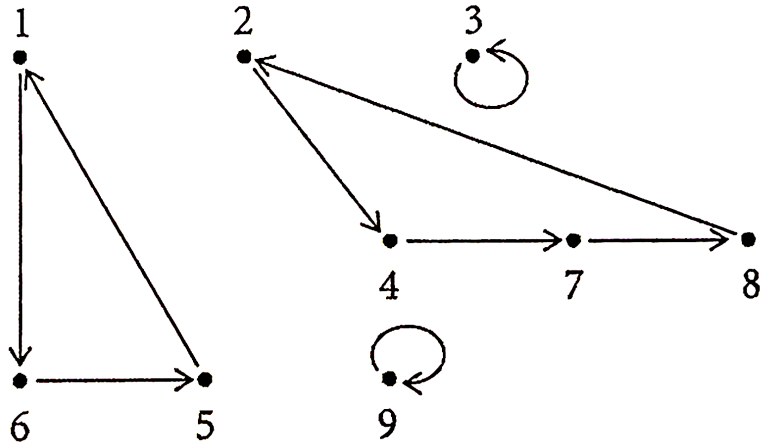


Fig. 7.1 Grafo di permutazione

di immediata interpretazione. Come risulta anche visivamente, ogni permutazione può decomporsi in un prodotto di *cicli*. Nel caso di sopra si ha:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 3 & 7 & 1 & 5 & 8 & 2 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 5 \end{pmatrix} \begin{pmatrix} 2 & 4 & 7 & 8 \end{pmatrix} (3)\,(9) \qquad (7.19)$$

dove per ciclo si intende una permutazione ciclica, per esempio (1 6 5) indica la permutazione $1 \to 6 \to 5 \to 1$. Cicli *disgiunti*, cioè che non abbiano nessun elemento in comune, corrispondono a permutazioni su elementi diversi, e quindi non importa l' ordine con cui vengono eseguiti. In altre parole cicli disgiunti commutano tra loro. La lunghezza di un ciclo è data dal numero di oggetti coinvolti. Cicli di lunghezza 1 sono semplicemente l' identiità, e quindi i cicli (3) e (9) dell' esempio di sopra possono essere omessi nella decomposizione della permutazione in cicli. La regola per trovare la decomposizione in prodotto di cicli disgiunti di qualunque permutazione è molto semplice, e desumibile immediatamente dall' esempio e dalla sua rappresentazione grafica.

Esercizio: verificare con un esempio che per due cicli f e g non disgiunti si ha $f \circ g \neq g \circ f$.

Esercizio: dimostrare che

$$(a_1\ a_2\ \cdots\ a_d)^{-1} = (a_d\ a_{d-1}\ \cdots\ a_1) \qquad (7.20)$$

Definizione: i cicli di lunghezza 2 si dicono *trasposizioni*, e consistono nello scambio di due elementi.

Teorema: ogni permutazione può essere scritta come prodotto di trasposizioni.

Dimostrazione: segue dalla discussione precedente e dal fatto che ogni ciclo può scriversi come prodotto di trasposizioni come segue:

$$(a_1\ a_2\ \cdots\ a_d) = (a_1\ a_d)\ (a_1\ a_{d-1})\ (a_1\ a_{d-2})\ \cdots\ (a_1\ a_3)(a_1\ a_2) \qquad (7.21)$$

Esercizio: verificarlo.

Nota: la stessa permutazione può avere più decomposizioni in prodotto di trasposizioni. Per esempio:

$$(1\ 3)\ (2\ 4) = (1\ 4)\ (1\ 2)\ (3\ 4)\ (1\ 4) = (2\ 4)\ (1\ 4)\ (3\ 4)\ (1\ 4) \qquad (7.22)$$

Teorema: le rappresentazioni di una data permutazione come prodotto di trasposizioni hanno tutte un numero pari o tutte un numero dispari di fattori.

Dimostrazione: una disposizione di n oggetti $a_1, ...a_n$ è caratterizata da un ordinamento, dove $a_i < a_j$ significa che a_i sta a sinistra di a_j. Quindi alla particolare

disposizione $a_1, ...a_n$ si può far corrispondere una lista di comparazioni di coppie:

$$\begin{aligned} a_1 < a_2,\ a_1 < a_3, ..., a_1 < a_n \\ a_2 < a_3,\ a_2 < a_4, ..., a_2 < a_n \\ ..... \\ a_{n-1} < a_n \end{aligned} \tag{7.23}$$

Come si modifica questa lista se scambiamo due elementi a_i, a_j con $a_i < a_j$? Risposta:

1) $a_i < a_j$ diventa $a_j < a_i$,
2) se a_k sta a sinistra di a_i e a_j, le comparazioni $a_k < a_i$, $a_k < a_j$ non cambiano,
3) se a_k sta a destra di a_i e a_j, le comparazioni $a_k > a_i$, $a_k > a_j$ non cambiano.
4) se a_k è compreso tra a_i e a_j, le comparazioni $a_i < a_k$, $a_k < a_j$ diventano $a_j < a_k$, $a_k < a_i$
5) tutte le altre comparazioni non cambiano

L' effetto di una trasposizione è quindi quello di cambiare un numero *dispari* di comparazioni di coppie. Una qualsiasi permutazione è caratterizzata da un certo numero N di comparazioni di coppie cambiate. Se questo numero N è pari, deve essere pari anche il numero di fattori nella rappresentazione della permutazione come prodotto di trasposizioni (dato che ad ogni trasposizione corrisponde un numero dispari di cambi di comparazioni). Viceversa se N è dispari, deve essere dispari il numero di fattori. Ne consegue che ogni permutazione è il prodotto di un numero pari o di un numero dispari di trasposizioni. Si hanno allora *permutazioni pari* e *permutazioni dispari*. □

• La *segnatura* di una permutazione f è +1 se f è pari, ed è -1 se f è dispari. Si indica con $\mathrm{sgn}(f)$.

Osservazione: un ciclo di lunghezza d è equivalente a un prodotto di $d-1$ trasposizioni, vedi la formula (7.21), e pertanto ha segnatura $(-1)^{d-1}$. Una volta decomposta una permutazione in cicli, è allora immediato trovare la sua segnatura. La composizione di due permutazioni pari, o di due permutazioni dispari, è una permutazione pari, mentre la composizione di una permutazione pari con una permutazione dispari è una permutazione dispari.

Esempio: la permutazione in Fig. 7.1 è dispari.

Esercizio: dimostrare che le permutazioni pari di S_n formano un sottogruppo di S_n. Questo sottogruppo è chiamato *gruppo alterno* A_n. Dimostrare che le permutazioni dispari non formano un sottogruppo.

Il seguente importante teorema fa capire l' importanza del gruppo delle permutazioni nell' ambito della teoria dei gruppi finiti:

Teorema di Cayley: ogni gruppo finito di ordine n è isomorfo a un sottogruppo di S_n

Dimostrazione: a ogni elemento g del gruppo G di ordine n si fa corrispondere un elemento ϕ_g di S_n tramite l' applicazione $\omega : G \to S_n$ definita da

$$\omega(g) = \phi_g, \quad \phi_g(i) = j \Leftrightarrow gg_i = g_j, \quad i, j = 1, ...n \tag{7.24}$$

dove abbiamo numerato gli n elementi di G come $g_1, g_2, ...g_n$. Quindi ϕ_g agisce sull' insieme $\{1, 2, ...n\}$ trasformandolo in $\{\phi_g(1), \phi_g(2), ...\phi_g(n)\}$. Notiamo che ϕ_g è un' applicazione biiettiva dall' insieme $\{1, 2, ...n\}$ in se stesso, e quindi una permutazione su n elementi. Infatti ϕ_g
- è iniettiva: se $i \neq k$ (e allora $g_i \neq g_k$) segue $\phi_g(i) \neq \phi_g(k)$ dato che $gg_i = gg_k$ implicherebbe $g_i = g_k$.
- è suriettiva: per ogni g_j esiste un g_i tale che $gg_i = g_j$.
L' applicazione ω è un isomorfismo: infatti è una biiezione tra gli insiemi $\{g_1, ...g_n\}$ e $\{\phi_{g_1}, ...\phi_{g_n}\}$ e inoltre $\omega(gg') = \phi_{gg'} = \phi_g \circ \phi_{g'} = \omega(g) \circ \omega(g')$ come si deduce comparando $(gg')g_i = g_{\phi_{gg'}(i)}$ con $g(g'g_i) = gg_{\phi_{g'}(i)} = g_{\phi_g \circ \ \phi_{g'}(i)}$. Si è così dimostrato che G è isomorfo al sottogruppo $\{\phi_{g_1}, ...\phi_{g_n}\}$ di S_n, dove $\phi_g \circ \phi_{g'} = \phi_{gg'}$, l' identità è ϕ_{1_G} e l' inverso di ϕ_g è $\phi_{g^{-1}}$. □

• E' stata completata intorno al 2005 la classificazione di tutti i gruppi finiti. Nella tabella che segue diamo la lista dei gruppi finiti fino all' ordine 8:

Ordine	Gruppi
1	I
2	C_2
3	C_3
4	$C_2 \times C_2,\ C_4$
5	C_5
6	$C_6 = C_2 \times C_3, S_3$ (*non abeliano*)
7	C_7
8	$C_8,\ C_4 \times C_2,\ C_2 \times C_2 \times C_2,\ D_4,\ Q$ (*quaternioni*)

7.9 Il gruppo S_3

Il gruppo S_3 delle permutazioni di 3 oggetti contiene i sei elementi:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

La loro tavola di moltiplicazione è data in Fig. 7.2, e contiene tutti i possibili prodotti tra due elementi del gruppo. Per esempio per trovare $\rho_2 \cdot \tau_1$ si entra nella tavola da sinistra con la riga corrispondente a ρ_2 fino alla colonna corrispondente a τ_1, e si trova $\rho_2 \cdot \tau_1 = \tau_2$

$\circ$	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	id	τ_3	τ_1	τ_2
ρ_2	ρ_2	id	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	id	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	id

Fig. 7.2 Tavola di moltiplicazione del gruppo S_3

I sottogruppi di S_3 sono:

$$H = \{id, \rho_1, \rho_2\},\ H_1 = \{id, \tau_1\},\ H_2 = \{id, \tau_2\},\ H_3 = \{id, \tau_3\} \tag{7.25}$$

oltre ai sottogruppi impropri S_3 e $\{id\}$.

7.10 Classi laterali e sottogruppi normali

• Siano $(G, \cdot)$ un gruppo e $g \in G$. Se H è un sottogruppo di G, l' insieme $gH \subseteq G$ definito da[4]

$$gH = \{gh \mid h \in H\} \tag{7.26}$$

si dice *classe laterale sinistra* di G, con modulo H e *rappresentante* g. Definizione analoga vale per le classe laterali destre di G, denotate Hg. Quando $gH = Hg$ per ogni $g \in G$, cioè quando le classi laterali sinistre coincidono con le classi laterali destre per ogni rappresentante $g \in G$, il sottogruppo H si dice *sottogruppo normale* di G, e si indica con $H \trianglelefteq G$.

Esempio: si consideri il sottogruppo $H = \{id, \rho_1, \rho_2\}$ di S_3. La classe laterale sinistra con rappresentante $g \in H$ è evidentemente H stesso, mentre la classe laterale sinistra con rappresentante $g \notin H$ è data da $\{\tau_1, \tau_2, \tau_3\}$. Si hanno quindi solo due classi laterali sinistre distinte:

$$\begin{aligned} &id\ H = \rho_1 H = \rho_2 H = \{id, \rho_1, \rho_2\} = H \\ &\tau_1 H = \tau_2 H = \tau_3 H = \{\tau_1, \tau_2, \tau_3\} \end{aligned} \tag{7.27}$$

Per le classi laterali destre si ha

$$\begin{aligned} &H\ id = H\rho_1 = H\rho_2 = \{id, \rho_1, \rho_2\} = H \\ &H\tau_1 = H\tau_2 = H\tau_3 = \{\tau_1, \tau_2, \tau_3\} \end{aligned} \tag{7.28}$$

In questo caso si ha $gH = Hg$ per ogni $g \in G$, cioè classi laterali sinistre e destre coincidono per ogni rappresentante $g \in G$. Abbiamo così verificato che $H = \{id, \rho_1, \rho_2\}$ è un sottogruppo normale di S_3.

[4] si usa la notazione semplificata $a \cdot b = ab$ per l' operazione del gruppo.

Ci sono altri tre sottogruppi propri di S_3, e sono H_1, H_2, H_3 dati in (7.25). Consideriamo le classi laterali di $H_1 = \{id, \tau_1\}$. Si hanno le classi laterali sinistre

$$id\ H_1 = \{id, \tau_1\} = H_1,\ \rho_1 H_1 = \{\rho_1, \tau_3\},\ \rho_2 H_1 = \{\rho_2, \tau_2\} \tag{7.29}$$

$$\tau_1 H_1 = \{id, \tau_1\} = H_1,\ \tau_2 H_1 = \{\rho_2, \tau_2\},\ \tau_3 H_1 = \{\rho_1, \tau_3\} \tag{7.30}$$

e le classi laterali destre

$$H_1\ id = \{id, \tau_1\} = H_1,\ H_1\rho_1 = \{\rho_1, \tau_2\},\ H_1\rho_2 = \{\rho_2, \tau_3\} \tag{7.31}$$

$$H_1\tau_1 = \{id, \tau_1\} = H_1,\ H_1\tau_2 = \{\rho_1, \tau_2\},\ H_1\tau_3 = \{\rho_2, \tau_3\} \tag{7.32}$$

In questo caso $gH = Hg$ non vale per ogni $g \in G$, per esempio $\rho_1 H_1 \neq H_1\rho_1$, e pertanto il sottogruppo H_1 non è un sottogruppo normale di G. Per le classi laterali modulo H_2 e H_3 si ha una situazione analoga. L' unico sottogruppo normale di S_3 è quindi $H = \{id, \rho_1, \rho_2\}$.

Teorema: Se G è un gruppo e H un suo sottogruppo, gli insiemi H e gH sono equipotenti.

Dimostrazione: Basta dimostrare che l' applicazione $\varphi : H \to gH$ definita da $\varphi(h) = gh,\ \forall h \in H$ è una biiezione. E' suriettiva perchè ogni elemento y di gH è del tipo $y = gh$ per un opportuno $h \in H$, e quindi $\varphi(h) = y$. E' iniettiva perchè se $h_1, h_2 \in H$ e $\varphi(h_1) = \varphi(h_2)$ allora $gh_1 = gh_2$ e moltiplicando per g^{-1} si trova $h_1 = h_2$. $\square$

Osservazione 1: nel caso particolare $G = H$, l' applicazione φ definita sopra diventa una biiezione dell' insieme H in se stesso, e cioè una permutazione degli elementi di H. Ne consegue che $hH = H$ per ogni $h \in H$.

Osservazione 2: due rappresentanti g_1, g_2 individuano la stessa classe laterale, cioè $g_1 H = g_2 H$, se e solo se $g_2 = g_1 h$ per un certo h, o equivalentemente se e solo se $(g_1)^{-1} g_2 \in H$. Infatti se $g_1 H = g_2 H$, allora si ha $g_1 h = g_2 h'$ per opportuni $h, h' \in H$, da cui moltiplicando a destra per $(h')^{-1}$ si ricava l' asserto. Viceversa se vale $g_2 = g_1 h$, si ha $g_2 H = g_1 h H = g_1 H$, poichè $hH = H$ (vedi Osservazione 1).

Osservazione 3: l' insieme di tutte le classi laterali sinistre di G modulo H è una partizione di G. Infatti i sottoinsiemi gH di G sono tutti non vuoti ($g = g1_G = g1_H \in gH$), la loro unione coincide con G (l' unione comprende $g1_H = g1_G$ per tutti i $g \in G$, quindi comprende tutto G) e due classi laterali diverse formano insiemi disgiunti. Infatti se $g_1 H \neq g_2 H$, allora $g_1 H \cap g_2 H = \varnothing$, poichè se esistesse un $x \in g_1 H \cap g_2 H$, dovrebbe essere $x = g_1 h = g_2 h'$ per opportuni h, h', da cui seguirebbe $g_2 = g_1 h (h')^{-1} \to g_1 H = g_2 H$, vedi Osservazione 2.

Esercizio: verificare il teorema e le osservazioni di sopra nell' esempio $G = S_3$.

• Le considerazioni di questo paragrafo valgono anche per i gruppi infiniti. Per esempio se $G = \mathbb{R}^*$ e $H = \mathbb{R}^+$, con legge di composizione data dalla moltiplicazione,

allora $g\mathbb{R}^+ = \mathbb{R}^+$ se $g > 0$, e a $g\mathbb{R}^+ = \mathbb{R}^-$ se $g < 0$. L' insieme $\{\mathbb{R}^+, \mathbb{R}^-\}$ di queste due classi laterali forma una partizione di $\mathbb{R}^*$, in accordo con l' Osservazione 3.

• Il numero di classi laterali sinistre di G modulo H si chiama *indice* di H in G, e si indica con $[G : H]$. Esempi: $[\mathbb{R}^* : \mathbb{R}^+] = 2$, $[S_3 : H_1] = 3$.

Teorema di Lagrange: l' ordine di ogni sottogruppo H di un gruppo finito G è un divisore dell' ordine di G.

Dimostrazione:
G è ripartito in $[G : H]$ classi laterali gH, tutte con lo stesso numero di elementi ($|gH| = |H|$ poichè H e gH sono equipotenti), e quindi $|G| = [G : H]|H|$. □

Corollario: se l' ordine di G è primo, G non ha sottogruppi propri.

Teorema: H è un sottogruppo normale di G se e solo se $ghg^{-1} \in H$, per ogni $g \in G$ e per ogni $h \in H$.

Dimostrazione: da $gH = Hg$ si ricava che per ogni $g \in G$ e ogni $h \in H$ si deve avere $gh = h'g$ per un opportuno h', il che implica $ghg^{-1} \in H$. Viceversa, se $ghg^{-1} \in H$ per ogni $g \in G$ e ogni $h \in H$, si ha $gh = h'g$ per un opportuno $h' \in H$. Pertanto tutti gli elementi della classe gH sono scrivibili nella forma $h'g$ e quindi appartengono alla classe destra Hg. Analogamente si dimostra che tutti gli elementi della classe Hg appartengono alla classe gH, e si conclude che $gH = Hg$.

Osservazione 4: I sottogruppi impropri G e $\{1_G\}$ di un gruppo G sono normali, come risulta immediatamente dal Teorema di sopra.

• Si chiama *ordine* di $g \in G$ il più piccolo intero r tale che $g^r = 1_G$. Per esempio se $G = S_3$ si trova che l' ordine di ρ_1 e di ρ_2 è 3, mentre l' ordine di τ_1, τ_2, τ_3 è 2. L' insieme $\{1_G, g, g^2, ...g^{r-1}\}$ è un sottogruppo di G, isomorfo al gruppo C_r, come si verifica dalla sua tavola di moltiplicazione.

Teorema: se $|G| = p$ con p numero primo, allora $G = C_p$.

Dimostrazione: l' ordine r di qualunque elemento $g \in G$ non può essere minore di p. Se lo fosse, G dovrebbe contenere un sottogruppo C_r, e quindi r dovrebbe dividere p (teorema di Lagrange), impossibile poichè p è primo. Quindi si deve avere $r = p$, e allora $G = C_p$. □

7.11 Relazioni di equivalenza nei gruppi

Teorema: se $\sim$ è una relazione di equivalenza su G, compatibile con l' operazione del gruppo, allora la classe di equivalenza $[1_G]_\sim$ (= l' insieme di tutti gli elementi di G equivalenti all' identità) è un sottogruppo normale di G. Viceversa se N è un sottogruppo normale di G e $\sim_N$ è la relazione su G definita da $a \sim_N b$ se

$aN = bN$ (cioè se a e b stanno nella stessa classe laterale di G modulo N), allora $\sim_N$ è una relazione di equivalenza su G compatibile con l' operazione del gruppo, e $[1_G]_{\sim_N} = N$.

Dimostrazione:
1) sia $\sim$ una relazione di equivalenza su G, compatibile con l' operazione del gruppo. Allora in particolare se $a \sim 1_G$ e $b \sim 1_G$, si ha $ab \sim 1_G$, il che equivale a dire che se $a, b \in [1_G]_\sim$, anche $ab \in [1_G]_\sim$, e quindi $[1_G]_\sim$ è un sottogruppo di G. Inoltre se $a \in [1_G]_\sim$ e $g \in G$, si ha $gag^{-1} \sim g\ 1_G\ g^{-1} = 1_G$, quindi $gag^{-1} \in [1_G]_\sim$ e si conclude che $[1_G]_\sim$ è un sottogruppo normale di G.
2) Sia N un sottogruppo normale di G, e $\sim_N$ la relazione definita da $a \sim_N b$ se $aN = bN$. Allora $\sim_N$ è evidentemente riflessiva, simmetrica e transitiva, e quindi è una relazione di equivalenza. Inoltre se $aN = bN$ ($\Rightarrow a^{-1}b \in N$) e $cN = dN$ ($\Rightarrow c^{-1}d \in N$), si ha $c^{-1}(a^{-1}b)c \in N$ poichè N è normale, e quindi $(ac)^{-1}(bd) = c^{-1}a^{-1}bd = (c^{-1}a^{-1}bc)(c^{-1}d) \in N$. Si è così dimostrato che se $a \sim_N b$ e $c \sim_N d$, allora $ac \sim_N bd$, cioè che l' equivalenza $\sim_N$ è compatibile con l' operazione del gruppo. Finalmente $[1_G]_{\sim_N} = N$ poichè $[1_G]_{\sim_N} = \{a \in G \mid 1_G \sim_N a\} = \{a \in G \mid (1_G)^{-1}a \in N\} = N$.

Nota: dal Teorema precedente segue che in un gruppo G le relazioni di equivalenza compatibili con l' operazione del gruppo sono in corrispondenza biunivoca con i sottogruppi normali di G: data l' equivalenza $\sim$ si trova il sottogruppo normale $[1_G]_\sim$, e dato un sottogruppo normale N si trova l' equivalenza $\sim_N$ come appartenenza alla stessa classe laterale modulo N. Il quoziente $G/\sim_N$ è quindi dato dall' insieme delle classi laterali $\{gN \mid g \in G\}$, e viene denotato con G/N.

• Dalla Sezione 7.5 segue che $G/N = \{gN \mid g \in G\}$ è il monoide con operazione $(g_1N)(g_2N) = (g_1g_2)N$ e con identità $1_{G/N} = 1_GN = N$.

Teorema: Se G è un gruppo e N un suo sottogruppo normale, allora G/N è un gruppo.

Dimostrazione: dal teorema precedente sappiamo che G/N è un monoide con operazione $(g_1N)(g_2N) = (g_1g_2)N$ e con identità $1_{G/N} = 1_GN = N$. Basta allora dimostrare che in G/N ogni elemento è invertibile. Questo è vero: infatti per ogni $gN \in G/N$, esiste l' inverso $g^{-1}N$ (che appartiene sempre a G/N) poichè $(g^{-1}N)(gN) = N = 1_{G/N}$ e $(gN)(g^{-1}N) = N = 1_{G/N}$. □

• Riassumendo: G/N è il "gruppo quoziente di G modulo N", i cui elementi sono le classi laterali $gN = Ng$ (le classi laterali sinistre coincidono con le classi laterali destre, dato che N è normale) . L' operazione in G/N è definita da

$$(gN)(g'N) = (gg')N, \quad \forall gN, g'N \in G/N \tag{7.33}$$

e l' identità in G/N è data da

$$1_{G/N} = 1_GN = N \tag{7.34}$$

L' inverso di $gN \in G/N$ è

$$(gN)^{-1} = g^{-1}N \tag{7.35}$$

• Un' altra relazione di equivalenza (*coniugazione*) in un gruppo G è data da

$$a \sim b \;\Leftrightarrow\; \exists g \in G \mid a = gbg^{-1} \tag{7.36}$$

In questo caso le classi di equivalenza si chiamano *classi di coniugazione*. La classe di coniugazione che contiene 1_G contiene solo l' identità, come è immediato verificare.

Esercizio: dimostrare che questa equivalenza è compatibile con l' operazione di gruppo.

Osservazione: se $|G| = p$ con p numero primo, per il teorema di Lagrange i sottogruppi di G possono solo avere cardinalità uguale a 1 o a p. Esiste un solo sottogruppo di cardinalità 1, costituito dall' identità 1_G, e un solo sottogruppo di cardinalità p, che coincide con G ($= C_p$, vedi Sez. precedente). Entrambi questi sottogruppi impropri sono normali, come già osservato. La relazione di equivalenza corrispondente al sottogruppo normale $N = \{1_G\}$ è la relazione di uguaglianza. Infatti $a \sim_{\{1_G\}} b$ se $a1_G = b1_G \Rightarrow a = b$. L' equivalenza corrispondente a $N = G$ è invece l' equivalenza banale (tutti gli elementi di G equivalenti tra loro).

7.12 Nucleo di un omomorfismo

• Sia $f : G \to G'$ un omomorfismo tra gruppi (vedi Sez 7.7). Il **nucleo** di f è l' insieme $f^{-1}(1_{G'}) = \{g \in G \mid f(g) = 1_{G'}\}$, cioè è l' insieme degli elementi di G che vengono trasformati da f nell' identità di G'. Questo insieme viene denotato[5] con $\mathrm{Ker}f$. Dimostriamo due teoremi:

Teorema 1: il nucleo $\mathrm{Ker}f$ di un omomorfismo tra gruppi $f : G \to G'$ è un sottogruppo normale di G.

Dimostrazione: i) $f(1_G) = 1_{G'}$ poichè f è un omomorfismo tra gruppi. Allora $\mathrm{Ker}f \neq \varnothing$. ii) se $a, b \in \mathrm{Ker}f$, si ha $f(ab) = f(a)f(b) = 1_{G'}1_{G'} = 1_{G'}$ e quindi anche $ab \in \mathrm{Ker}f$. iii) se $g \in G$, $a \in \mathrm{Ker}f$, si ha $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)1_{G'}f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(1_G) = 1_{G'}$ e quindi $gag^{-1} \in \mathrm{Ker}f$. □

Teorema 2: sia $f : G \to G'$ un omomorfismo tra gruppi. Allora f è iniettivo se e solo se $\mathrm{Ker}f = \{1_G\}$.

Dimostrazione: se f è iniettivo, $\mathrm{Ker}f = f^{-1}(1)$ può contenere al più un elemento di G. Dato che $f(1_G) = 1_{G'}$, questo elemento deve essere 1_G. Viceversa, se $\mathrm{Ker}f = \{1_G\}$, e $a, b \in G$ tali che $f(a) = f(b)$, allora $f(ab^{-1}) = f(a)f(b)^{-1} = 1_{G'}$ e quindi $ab^{-1} \in \mathrm{Ker}f = \{1_G\}$. Ne segue $ab^{-1} = 1_G$, cioè $a = b$, e quindi f è un omomorfismo iniettivo. □

[5] dal tedesco Kernel (nucleo).

8 Insiemi dotati di più operazioni

8.1 Anelli

• Un *anello* è un insieme R dotato di due operazioni tradizionalmente indicate con $+$ e $\cdot$, e tale che
i) $(R, +)$ è un gruppo abeliano
ii) $(R, \cdot)$ è un semigruppo
iii) per ogni $a, b, c, \in R$ si ha $a(b + c) = ab + ac$, $(b + c)a = ba + ca$

Le operazioni $+, \cdot$ si dicono *addizione* e *moltiplicazione*, e $a+b$ e ab si dicono *somma* e *prodotto* di $a, b \in R$. Per evidenziarne le operazioni, l' anello R può scriversi come $(R, +, \cdot)$. Un anello si dice *commutativo* se $ab = ba$ per ogni $a, b \in R$, cioè se il semigruppo $(R, \cdot)$ è commutativo.

L' identità del gruppo additivo $(R, +)$ viene indicata con 0_R oppure 0, e viene detta lo *zero* dell' anello. Se il semigruppo $(R, \cdot)$ ha un' identità $e_R \neq 0$, allora e_R è detta *identità* dell' anello, e indicata con 1_R o 1.

Esempi: $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ dove $+$ e $\cdot$ sono le usuali operazioni di addizione e moltiplicazione, sono anelli commutativi con identità. L' identità è il numero 1.

Osservazione: Se R è un anello, per ogni $a, b \in R$ si ha

$$0a = a0 = 0 \quad e \quad (-a)b = a(-b) = -(ab) \tag{8.1}$$

dove $-a$ è l' inverso (detto anche opposto) di a nel gruppo additivo $(R, +)$. Infatti:
i) si ha $0a = (0 + 0)a = 0a + 0a$, da cui, sommando $-0a$ a entrambi i membri, si ricava $0a = 0$. Analogamente per $a0 = 0$.
ii) si ha $ab + (-a)b = (a + (-a))b = 0b = 0$ e quindi $(-a)b$ è l' opposto di ab, cioè $(-a)b = -(ab)$. Analogamente $a(-b) = -(ab)$. Si possono allora indicare $(-a)b = a(-b) = -(ab)$ con lo stesso simbolo $-ab$, senza parentesi.

• Se R è un anello, un *sottoanello* di R è un sottoinsieme S di R tale che $(S, +)$ sia un sottogruppo di $(R, +)$ e $(S, \cdot)$ sia un sottosemigruppo di $(R, \cdot)$. In tal caso S, con le operazioni indotte di R , è un anello. Se R è un anello con identità 1_R, si richiede anche che 1_R appartenga a S, cioè che $(S, \cdot)$ sia un sottomonoide di $(R, \cdot)$. In tal caso S è un sottoanello con identità di R.

Esempi:
1) $\mathbb{Z}$ è un sottoanello con identità di $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
2) $\mathbb{Q}$ è un sottoanello con identità di $\mathbb{R}$, $\mathbb{C}$.
3) $\mathbb{R}$ è un sottoanello con identità di $\mathbb{C}$.

• Se R è un anello con identità, gli elementi invertibili del monoide $(R, \cdot)$ si dicono

anche elementi invertibili dell' anello R. E' facile dimostrare che formano un gruppo, denotato $U(R)$.

8.2 Campi

Un *campo* (o *corpo*) è un anello R, commutativo e con identità, in cui ogni elemento tranne 0_R è invertibile.

Esempi: l' anello $\mathbb{Z}$ degli interi non è un campo: infatti i suoi elementi invertibili sono solo 1 e -1. Gli anelli $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono campi.

Osservazione: per ogni a, b appartenenti a un campo R si ha che $ab = 0$ implica $a = 0$ oppure $b = 0$.

Dimostrazione: basta dimostrare che non possono esistere $a \neq 0$ e $b \neq 0$ tali che $ab = 0$. Infatti se esistessero, moltiplicando $ab = 0$ a sinistra per l' inverso di a, si troverebbe $b = 0$, in contraddizione con l' ipotesi.

8.3 L' anello $R[x]$ dei polinomi

Sia $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un polinomio nella variabile x (chiamata anche *indeterminata*), con coefficienti a_i appartenenti a un campo R. Si definiscono allora nel modo solito la somma e il prodotto di due polinomi $f(x)$, $g(x)$ non necesariamente dello stesso grado. Queste due operazioni hanno come identità rispettivamente 0_R e 1_R (se il campo R è costituito dai numeri reali $\mathbb{R}$, le identità sono rispettivamenti i numeri 0 e 1). Nell' anello dei polinomi è possibile definire anche una divisione (*divisione euclidea*) tra un polinomio $f(x)$ di grado m e un polinomio $g(x)$ di grado n, con $m \geq n$. Si trova allora un quoziente $q(x)$ e un resto $r(x)$ tali che

$$f(x) = q(x)g(x) + r(x) \tag{8.2}$$

Il procedimento è simile a quello delle divisioni tra numeri, e riportiamo tre esempi che lo illustrano:

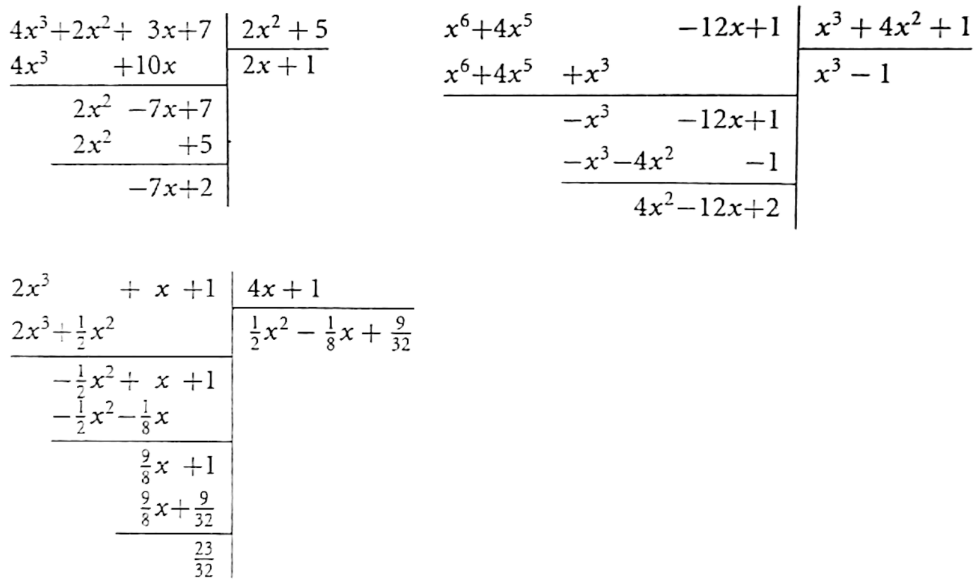


Fig. 8.1 Divisione di polinomi

8.4 L' anello Z_n delle classi resto modulo n

L' insieme delle classi resto (vedi Sezione 4.4) modulo n può scriversi

$$\{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\} \tag{8.3}$$

In questo insieme si definiscono due operazioni, la somma + e il prodotto $\cdot$:

$$[a] + [b] = [a + b] \tag{8.4}$$

$$[a] \cdot [b] = [ab] \tag{8.5}$$

Esempio: se $n = 5$, $[3]_5 + [4]_5 = [7]_5 = [2]_5$, e $[2]_5 \cdot [4]_5 = [8]_5 = [3]_5$.

L' identità per la somma è allora [0] e l' identità per la moltiplicazione è [1]. Infine è immediato verificare che valgono le proprietà distributive $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ e simile per $([b] + [c]) \cdot [a]$. Pertanto l' insieme delle classi resto modulo n è un anello (commutativo) con identità, denotato $\mathbb{Z}_n$.

Osservazione: rispetto all' addizione, l' insieme delle classi resto modulo n forma il gruppo C_n, come si può verificare confrontando la tabella di addizione di Z_n e la tabella di moltiplicazione di C_n.

• Ci si può chiedere se un elemento $[a] \in \mathbb{Z}_n$ è invertibile, cioè se esiste un $[b]$ tale che $[a][b] = [1]$, o equivalentemente $ab \equiv_n 1$. Si ha il seguente teorema:

Teorema: $[a] \in \mathbb{Z}_n$ è invertibile se e solo se a e n sono coprimi.

Dimostrazione: se $[a]$ ha un inverso $[b]$, si ha $ab = 1 + kn$ con $k \in \mathbb{Z}$. Segue che $ab + (-k)n = 1$, e dal Teorema in Sez. 2.2 si ha $\text{MCD}(a, n) = 1$. Viceversa se

$\mathrm{MCD}(a,n) = 1$, allora sempre per il Teorema in Sez. 2.2 esistono interi b e k tali che $ab + kn = 1$, da cui si ricava $ab \equiv_n 1$. $\square$

Esempio: $2 \cdot 3 \equiv_5 1$, quindi 3 è l' inverso (mod 5) di 2, ma non esiste l' inverso (mod 4) di 2.

Teorema: l'equazione modulare $ax \equiv_n b$, con $a, b, n \in \mathbb{Z}, n \geq 1$, ha una soluzione $x \in \mathbb{Z}$ se e solo se $\mathrm{MCD}(a,n)$ divide b.

Dimostrazione: se $ax \equiv_n b$, si ha $ax = b + kn$ con $k \in \mathbb{Z}$, e cioè $b = ax - kn$. Siccome $\mathrm{MCD}(a,n)$ divide a e divide n, divide anche b. Viceversa, se $\mathrm{MCD}(a,n)$ divide b si ha $\mathrm{MCD}(a,n)b' = b$ con $b' \in \mathbb{Z}$. Inoltre per definizione di MCD si deve avere $\mathrm{MCD}(a,n)a' = a$, $\mathrm{MCD}(a,n)n' = n$, con $a', n' \in \mathbb{Z}$ e $\mathrm{MCD}(a',n') = 1$. Esprimendo allora $\mathrm{MCD}(a',n')$ come nel Teorema in Sez. 2.2, si trova $\mathrm{MCD}(a',n') = 1 = a'\alpha + n'\beta$ $(\alpha, \beta \in \mathbb{Z})$ ovvero $a'\alpha = 1 - n'\beta$. Moltiplicando per b si trova $ba'\alpha = (1 - n'\beta)b \Rightarrow ab'\alpha = b - nb'\beta$, e quindi si ha $ax \equiv_n b$ con $x = b'\alpha$. $\square$

8.5 L' anello $M_n[R]$ delle matrici $n \times n$

L' insieme delle matrici $n \times n$ con elementi in un campo R è un anello con identità, dove le operazioni di somma e moltiplicazione matriciale sono le solite, l' identità per la somma è la matrice con elementi tutti uguali a 0_R e l' identità per la moltiplicazione è la matrice diagonale con elementi tutti uguali a 1_R. Vedremo nella parte di algebra lineare la condizione per l' esistenza dell' inverso di una matrice $n \times n$.

9 Algebra lineare

9.1 Spazi vettoriali

Uno **spazio vettoriale** V **su un campo** K è un gruppo abeliano additivo $(V,+)$ dotato di un' ulteriore operazione $K \times V \to V$ definita da $(a,v) \to av$, che soddisfi alle proprietà

1) *associatività:* $(ab)v = a(bv)$ per $\forall a,b \in K$ e $v \in V$
2) *distributività:* $a(v+w) = av + aw$, $(a+b)v = av + bv$, per $\forall a,b \in K$ e $v,w \in V$.
3) *identità*: $1_K v = v$, $\forall v \in V$ e 1_K = identità moltiplicativa di K.

Esercizio: se 0_V e 0_K sono gli zeri di V e K, dimostrare che
a) $a0_V = 0_V,\ \forall a \in K$
b) $0_K v = 0_V,\ \forall v \in V$
c) $(-a)v = a(-v) = -(av),\ \forall a \in K,\ \forall v \in K$
d) $\forall a \in K, v \in V$ si ha $av = 0_V$ se e solo se $a = 0_K$ oppure $v = 0_V$.

Gli elementi di V si chiamano **vettori**. I vettori quindi sono oggetti che si sommano tra loro e si moltiplicano per elementi di un corpo K, ad esempio numeri reali, con le usuali proprietà associative e distributive.

• Se V è uno spazio vettoriale su K, un **sottospazio (vettoriale)** W di V è un sottogruppo di $(V,+)$ tale che $aw \in W$ per ogni $a \in K$ e $w \in W$.

• Una **combinazione lineare** dei vettori $u_1, u_2 ..., u_n \in V$ è un elemento di V del tipo:

$$a_1 u_1 + a_2 u_2 + ... + a_n u_n, \quad a_i \in K, \quad u_i \in V \tag{9.1}$$

e l' insieme X di tutte queste combinazioni lineari è un sottospazio vettoriale di V, come è facile verificare. Si dice che X è **generato** dai vettori $u_1, u_2, ..., u_n$.

9.2 Esempi di spazi vettoriali

9.2.1 Lo spazio delle n-uple di elementi di K

L' insieme delle n-uple $(a_1, a_2, ..., a_n)$ di elementi di un campo K, indicato con K^n, può essere dotato di un' operazione abeliana + definita da

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) \equiv (a_1 + b_1, a_2 + b_2, ..., a_n + b_n), \quad \forall, a_i, b_i \in K \tag{9.2}$$

e di una moltiplicazione per elementi di K (moltiplicazione scalare):

$$c(a_1, a_2, ..., a_n) \equiv (ca_1, ca_2, ..., ca_n) \quad \forall a_i, c \in K \tag{9.3}$$

L' identità in K^n è $0_{K^n} = (0_K, 0_K, ..., 0_K)$, e l' elemento opposto di $(a_1, a_2, ..., a_n)$ è $(-a_1, -a_2, ..., -a_n) = -(a_1, a_2, ..., a_n)$. Ne consegue che $(K^n, +)$ è uno spazio vettoriale su K.

E' immediato vedere che gli n vettori $E_1 = (1, 0, 0....0)$, $E_2 = (0, 1, 0, ...0)$,...
..., $E_n = (0, 0, 0, ...1)$ generano tutto lo spazio K^n.

Nota: per semplicità di notazioni scriveremo 0 e 1 per le identità additive e moltiplicative di K, e sempre 0 per l' identità additiva di V. Di solito si capisce dal contesto di che identità si tratta.

9.2.2 Lo spazio delle matrici $m \times n$

Un altro insieme di oggetti che si possono sommare tra loro e moltiplicare per scalari è dato dalle matrici $m \times n$ con elementi in un campo K. La somma è semplicemente la somma matriciale, la moltiplicazione per un elemento a di K è data dalla moltiplicazione per a di ogni elemento della matrice. L' identità 0_V è la matrice con tutti gli elementi uguali a 0_K. Un insieme di matrici $m \times n$ che generi tutto V è dato dalle mn matrici M dove tutti gli elementi M_{ij} sono uguali a 0_K tranne un elemento che è uguale a 1_K.

9.2.3 Lo spazio delle funzioni

Anche le funzioni (per esempio da $\mathbb{R}$ in un campo K) si possono sommare tra loro e moltiplicare per uno scalare. La somma di due funzioni f e g è definita da

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in \mathbb{R} \tag{9.4}$$

e la moltiplicazione per un elemento a di K:

$$(af)(x) = af(x), \quad \forall a \in K, x \in \mathbb{R} \tag{9.5}$$

L' identità 0_V in questo caso è la "funzione 0", cioè la funzione che manda ogni $x \in \mathbb{R}$ in 0_K.

9.3 Vettori linearmente dipendenti

I vettori $u_1, ..., u_n$ si dicono **linearmente dipendenti** se esistono elementi $a_1, ..., a_n$ di K non tutti nulli tali che

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = 0 \tag{9.6}$$

Equivalentemente $u_1, ..., u_n$ sono linearmente dipendenti se uno dei vettori può essere espresso come combinazione lineare degli altri.

I vettori $u_1, u_2..., u_n$ si dicono **linearmente indipendenti** se non sono linearmente dipendenti, cioè se non esiste una relazione lineare (9.6) tra loro. In tal caso nessun u_i può essere espresso come combinazione lineare degli altri, e la relazione (9.6) è soddisfatta solo se tutti gli a_i sono nulli. Viceversa, se la (9.6) è soddisfatta solo con $a_i = 0$, $\forall i$, allora $u_1, u_2..., u_n$ sono linearmente indipendenti.

Esempio: i vettori $(1,1)$ e $(-3,2)$ in $\mathbb{R}^2$ sono linearmente indipendenti. Infatti $a(1,1)+b(-3,2)=0$ implica $a-3b=0$ e $a+2b=0$, da cui $a=0,\ b=0$.

Esercizio 1: i polinomi di grado n a coefficienti in K formano uno spazio vettoriale su K, con l' usuale somma di polinomi e moltiplicazione per un elemento di K. Dimostrare che i polinomi a coefficienti reali

$$x^2+2x+3, \quad x^2+4x+2, \quad x^2+4 \tag{9.7}$$

sono linearmente indipendenti.

Esercizio 2: dimostrare che i 4 vettori in K^4:

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}, \begin{pmatrix} 0 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ c_3 \\ c_4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ d_4 \end{pmatrix} \tag{9.8}$$

sono linearmente indipendenti se e solo se $a_1, b_2, c_3.d_4$ sono tutti diversi da 0. Nota: si generalizza a n vettori in K^n.

9.4 Base

Una **base** di V è un insieme di vettori linearmente indipendenti che generano V.

Se questo insieme è formato da n vettori $u_1, u_2..., u_n$, ogni vettore $v \in V$ può esprimersi come combinazione lineare dei u_i, in un unico modo. Se infatti vi fossero due combinazioni lineari diverse per esprimere lo stesso vettore, si avrebbe $a_1u_1 + a_2u_2 + ... + a_nu_n = b_1u_1 + b_2u_2 + ... + b_nu_n$, da cui segue $(a_1-b_1)u_1 + (a_2-b_2)u_2 + ... + (a_n-b_n)u_n = 0_V$, e quindi $a_i - b_i = 0_K$ per l' indipendenza lineare della base $u_1, u_2..., u_n$. Le due combinazioni lineari sono allora identiche. □

Teorema: se $\{u_1, u_2..., u_n\}$ è una base di V e $\{z_1, z_2..., z_m\}$ è un insieme di m vettori non nulli con $m > n$, allora questi m vettori sono linearmente dipendenti.

Dimostrazione: z_1 può scriversi come combinazione lineare dei vettori di base u_i:

$$z_1 = a_1u_1 + a_2u_2 + ... + a_nu_n \tag{9.9}$$

Poichè $z_1 \neq 0_V$, almeno uno degli a_i deve essere diverso da zero, supponiamo $a_1 \neq 0$. Allora si può esprimere u_1 come combinazione lineare di $z_1, u_2, ...u_n$:

$$u_1 = (a_1)^{-1}z_1 - (a_1)^{-1}a_2u_2 - (a_1)^{-1}a_3u_3 - ... - (a_1)^{-1}a_nu_n \tag{9.10}$$

L' insieme $\{z_1, u_2, ...u_n\}$ genera V (infatti contiene u_1, che insieme a $\{u_2, ...u_n\}$ genera V). Quindi z_2 può essere espresso come combinazione lineare di questo insieme di vettori:

$$z_2 = b_1z_1 + b_2u_2 + b_3u_3 + ... + b_nu_n \tag{9.11}$$

Se $b_2, b_3, ...b_n$ sono tutti nulli, allora $z_2 = b_1 z_1$ e il teorema è dimostrato. Se non sono tutti nulli, supponiamo che $b_2 \neq 0$. Si può allora esprimere u_2 come combinazione lineare di $z_1, z_2, u_3, ...u_n$:

$$u_2 = -(b_2)^{-1} b_1 z_1 + (b_2)^{-1} z_2 - (b_2)^{-1} b_3 u_3 - ... - (b_2)^{-1} b_n u_n \tag{9.12}$$

L' insieme $\{z_1, z_2, u_3 ... u_n\}$ genera V (infatti contiene u_2, che insieme a $\{z_1, u_3, ...u_n\}$ genera V). Si procede nello stesso modo fino a dimostrare che $\{z_1, ...z_n\}$ genera V. A questo punto z_{n+1} è esprimibile come combinazione lineare di $z_1, ...z_n$, e il teorema è dimostrato. □

Corollario: se $\{u_1, u_2..., u_n\}$ e $\{z_1, z_2..., z_m\}$ sono due basi per V, allora $n = m$. Dimostrazione: basta applicare il teorema precedente alle due basi. Quindi ogni possibile base per V ha lo stesso numero di vettori, e questo numero si dice **dimensione** dello spazio vettoriale V, e si indica con dim$V$. Se V contiene solo il vettore 0, allora non ha una base, e si pone dim$V = 0$.

• Se $v \in V$, possiamo scriverlo come combinazione lineare sulla base $\{u_i\}$:

$$v = v_1 u_1 + v_2 u_2 + ... + v_n u_n \tag{9.13}$$

dove v_1,...$v_n \in K$ sono chiamate le **componenti** del vettore v sulla base $\{u_i\}$. Il vettore v può allora essere rappresentato dalla colonna (matrice $n \times 1$):

$$v \quad \longrightarrow \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \tag{9.14}$$

Il vettore nullo 0_V è rappresentato da una colonna di 0_K. In seguito indicheremo gli zeri di V e di K con un unico simbolo 0.

Nota : ci possono essere molteplici basi in uno spazio vettoriale V. Per esempio se $\{u_1, u_2\}$ è una base per uno spazio vettoriale di dimensione 2, anche $\{u_1 + u_2, u_1 - u_2\}$ è una base (dimostrarlo). Le componenti di un vettore *dipendono* evidentemente dalla scelta della base.

9.5 Somma diretta

Siano U e W sottospazi vettoriali di V. Si definisce **somma** di U e W, indicata con $U + W$, il sottoinsieme di V formato da tutte le somme $u + w$, con $u \in U$ e $w \in W$. E' immediato verificare che $U + W$ è un sottospazio vettoriale di V.

Si dice che V è **somma diretta** di U e W, indicata con $U \oplus W$, se ogni vettore di V può esprimersi *in un unico modo* come somma di un vettore $u \in U$ e un vettore $w \in W$.

Teorema: se $V = U + W$ e $U \cap W = \{0\}$, allora $V = U \oplus W$.

Dimostrazione: se $v = u + w = u' + w'$ (con $v \in V$, $u, u' \in U$ e $w, w' \in W$), allora $u - u' = w' - w$. Poichè $u - u' \in U$ e $w' - w \in W$, e $U \cap W = \{0\}$, si ha $u - u' = 0 = w' - w$, cioè $u = u'$, $w = w'$. □

Teorema: se V è uno spazio vettoriale di dimensione finita, ed è somma diretta di sottospazi U e W, si ha

$$\dim V = \dim U + \dim W \tag{9.15}$$

Dimostrazione: se $\{u_1, ..., u_r\}$ è una base per U, e $\{w_1, ..., w_s\}$ è una base per W, ogni elemento di U ha un' espressione unica come combinazione lineare degli u_i e ogni elemento di W ha un' espressione unica come combinazione lineare degli w_j. Essendo V somma diretta di U e W, ogni suo elemento ha un' espressione unica come somma di un elemento di U e un elemento di W, e quindi un' espressione unica come combinazione lineare dei vettori $u_1, ...u_r, w_1, ...w_s$, i quali costituscono allora una base per V. Ne segue dim $V = r + s$. □

9.6 Prodotto diretto

Se U e W sono due spazi vettoriali sul campo K, si definisce **prodotto diretto** di U con W, denotato $U \times W$, l' insieme di tutte le coppie (u, w), dove $u \in U$ e $w \in W$. In questo insieme si definisce una somma e un prodotto per un elemento di K:

$$(u, w) + (u', w') = (u + u', w + w'), \tag{9.16}$$

$$c(u, w) = (cu, cw) \qquad u, u' \in U, \quad w, w' \in W, c \in K \tag{9.17}$$

così che $U \times W$ diventa uno spazio vettoriale. Si dimostra facilmente che

$$\dim U \times W = \dim U + \dim W \tag{9.18}$$

9.7 Applicazioni lineari

Consideriamo un' applicazione f tra due spazi vettoriali: $f : V \to W$, con dim$V = n$ e dim$W = m$, e V, W definiti sullo stesso campo K. L' applicazione f è **lineare** se, per ogni $a, b \in K$ e $u, v \in V$, si ha

$$\boxed{f(au + bv) = af(u) + bf(v)} \tag{9.19}$$

Un' applicazione lineare trasforma quindi una combinazione lineare di vettori nella stessa combinazione lineare dei vettori trasformati. Per specificare completamente un' applicazione lineare f, è sufficiente conoscere la sua azione sui vettori di una base $\{u_1, ...u_n\}$. In tal caso infatti risulta determinata anche la sua azione su un qualunque vettore $v = v_1u_1 + ...v_nu_n \in V$:

$$f(v) = f(v_1u_1 + ...v_nu_n) = v_1f(u_1) + ...v_nf(u_n) \in W \tag{9.20}$$

L' azione di f sul j-esimo vettore di base di V, cioè $f(u_j)$, è un vettore di W. Se $\{z_1, ...z_m\}$ è una base per W, si può esprimere ogni vettore $f(u_j)$ con $j = 1, 2, ...n$ come combinazione lineare dei vettori di questa base:

$$\begin{aligned} f(u_1) &= f_{11}z_1 + f_{21}z_2 + f_{31}z_3 + ...f_{m1}z_m \\ f(u_2) &= f_{12}z_1 + f_{22}z_2 + f_{32}z_3 + ...f_{m2}z_m \\ \vdots &\qquad \vdots \\ f(u_n) &= f_{1n}z_1 + f_{2n}z_2 + f_{3n}z_3 + ...f_{mn}z_m \end{aligned} \tag{9.21}$$

Si è costruita così una matrice di elementi $f_{ij} \in K$ con m righe e n colonne:

$$f_{ij} = \begin{pmatrix} f_{11} & f_{12} & f_{13} & ... & f_{1n} \\ f_{21} & f_{22} & f_{23} & ... & f_{2n} \\ f_{31} & f_{32} & f_{33} & ... & f_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{m1} & f_{m2} & f_{m3} & ... & f_{mn} \end{pmatrix} \tag{9.22}$$

dove la prima colonna è formata dalle componenti di $f(u_1)$, la seconda colonna dalle componenti di $f(u_2)$ e così via fino alla colonna n-esima. Si dice allora che l' applicazione lineare f è **rappresentata** dalla matrice f_{ij}, una matrice $m \times n$. Naturalmente la **matrice rappresentativa** di f dipende dalla scelta delle basi in V e W.

Possiamo anche esprimere le componenti di $f(v) \in W$ in termini delle componenti v_1,...v_n di v: si ha

$$\begin{aligned} f(v) = v_1 f(u_1) + ...v_n f(u_n) = v_1(f_{11}z_1 + f_{21}z_2 + f_{31}z_3 + ...f_{m1}z_m) \\ + v_2(f_{12}z_1 + f_{22}z_2 + f_{32}z_3 + ...f_{m2}z_m) \\ \vdots \qquad \vdots \\ + v_n(f_{1n}z_1 + f_{2n}z_2 + f_{3n}z_3 + ...f_{mn}z_m) \end{aligned} \tag{9.23}$$

da cui si vede che la prima componente di $f(v)$ (sulla base $\{z_i\}$) è data da $w_1 = f_{11}v_1 + f_{12}v_2 + ...f_{1n}v_n = \sum_{j=1}^{n} f_{1j}v_j$, e in generale la i-esima componente di $f(v)$ è data da $\sum_{j=1}^{n} f_{ij}v_j$. Se chiamiamo w_i le componenti di $w = f(v)$ sulla base $\{z_i\}$, si ha

$$\boxed{w_i = \sum_{j=1}^{n} f_{ij}v_j} \tag{9.24}$$

Questa equazione può anche scriversi in forma matriciale come $w = fv$ dove w e v sono vettori colonna e f la matrice $m \times n$ che rappresenta l' applicazione f (usiamo

lo stesso simbolo per indicare l' applicazione e la sua matrice rappresentativa):

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} = \begin{pmatrix} f_{11} & f_{12} & f_{13} & \cdots & f_{1n} \\ f_{31} & f_{32} & f_{33} & \cdots & f_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{m1} & f_{m2} & f_{m3} & \cdots & f_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_n \end{pmatrix} \tag{9.25}$$

Esercizio: siano $f : V \to W$ e $g : W \to T$ due applicazioni lineari, e V, W, T tre spazi vettoriali con $\dim V = n$, $\dim W = m$, $\dim T = q$. Dimostrare che $g \circ f$ è lineare, e che la matrice rappresentativa di $g \circ f$ è il prodotto matriciale della matrice $q \times m$ che rappresenta g con la matrice $m \times n$ che rappresenta f:

$$\boxed{(g \circ f)_{ij} = \sum_{k=1}^{m} g_{ik} f_{kj}} \tag{9.26}$$

Suggerimento: dato un vettore $v \in V$ si ponga $w = f(v)$ e $z = g(w)$. Scrivendo queste due relazioni in componenti come in (9.24), e sostituendo la prima nella seconda si trova $(g \circ f)_{ij}$.

Nota: se $f : V \to W$ è lineare, si ha $f(0) = 0$, poichè $f(0) = f(0 \cdot v) = 0 f(v) = 0$.

Esempio: consideriamo lo spazio vettoriale V dei polinomi di secondo grado $f(x) = ax^2 + bx + c$ a coefficienti reali, con somma e moltiplicazione per uno scalare definite nel modo usuale, e con lo zero 0_V dell' addizione dato dal polinomio nullo ($a = b = c = 0$). Una base è data dai tre polinomi $\{x^2, x, 1\}$: infatti $ax^2 + bx + c = 0_V$ implica $a = b = c = 0$, e ogni $f(x) = ax^2 + bx + c$ può scriversi come combinazione lineare degli elementi della base.

La derivata $D = d/dx$ è un' applicazione lineare su questo spazio vettoriale, essendo la derivata di una combinazione lineare di funzioni uguale alla combinazione lineare delle derivate. Cerchiamo allora la sua matrice rappresentativa sulla base $\{x^2, x, 1\}$. Bisogna agire su ogni elemento della base con la derivata D, e esprimere il vettore risultante sulla base $\{x^2, x, 1\}$. Per esempio $Dx^2 = 2x$ e quindi la prima colonna della matrice è formata dal vettore colonna $(0, 2, 0)$. Si ottiene così la matrice rappresentativa

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{9.27}$$

Possiamo verificare che applicando la matrice D sul vettore colonna (a, b, c) si ottiene il vettore che corrisponde alla derivata del polinomio rappresentato da (a, b, c): infatti

$$\begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 2a \\ b \end{pmatrix} \to 2ax + b \tag{9.28}$$

9.8 Cambio di base

Supponiamo di scegliere in V una base diversa $\{z_1, ...z_n\}$. Come cambiano le componenti di un vettore v e come cambia la matrice rappresentativa di un' applicazione f ?

Per trovare la risposta esprimiamo i vettori della vecchia base $\{u_i\}$ come combinazioni lineari dei vettori della nuova base $\{z_j\}$:

$$u_i = \sum_j S_{ji} z_j \tag{9.29}$$

dove i coefficienti S_{ij} della combinazione lineare appartengono al campo K e formano una matrice $n \times n$, chiamata **matrice di cambio di base** S. Inoltre, poichè anche $\{u_i\}$ è una base, ogni z_j può esprimersi come combinazione lineare dei u_i:

$$z_j = \sum_i S'_{ij} u_i \tag{9.30}$$

Da queste due relazioni segue che la matrice S' è l' inversa della matrice S, e scriveremo $S' = S^{-1}$. Consideriamo ora un qualunque vettore v, espresso sulla vecchia base come

$$v = v_1 u_1 + ... + v_n u_n = \sum_i v_i u_i \tag{9.31}$$

Sostituendo le espressioni di $u_1, ...u_n$ in termini della nuova base si trova

$$v = \sum_i v_i u_i = \sum_i v_i \sum_j S_{ji} z_j = \sum_j (\sum_i S_{ji} v_i) z_j \tag{9.32}$$

da cui si ricavano le componenti v'_j di v sulla nuova base:

$$v'_j = \sum_i S_{ji} v_i \tag{9.33}$$

che possiamo riscrivere in forma matriciale come

$$v' = Sv \Leftrightarrow v = S^{-1} v' \tag{9.34}$$

che riassume la relazione tra componenti v_i sulla vecchia base e componenti v'_i sulla nuova base per qualunque vettore v.

Troviamo ora la matrice che rappresenta una applicazione $f : V \to W$ sulla nuova base $\{z_1, ...z_n\}$ di V e su una nuova base $\{t_1, ...t_m\}$ di W. Siano S e T le matrici di cambiamento di base rispettivamente per V e W. Se $w = f(v)$, in notazione matriciale si ha

$$w = fv \quad \Longrightarrow \quad T^{-1} w' = f S^{-1} v' \quad \Longrightarrow \quad w' = T f S^{-1} v' \tag{9.35}$$

da cui risulta che la matrice che rappresenta f sulla nuova base è la matrice f' data da

$$f' = TfS^{-1} \tag{9.36}$$

Se $V = W$, la matrice rappresentativa di f sulla nuova base è

$$\boxed{f' = SfS^{-1}} \tag{9.37}$$

Questa trasformazione $f \to f'$ viene anche detta trasformazione di *similitudine*.

9.9 Nucleo e immagine di applicazioni lineari

Siano V e W due spazi vettoriali su K, e $f : V \to W$ una applicazione lineare. Si definisce **nucleo** di f, e si indica con Ker$f$, l' insieme degli elementi $v \in V$ tali che $f(v) = 0$.

Osservazione: Ker$f$ è un sottospazio vettoriale di V. Infatti poichè $f(0) = 0$, il vettore nullo di V appartiene a Ker$f$. Inoltre se $v, w \in$ Ker$f$, si ha $f(v + w) = f(v)+f(w) = 0+0 = 0$, e quindi $v+w \in$ Ker$f$, e se $c \in K$, si ha $f(cv) = cf(v) = 0$, cosicché anche $cv \in$ Ker$f$. □

Il nucleo di un' applicazione lineare f è utile per determinare se f è iniettiva. Ricordiamo che f è iniettiva se $f(v) = f(w) \Rightarrow v = w$.

Teorema 1: l' applicazione lineare f è iniettiva se e solo se Ker$f$ =$\{0\}$, i.e. il suo nucleo contiene solo il vettore nullo.

Dimostrazione: supponiamo che Ker$f$ =$\{0\}$, e che $f(v) = f(w)$. Allora $f(v-w) = f(v) - f(w) = 0$, quindi $v - w \in$ Ker$f \Rightarrow v - w = 0$ e allora $v = w$. Viceversa supponiamo che f sia iniettiva. In tal caso se $f(v) = 0$, si ha $f(v) = f(0)$, e per l' iniettività deve essere $v = 0$. Ne segue che Ker$f$ =$\{0\}$. □

Teorema 2: se $f : V \to W$ è un' applicazione lineare iniettiva, allora f trasforma vettori linearmente indipendenti di V in vettori linearmente indipendenti di W.

Dimostrazione: se $v_1, ...v_n$ sono vettori linearmente indipendenti di V, e se $x_1 f(v_1)+ \cdots + x_n f(v_n) = 0$, dimostriamo che tutti gli $x_i \in K$ devono essere nulli. Per linearità si ha $f(x_1v_1 + \cdots + x_nv_n) = 0$. Poichè il nucleo di f contiene solo il vettore nullo di V, bisogna che sia $x_1v_1 + \cdots + x_nv_n = 0$, e quindi per l' indipendenza lineare dei v_i, tutti gli x_i devono essere nulli. □

Osservazione: l' immagine di $f : V \to W$, denotata Imf, è un sottospazio vettoriale di W. Infatti: i) $f(0) = 0$, e quindi 0 appartiene a Imf; ii) supponendo che w_1, w_2 appartengano a Imf, allora esistono $v_1, v_2 \in V$ tali che $f(v_1) = w_1, f(v_2) = w_2$. Ne segue che $f(v_1 + v_2) = f(v_1) + f(v_2) = w_1 + w_2$ e quindi $w_1 + w_2$ è in Imf; iii) per ogni $c \in K$ si ha $f(cv_1) = cf(v_1) = cw_1$, e quindi $cw_1 \in$ Imf. □

Teorema 3: se $f : V \to W$ è un' applicazione lineare, si ha

$$\boxed{\dim V = \dim \mathrm{Ker} f + \dim \mathrm{Im} f} \tag{9.38}$$

Dimostrazione: se Imf è solo il vettore nullo, si ha dim Im$f = 0$, e il teorema è banalmente verificato. Supponiamo che $w_1, ...w_s$ sia una base di Imf, e che $v_1, ...v_s$ siano i vettori di V tali che $f(v_i) = w_i$. Se Ker$f \neq 0$, sia $u_1, ...u_q$ una base per Ker$f$ (se Ker$f = 0$ si omettono i vettori u_i da quello che segue). Dimostriamo allora che $\{v_1, ...v_s, u_1, ...u_q\}$ è una base per V, da cui segue che dim$V = s+q$, cioè l' enunciato del teorema. Per ogni $v \in V$, esistono $x_1, ...x_s \in K$ tali che $f(v) = x_1 w_1 + ...x_s w_s$ poichè $w_1, ...w_s$ è una base di Imf. Per linearità si ha $f(v) = f(x_1 v_1 + ...x_s v_s)$ e quindi $f(v - x_1 v_1 - ...x_s v_s) = 0$, il che dimostra che $v - x_1 v_1 - ...x_s v_s$ è nel nucleo di f. Allora esistono $y_1, ...y_q \in K$ tali che $v - x_1 v_1 - ...x_s v_s = y_1 u_1 + ... + y_q u_q$ e cioè $v = x_1 v_1 + ... + x_s v_s + y_1 u_1 + ... + y_q u_q$, e quindi i vettori $v_1, ...v_s, u_1, ...u_q$ generano V.

Per dimostrare che sono linearmente indipendenti, e che quindi formano una base per V, supponiamo che esista una loro combinazione lineare nulla: $x_1 v_1 + ... + x_s v_s + y_1 u_1 + ... + y_q u_q = 0$, e dimostriamo che tutti i coefficienti della combinazione devono essere nulli. Applicando f alla combinazione, e usando $f(u_i) = 0$, si ha $x_1 f(v_1) + ... + x_s f(v_s) = 0$, e poichè i vettori $w_i = f(v_i)$ sono linearmente indipendenti bisogna avere $x_i = 0$. La combinazione lineare diventa così $y_1 u_1 + ... + y_q u_q = 0$, ed essendo $u_1, ...u_q$ una base si deve avere $y_i = 0$. □

La figura 9.1 illustra le definizioni di nucleo e immagine di un' applicazione f.

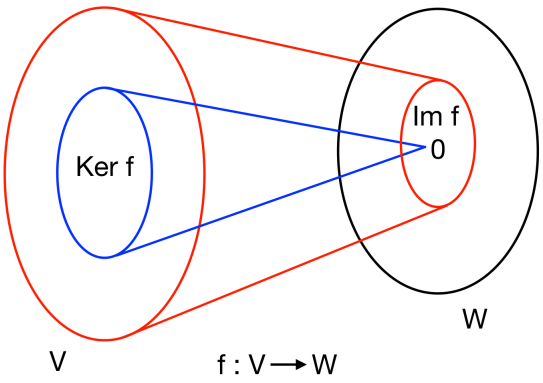


Fig. 9.1 Nucleo e immagine di un' applicazione.

Esempio 1: consideriamo l' applicazione $L : \mathbb{R}^3 \to \mathbb{R}^2$ definita da

$$L(x, z) = 3x - 2y + z \tag{9.39}$$

Il nucleo Ker$L$ è l' insieme delle soluzioni dell' equazione $3x - 2y + z = 0$. L' immagine ImL è $\mathbb{R}$, e quindi dim ImL=1. Dalla formula delle dimensioni (9.38) risulta allora dim Ker$L$ =2.

Esempio 2: sia $P : \mathbb{R}^3 \to \mathbb{R}^2$ definita da

$$P(x, y, z) = (x, y) \tag{9.40}$$

Il nucleo Ker$P$ è formato dagli elementi $(0, 0, z) \in \mathbb{R}^3$. Si ha dim Ker$P = 1$, dim Im$P = 2$ (l' applicazione è suriettiva), e la formula (9.38) risulta verificata.

Esempio 3: sia $F : \mathbb{R}^2 \to \mathbb{R}^2$ definita da:

$$F(x, y) = (3x - y, 4x + 2y) \tag{9.41}$$

E' facile dimostrare che il sistema lineare $3x - y = 0,\ 4x + 2y = 0$ ha per unica soluzione $x = y = 0$, e quindi Ker$F = \{0_{\mathbb{R}^2}\}$. Per il Teorema 1, l' applicazione F è iniettiva. E' anche suriettiva poichè per ogni vettore (v_1, v_2) di $\mathbb{R}^2$ esistono x, y tali che $F(x, y) = (v_1, v_2)$ (dimostrarlo). Si ha allora dim Ker$F = 0$, dim ImF=2, sempre in accordo con la formula (9.38).

Nota: se $f : V \to W$ è lineare con Ker$f$=$\{0\}$, e suriettiva, allora f è biiettiva e quindi invertibile. Dimostrazione: immediata poichè f in questo caso è iniettiva per il Teorema 1, e suriettiva. □

9.10 Operatori lineari

Un **operatore lineare** su uno spazio vettoriale V è un' applicazione lineare $A : V \to V$. Quindi A trasforma un vettore v di V in un vettore w di V, e si usa scrivere $Av = w$ al posto di $A(v) = w$. Gli operatori lineari vengono solitamente denotati con lettere maiuscole.

• La matrice che rappresenta A su una base di V è una matrice quadrata dim V×dim V.

• Dati due operatori A e B, la loro *somma* $A + B$ è definita da:

$$(A + B)v \equiv Av + Bv \quad \forall v \in V \tag{9.42}$$

La sua rappresentazione matriciale è la somma delle matrici che rappresentano A e B. L' *operatore nullo* $\mathbf{0}$ è tale che $\mathbf{0}v = 0_V$ per ogni $v \in V$, e si ha $A + \mathbf{0} = A$ per ogni operatore A.

• Il prodotto di uno scalare $c \in K$ con un operatore A è definito da $(cA)v \equiv c(Av), \forall v \in V$. La matrice che rappresenta cA è quindi la matrice la matrice che rappresenta A moltiplicata per lo scalare c. Nota: $cA = Ac$.

• Dati due operatori A e B, il loro *prodotto* AB è definito dalla legge di composizione di applicazioni:

$$(AB)v \equiv A(Bv) \tag{9.43}$$

• L' *operatore identità* I è definito da $Iv = v$ per ogni $v \in V$, e soddisfa $AI = IA = A$. La matrice che rappresenta I è la matrice diagonale con elementi sulla diagonale tutti uguali a 1.

• La matrice che rappresenta AB viene ottenuta moltiplicando (prodotto righe per colonne) la matrice che rappresenta A per la matrice che rappresenta B.

• Due operatori A e B sono uguali se la loro azione su tutti i vettori è uguale (o equivalentemente se la loro differenza è l' operatore nullo).

• L' operatore *inverso* A^{-1} è definito da

$$A^{-1}A = AA^{-1} = I \tag{9.44}$$

La matrice che lo rappresenta è quindi l' inversa della matrice che rappresenta A. Vedremo in seguito la condizione di esistenza della matrice inversa A^{-1}, e come costruirla esplicitamente.

• In genere gli operatori non commutano, cioè $AB \neq BA$, come si può capire considerando la loro rappresentazione matriciale (il prodotto di matrici in genere non commuta). La differenza tra AB e BA viene chiamata **commutatore** e indicata come segue:

$$[A, B] \equiv AB - BA \tag{9.45}$$

Esercizio: dalla definizione di sopra dimostrare le proprietà:

$$[A, B] = -[B, A] \quad \text{antisimmetria} \tag{9.46}$$
$$[A, BC] = [A, B]C + B[A, C] \tag{9.47}$$
$$[AB, C] = A[B, C] + [A, C]B \tag{9.48}$$
$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0 \tag{9.49}$$

9.11 Prodotto scalare

Sia V uno spazio vettoriale su un campo K. Un **prodotto scalare** su V associa a ogni paio di elementi v, w di V uno scalare $\in K$, denotato con $\langle v, w\rangle$, che soddisfa le proprietà:

1) $\langle v, w\rangle = \langle w, v\rangle \quad \forall v, w \in V$.
2) $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle \quad \forall u, v, w \in V$.
3) $\langle u, xv\rangle = x\langle u, v\rangle \quad \forall u, v \in V, x \in K$

Da queste tre proprietà si deduce immediatamente che il prodotto scalare è lineare nei suoi due argomenti:

$$\langle u, av + bw\rangle = a\langle u, v\rangle + b\langle u, w\rangle \tag{9.50}$$
$$\langle av + bw, u\rangle = a\langle v, u\rangle + b\langle w, u\rangle \quad \forall u, v, w \in V, a, b \in K \tag{9.51}$$

Esempio: prodotto scalare su K^n definito da $\langle v, w\rangle = v_1 w_1 + \cdots v_n w_n$, se i vettori v, w sono le n-uple $v = (v_1, ..., v_n)$, $w = (w_1, ...w_n)$.

• Due vettori v, w si dicono **ortogonali** se $\langle v, w\rangle = 0$; si scrive anche $v \perp w$. Se S è un sottoinsieme di V, si denota con $S^\perp$ l' insieme di tutti i vettori di V ortogonali a tutti i vettori di S. Dalle proprietà del prodotto scalare si deduce immediatamente che $S^\perp$ è un sottospazio vettoriale di V, detto lo *spazio ortogonale* a S.

Nota: se $w \perp S$, cioè se w è ortogonale a ogni vettore di S, allora w è ortogonale a tutte le combinazioni lineari di vettori di S, cioè al sottospazio vettoriale U generato dai vettori di S.

9.12 Prodotto scalare in campo reale

Se V è uno spazio vettoriale V sul campo dei numeri reali $\mathbb{R}$, con un prodotto scalare. Il prodotto scalare è **definito positivo** se per ogni $v \in V$ si ha $\langle v, v\rangle \geq 0$, dove l' uguaglianza vale solo se $v = 0$.

• La **norma** (o **lunghezza**) di un vettore $v \in V$, denotata $||v||$, è definita da

$$||v|| = \sqrt{\langle v, v\rangle} \tag{9.52}$$

Se $c \in \mathbb{R}$, si ha $||cv|| = \sqrt{\langle cv, cv\rangle} = \sqrt{c^2\langle v, v\rangle} = |c|\ ||v||$.

• La **distanza** tra due vettori v, w è definita da

$$dist(v, w) = ||v - w|| \tag{9.53}$$

• **Teorema di Pitagora:** se v e w sono ortogonali, si ha

$$||v + w||^2 = \langle v + w, v + w\rangle = \langle v, v\rangle + 2\langle v, w\rangle + \langle w, w\rangle = ||v||^2 + ||w||^2 \tag{9.54}$$

poichè $\langle v, w\rangle = 0$.

• Se $||w|| \neq 0$, per ogni v esiste un unico numero c tale che $v - cw$ sia ortogonale a w. Infatti da $\langle v - cw, w\rangle = 0$ si trova

$$c = \frac{\langle v, w\rangle}{\langle w, w\rangle} \tag{9.55}$$

c è detta la *componente di v lungo w*, e cw la *proiezione di v su w*.

• **Disuguaglianza di Schwarz:** $|\langle v, w\rangle| \leq ||v||\ ||w||$.

Dimostrazione: applichiamo il teorema di Pitagora (vedi sopra) ai vettori ortogonali $v - cw$ e cw, dove c è la componente di v lungo w. Si ha:

$$||v||^2 = ||v - cw||^2 + ||cw||^2 \quad \Rightarrow \quad ||cw||^2 \leq ||v||^2 \quad \Rightarrow \quad c^2||w||^2 \leq ||v||^2 \tag{9.56}$$

Sostituendo per c l' espressione (9.55) si trova la disuguaglianza di Schwarz. $\square$

• **Disuguaglianza triangolare:** $||v + w|| \leq ||v|| + ||w||$

Dimostrazione: ambo i membri sono numeri ≥ 0. Allora basta verificare che i loro quadrati verificano la disuguaglianza. Si ha:

$$\langle v+w, v+w\rangle = \langle v, v\rangle + 2\langle v, w\rangle + \langle w, w\rangle \leq ||v||^2 + 2||v||\ ||w|| + ||w||^2 = (||v|| + ||w||)^2$$

dove si è usata la disuguaglianza di Schwarz. Si ha pertanto $||v + w||^2 \leq (||v|| + ||w||)^2$. $\square$

9.13 Esempio: prodotto scalare in $\mathbb{R}^n$

Consideriamo lo spazio vettoriale delle n-uple di elementi di $\mathbb{R}$, denotato $\mathbb{R}^n$, con somma e prodotto per un numero reale definiti come in Sez. 9.2. Se $v = (v_1, ..., v_n)$ e $w = (w_1, ..., w_n)$ sono due vettori di $\mathbb{R}^n$, si definisce il loro prodotto scalare:

$$v \cdot w = v_1 w_1 + \cdots v_n w_n \tag{9.57}$$

Esercizio: verificare che questo prodotto scalare soddisfa tutte le proprietà di un prodotto scalare definito positivo (vedi Sez. 9.11). Valgono allora tutte le definizioni (norma, distanza) e disuguaglianze della Sezione 9.12.

• I vettori di $\mathbb{R}$ individuano punti nello spazio cartesiano a n dimensioni, e possono rappresentarsi come segmenti orientati (frecce) dall' origine dello spazio al punto individiato dalle n coordinate della n-upla. Per il teorema (geometrico) di Pitagora, la lunghezza di un vettore (freccia) v, denotata $||v||$, è data da

$$||v|| = \sqrt{v_1 v_1 + \cdots v_n v_n} \tag{9.58}$$

In termini del prodotto scalare si ha $||v|| = \sqrt{v \cdot v}$, il che giustifica la definizione di norma della Sezione 9.12.

• Se due vettori v, w sono ortogonali (cioè i segmenti che li rappresentano nello spazio cartesiano sono ortogonali) allora si dimostra che $v \cdot w = 0$. Infatti dalla linearità del prodotto scalare si ha

$$(v + w) \cdot (v + w) = v \cdot v + w \cdot w + 2v \cdot w \tag{9.59}$$

D' altra parte, per il teorema (geometrico) di Pitagora applicato al triangolo rettangolo di cateti v e w si deve avere

$$(v + w) \cdot (v + w) = v \cdot v + w \cdot w \tag{9.60}$$

da cui si deduce che $v \cdot w = 0$ $\square$.

• La definizione del prodotto scalare $v \cdot w$ dà lo stesso risultato della definizione "geometrica"

$$v \cdot w = ||v||\ ||w||\ \cos\theta \tag{9.61}$$

dove θ è l' angolo formato dai due vettori (frecce) v e w. Dimostrazione: consideriamo i vettori perpendicolari w e $v - cw$ con $c = (v \cdot w)/(w \cdot w)$. Dalla definizione di $\cos\theta$, si ha $c\ ||w|| = ||v||\ \cos\theta$, da cui segue la formula di sopra. □

9.14 Prodotto scalare in campo complesso

Sia V uno spazio vettoriale sul campo dei numeri complessi $\mathbb{C}$. In questo caso le proprietà del prodotto scalare vanno generalizzate come segue:

1) $\langle v, w\rangle = \langle w, v\rangle^*\ \ \forall v, w \in V$.
2) $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle\ \ \forall u, v, w \in V$.
3) $\langle u, zv\rangle = z\langle u, v\rangle\ \ \forall u, v \in V, z \in \mathbb{C}$

Solo la proprietà 1) è stata generalizzata, ma questa ha conseguenze sulla linearità del prodotto scalare. Infatti dalle tre proprietà si deduce che il prodotto scalare è lineare nel suo secondo argomento e *antilineare* nel primo argomento:

$$\langle u, av + bw\rangle = a\langle u, v\rangle + b\langle u, w\rangle \tag{9.62}$$

$$\langle av + bw, u\rangle = a^*\langle v, u\rangle + b^*\langle w, u\rangle \quad \forall u, v, w \in V, a, b \in \mathbb{C} \tag{9.63}$$

La leggera modifica della proprietà 1) è necessaria per avere un prodotto scalare definito positivo, per il quale $\langle v, v\rangle \geq 0,\ \forall v \in V$, dove l' uguaglianza vale solo se $v = 0$. Infatti dalla proprietà 1) risulta che $\langle v, v\rangle$ è uguale al suo complesso coniugato, cioè è un numero reale, e ha senso richiedere che sia maggiore di zero per $v \neq 0$. Si può inoltre definire la norma di un vettore e la distanza tra due vettori esattamente come nel caso reale, e dimostrare il teorema di Pitagora e le disuguaglianze di Schwarz e triangolare in modo analogo (con lievi modifiche, da verificare come esercizio).

9.15 Base ortonormale

In questa Sezione consideriamo spazi vettoriali sul campo dei numeri complessi. Ovviamente tutti i risultati valgono anche sul campo reale come caso particolare.

Data una base $\{v_1, ...v_n\}$ in uno spazio vettoriale V con prodotto scalare definito positivo, si può sempre costruire una base $\{v'_1, ...v'_n\}$ di vettori ortogonali come segue:

$$
\begin{aligned}
v'_1 &= v_1, \\
v'_2 &= v_2 - \frac{\langle v'_1, v_2\rangle}{\langle v'_1, v'_1\rangle}\, v'_1, \\
v'_3 &= v_3 - \frac{\langle v'_2, v_3\rangle}{\langle v'_2, v'_2\rangle}\, v'_2 - \frac{\langle v'_1, v_3\rangle}{\langle v'_1, v'_1\rangle}\, v'_1, \\
&\vdots \qquad\qquad \vdots \\
v'_n &= v_n - \frac{\langle v'_{n-1}, v_n\rangle}{\langle v'_{n-1}, v'_{n-1}\rangle}\, v'_{n-1} - \cdots - \frac{\langle v'_1, v_n\rangle}{\langle v'_1, v'_1\rangle}\, v'_1.
\end{aligned} \tag{9.64}
$$

Questa costruzione è detta *procedura di ortogonalizzazione di Gram-Schmidt*.

Esercizio: verificare l' ortogonalità dei vettori v'_i.

Esercizio: verificare che n vettori ortogonali sono linearmente indipendenti.

I vettori ortogonali $v'_1, ...v'_n$ formano una base se $\dim V = n$. Possono essere **normalizzati**, cioè divisi per la loro norma:

$$
u_i = \frac{v'_i}{||v'_i||} \tag{9.65}
$$

I vettori u_i risultanti sono allora **ortonormali**, cioè ortogonali e con norma uguale a 1:

$$
\boxed{\langle u_i, u_j\rangle = \delta_{ij}} \tag{9.66}
$$

• Espressione del prodotto scalare di due vettori v, w in termini delle loro componenti v_i, w_j su una base ortonormale $u_1, ..., u_n$:

$$
\langle v, w\rangle = \langle \sum_i v_i u_i, \sum_j w_j u_j\rangle = \sum_i \sum_j v_i^* w_j \langle u_i, u_j\rangle = \sum_i v_i^* w_i \tag{9.67}
$$

Questa formula generalizza la nota formula per il prodotto scalare in campo reale (somma dei prodotti delle componenti omologhe).

• Espressione della matrice che rappresenta un operatore lineare $A : V \to V$ su una base ortonormale $u_1, ..., u_n$: applicando A a u_j si ha (vedi Sez. 9.7)

$$
Au_j = A_{1j}u_1 + \cdots + A_{ij}u_i + \cdots + A_{nj}u_n \tag{9.68}
$$

da cui si ricava, usando l' ortonormalità della base $\langle u_i, u_j\rangle = \delta_{ij}$:

$$
\boxed{A_{ij} = \langle u_i, Au_j\rangle} \tag{9.69}
$$

• **Teorema:** se S è un sottospazio di V, si ha $\dim S + \dim S^{\perp} = \dim V$.

Dimostrazione: si può costruire una base ortogonale $u_1, ..., u_m$ per il sottospazio S. Se S è un sottospazio proprio di V, deve esistere un vettore v tale che $u_1, ..., u_m, v$ siano linearmente indipendenti (altrimenti V coinciderebbe con S). Con la procedura di Gram-Schmidt si può allora ottenere un insieme di $m+1$ vettori ortogonali $u_1, ...u_m, u_{m+1}$. Se esiste un vettore w tale che $u_1, ...u_m, u_{m+1}, w$ siano linearmente indipendenti si ripete la procedura, finchè tutti i vettori di V sono esprimibili come combinazioni lineari di un insieme di vettori ortogonali $u_1, ...u_m, u_{m+1}, ...u_n$, che costituiscono pertanto una base ortogonale per V. I vettori ortogonali a S sono allora generati da $u_{m+1}, ...u_n$, che formano quindi una base per $S^{\perp}$. Ne segue il teorema. □

10 Sistemi di equazioni lineari

10.1 Sistema lineare omogeneo

Consideriamo il sistema di m equazioni lineari per le n incognite $x_1, ..., x_n$:

$$\begin{aligned} A_{11}x_1 + \cdots + A_{1n}x_n &= 0 \\ \vdots \qquad\qquad & \quad \vdots \\ A_{m1}x_1 + \cdots + A_{mn}x_n &= 0 \end{aligned} \tag{10.1}$$

dove gli elementi della matrice A_{ij} appartengono a un campo K. Si tratta di trovare le soluzioni $X = (x_1, ..., x_n)$, che possiamo considerare come vettori di K^n. Queste soluzioni formano un sottospazio vettoriale di K^n: è immediato vedere che una combinazione lineare di soluzioni X è ancora soluzione. Il sistema (10.1) può scriversi sotto forma matriciale come $AX = 0$, dove la matrice A agisce sul vettore X con moltiplicazione righe per colonne.

Possiamo interpretare lo spazio vettoriale delle soluzioni in tre modi:

1) le soluzioni sono date dai vettori $X = (x_1, ..., x_n)$ che corrispondono alle relazioni lineari $x_1A^1 + \cdots + x_nA^n = 0$ tra le colonne A^i della matrice A.
2) le soluzioni X formano lo spazio ortogonale ai vettori riga della matrice A.
3) le soluzioni X formano il nucleo dell' applicazione lineare rappresentata dalla matrice A, cioè sono soluzioni dell' equazione $AX = 0$.

10.2 Rango di una matrice

Sia A_{ij} una matrice $m \times n$. Le colonne $A^1, ..., A^n$ della matrice, considerate come vettori in uno spazio m-dimensionale, generano un sottospazio la cui dimensione è chiamato *rango delle colonne* della matrice. Questo rango è quindi il massimo numero di colonne A^i linearmente indipendenti. Analogamente, le righe $A_1, ..., A_m$ della matrice generano un sottospazio la cui dimensione è detta *rango delle righe* della matrice, ed è uguale al massimo numero di righe linearmente indipendenti.

• **Teorema del rango:** Sia A_{ij} una matrice $m \times n$. Allora il rango delle colonne e il rango delle righe sono uguali ad uno stesso numero r, e $n - r$ è la dimensione dello spazio delle soluzioni X del sistema lineare $AX = 0$.

Dimostrazione: definiamo l' applicazione $L_A : K^n \to K^m$:

$$L_A(X) \equiv x_1A^1 + \cdots + x_nA^n = AX \tag{10.2}$$

L' applicazione L_A è lineare (la verifica è immediata), ed è rappresentata dalla matrice A. Inoltre $\mathrm{Im}L_A$ è lo spazio generato dai vettori colonna di A, e $\mathrm{Ker}L_A$ è per definizione lo spazio delle soluzioni X di $AX = 0$. Applicando il teorema 3 della Sezione 9.9, si trova

$$\text{rango delle colonne} + \text{dimensione spazio delle soluzioni} = n$$

D' altra parte, interpretando lo spazio delle soluzioni come lo spazio ortogonale ai vettori riga della matrice, si ha

$$\text{rango delle righe} + \text{dimensione spazio delle soluzioni} = n$$

per l' ultimo Teorema della Sezione 9.15. Da queste due relazioni si ricava il Teorema. □

Si definisce **rango** della matrice A il numero r, uguale sia al rango delle colonne che al rango delle righe. Notiamo che il rango delle colonne è anche la dimensione di ImL_A, e quindi

$$\text{rango } A = \dim \text{ Im } L_A$$

• Tornando al sistema lineare omogeneo (10.1), dalla discussione di sopra segue che

$$\boxed{\text{dimensione spazio delle soluzioni} = n - \text{rango } A} \tag{10.3}$$

Se KerL_A contiene solo il vettore nullo (in tal caso la dimensione dello spazio soluzioni è 0), il sistema (10.1) ha per unica soluzione $X = 0$. Questo succede quando il rango di A è uguale a n.

Esempio: al sistema di 3 equazioni in 3 incognite x, y, z:

$$\begin{aligned} &x + 2z = 0 \\ &2x + 3y + z = 0 \\ &4x + 3y + 5z = 0 \end{aligned} \tag{10.4}$$

corrisponde la matrice

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 3 & 1 \\ 4 & 3 & 5 \end{pmatrix} \tag{10.5}$$

che ha rango 2 (verificarlo). La soluzione si ottiene in modo elementare per sostituzione, e si trova $x = -2z, y = z$ con z arbitrario, o equivalentemente $x = -2\alpha, y = \alpha, z = \alpha$ con α arbitrario. Lo spazio vettoriale delle soluzioni X di $AX = 0$ ha allora dimensione = 1, poichè contiene tutti i vettori proporzionali a

$$X = \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \tag{10.6}$$

Il vettore X può essere scelto come base dello spazio KerL_A. Si è così verificato che lo spazio delle soluzioni ha dimensione uguale a $3 -$ rango $A = 1$.

• **Teorema di invertibilità:** se A è una matrice $n \times n$, esiste il suo inverso A^{-1} se e solo se le sue colonne sono vettori linearmente indipendenti (ovvero rango $A = n$).

Dimostrazione: se le colonne $A^1, ..., A^n$ sono linearmente indipendenti, formano una base in K^n. In tal caso $L_A(X) = x_1A^1 + \cdots + x_nA^n$ è nullo solo per $X = (x_1, ..., x_n) = 0$. Quindi KerL_A=$\{0\}$ e L_A è iniettiva. Ma è anche suriettiva perchè ImL_A=K^n, e allora L_A è biiettiva e quindi invertibile, e la matrice che rappresenta L_A^{-1} è l' inversa della matrice A.

Viceversa, supponiamo che A sia invertibile. Allora il nucleo dell' applicazione L_A deve contenere solo il vettore nullo, cioè $AX = 0$ implica $X = 0$, e di conseguenza le colonne $A^1, ..., A^n$ sono linearmente indipendenti. □

10.3 Sistema lineare inomogeneo

Consideriamo il sistema inomogeneo di equazioni lineari:

$$\begin{aligned} A_{11}x_1 + \cdots + A_{1n}x_n &= b_1 \\ \vdots \qquad\qquad & \vdots \\ A_{m1}x_1 + \cdots + A_{mn}x_n &= b_m \end{aligned} \tag{10.7}$$

dove gli elementi di matrice A_{ij} e i **termini noti** b_i appartengono a un campo K. Il sistema può scriversi sotto forma matriciale come $AX = B$, con X vettore colonna di componenti $x_1, ...x_n$ e B vettore colonna di componenti $b_1, ...b_m$.

La matrice A (matrice $m \times n$) si dice la **matrice incompleta** del sistema. La matrice A' (matrice $m \times (n + 1)$) definita da $A' = (A^1, ...A^n, B)$, cioè ottenuta aggiungendo ad A come $(n+1)$-esima colonna la colonna B dei termini noti, si dice **matrice completa** del sistema.

Si chiama **soluzione** del sistema ogni vettore C di componenti $c_1, ...c_n \in K^n$ tale che $AC = B$, o equivalentemente $L_A(C) = B$. Ne consegue in particolare che il sistema ha soluzioni se e solo se B appartiene all' immagine dell' applicazione L_A.

Può succedere che il sistema non abbia soluzioni: per esempio

$$\begin{aligned} x + 3y - 2z &= 1 \\ x + 3y - 2z &= 2 \end{aligned} \tag{10.8}$$

non ha soluzioni per x, y, z. Se però esiste almeno una soluzione, allora tutte le soluzioni sono ottenibili sommando a questa soluzione una qualunque soluzione del sistema lineare omogeneo associato (con tutti i $b_i = 0$). Infatti se C è una soluzione di (10.9), cioè se $L_A(C) = B$, si ha anche $L_A(C + H) = B$ quando $H \in$ KerL_A. Infatti $L_A(C + H) = L_A(C) + L_A(H) = B + 0 = B$.

Anche in questo caso si può parlare di dimensione dello spazio delle soluzioni: è la dimensione dello spazio delle soluzioni del sistema omogeneo.

Il teorema che segue riguarda il caso $n = m$.

• **Teorema**: Un sistema di n equazioni lineari in n incognite:

$$\begin{aligned} A_{11}x_1 + \cdots + A_{1n}x_n &= b_1 \\ \vdots \qquad\qquad & \vdots \\ A_{n1}x_1 + \cdots + A_{nn}x_n &= b_n \end{aligned} \tag{10.9}$$

ha un' unica soluzione se e solo se la sua matrice incompleta A ha rango n, cioè è invertibile. In tal caso, l' unica soluzione del sistema è $C = A^{-1}B$.

Dimostrazione: Se il sistema ha un' unica soluzione C, allora $\mathrm{Ker}L_A = \{0\}$, poichè sappiamo che tutti i vettori colonna $C + H$ con $H \in \mathrm{Ker}L_A$ sono soluzioni. Dalla formula (9.38) si trova allora dim $\mathrm{Im}L_A = n$, e essendo rango $A =$ dim $\mathrm{Im}L_A$, si ha rango $A = n$.

Viceversa, se A è invertibile, applichiamo A^{-1} a entrambi i membri dell' equazione matriciale $AC = B$ e si trova la soluzione $C = A^{-1}B$. □

Col seguente teorema torniamo al caso generale con n non necessariamente uguale a m.

• **Teorema di Rouché-Capelli**. Il sistema di m equazioni lineari in n incognite $AX = B$ ha almeno una soluzione se e solo se la sua matrice incompleta A e la sua matrice completa A' hanno lo stesso rango. In tal caso, se C è una soluzione del sistema $AX = B$, le soluzioni del sistema sono tutte e sole del tipo $C + H$, con $H \in \mathrm{Ker}L_A$, cioè con H elemento del sottospazio vettoriale $\mathrm{Ker}L_A$ delle soluzioni del sistema omogeneo associato $AX = 0$. Se r è il rango di A, la dimensione di $\mathrm{Ker}L_A$ è $n - r$.

Dimostrazione: supponiamo che il sistema $AX = B$ abbia una soluzione $C \in K^n$, e quindi che valga $AC = B$. Questa equazione matriciale può riscriversi come $A^1c_1 + \cdots + A^nc_n = B$ dove $c_1, ...c_n$ sono le componenti di C, e $A^1, ...A^n$ le colonne della matrice A. Quindi B è combinazione lineare dei vettori $A^1, ...A^n$ in K^m, e il sottospazio generato da $A^1, ...A^n$ è uguale al sottospazio generato da $A^1, ...A^n, B$. Pertanto rango $A =$ rango A'.

Viceversa, supponiamo che il rango di A sia uguale al rango di A'. Allora il sottospazio generato da $A^1, ...A^n$ ha la stessa dimensione di quello generato da $A^1, ...A^n, B$, e essendo il primo contenuto nel secondo, devono coincidere (dimostrarlo). Quindi B appartiene al sottospazio di K^m generato da $A^1, ...A^n$, ossia è una combinazione lineare di $A^1, ...A^n$. Posto $c_1, ...c_n$ tali che $A^1c_1 + \cdots + A^nc_n = B$, si ha $AC = B$, e quindi C è una soluzione del sistema $AX = B$.

Due diverse soluzioni C e C' differiscono per un vettore di $\mathrm{Ker}L_A$, cioè per una soluzione del sistema omogeneo associato. Infatti da $AC = B$ e $AC' = B$ si ottiene $AC = AC'$ ovvero $A(C - C') = 0$ da cui si conclude che $C - C'$ appartiene al nucleo di $\mathrm{Ker}L_A$, cioè al sottospazio delle soluzioni di $AX = 0$. Viceversa, per ogni $H \in \mathrm{Ker}L_A$ e ogni soluzione C di $AX = B$, si ha $A(C + H) = AC + AH = AC + 0 = B$, cioè se C è soluzione lo è anche ogni $C + H$ con $H \in \mathrm{Ker}L_A$.

Finalmente da dim $\mathrm{Ker}L_A$ + dim $\mathrm{Im}L_A = n$, vedi la formula (9.38), ricordando che rango A = dim $\mathrm{Im}L_A$, si ha che la dimensione dello spazio delle soluzioni di $AX = 0$ è uguale a $n - r$. □

Esempio: consideriamo il sistema lineare inomogeneo

$$\begin{aligned} x + 2z &= 1 \\ 2x + 3y + z &= 2 \\ 4x + 3y + 5z &= 4 \end{aligned} \tag{10.10}$$

Il rango della matrice completa A' è 2, così come il rango della matrice incompleta A (verificarlo). Il sistema allora ammette soluzioni, con dimensione dello spazio delle soluzioni = 3 − 2 = 1. Una soluzione particolare è $x = -1, y = 1, z = 1$, e ogni altra soluzione si ottiene aggiungendo alla soluzione particolare una soluzione del sistema omogeneo associato, data da $x = -2\alpha, y = \alpha, z = \alpha$ con α arbitrario (vedi Esempio della Sezione precedente). Si ottiene allora

$$x = -1 - 2\alpha,\ y = 1 + \alpha,\ z = 1 + \alpha, \qquad \alpha \text{ arbitrario} \tag{10.11}$$

Nota: se si cambia il vettore dei termini noti in $(1, 2, 5)$, A' ha rango 3, e il sistema non ha soluzioni. Se poi si cambia da 4 a 6 il coefficiente di x nella terza equazione del sistema (10.10), si trova rango A = rango $A' = 3$, e la soluzione è unica: $x = 1/2, y = 1/4, z = 1/4$, in accordo col Teorema di Rouché-Capelli.

11 Determinanti

Prima di considerare le proprietà generali dei determinanti, trattiamo il caso particolare di matrici 2×2.

11.1 Determinante di una matrice 2×2

Sia A una matrice 2×2 con elementi di un campo K:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{11.1}$$

Il suo **determinante** $\det A$ è definito da

$$\boxed{\det A = ad - bc} \tag{11.2}$$

Il determinante può anche considerarsi funzione delle colonne A^1, A^2 o delle righe A_1, A_2 della matrice A e in tal caso lo scriviamo come $\det(A^1, A^2)$ oppure $\det(A_1, A_2)$. Si usa anche la notazione $D(A^1, A^2)$ etc.

Le seguenti proprietà di $\det A$ possono essere direttamente verificate sulla matrice (11.1).:

1) $\det(A + B, C) = \det(A, C) + \det(B, C)$, dove A, B, C sono vettori colonna (o vettori riga). Analogamente $\det(A, B+C) = \det(A, B) + \det(A, C)$. Inoltre se $t \in K$ si ha $\det(tA, B) = \det(a, tB) = t \det(A, B)$. Quindi il determinante, come funzione dei vettori colonna o dei vettori riga, è lineare.

2) se due colonne (o due righe) sono uguali, il determinante è nullo.

3) $\det I = 1$

4) il valore del determinante non cambia se a una colonna si aggiunge un multiplo di un' altra colonna. Idem per le righe.

5) se si scambiano due colonne (o due righe) il valore del determinante cambia segno.

6) i vettori colonna A^1 e A^2 della matrice A sono linearmente dipendenti se e solo se $\det A = 0$. Idem per i vettori riga.

11.2 Determinante di una matrice $n \times n$

Se A è una matrice $n \times n$, il suo determinante è definito per induzione, in termini di determinanti di matrici $(n-1) \times (n-1)$:

$$\boxed{\det A = (-1)^{i+1} A_{i1} \det \widetilde{A}_{i1} + \cdots + (-1)^{i+n} A_{in} \det \widetilde{A}_{in}} \tag{11.3}$$

dove $\widetilde{A}_{ij}$ è la matrice $(n-1)\times(n-1)$ ottenuta dalla matrice A togliendo la i-esima riga e la j-esima colonna. Dimostreremo nella Sezione 11.5 che questa definizione porta allo stesso risultato qualunque sia i, compreso tra 1 e n. Quindi per calcolare il determinante, si può scegliere una riga qualsiasi della matrice (riga i-esima) $A_{i1}, ...A_{in}$, e quindi calcolare la somma indicata in (11.3). Lo stesso si può fare con le colonne $A_{1j}, ...A_{nj}$:

$$\det A = (-1)^{j+1} A_{1j} \det \widetilde{A}_{1j} + \cdots + (-1)^{j+n} A_{nj} \det \widetilde{A}_{nj} \tag{11.4}$$

La formula (11.3) corrisponde allo *sviluppo per riga del determinante*, mentre la (11.4) corrisponde allo *sviluppo per colonna*.

Analogamente al caso di matrici 2×2, si può denotare il determinante di una matrice $n\times n$ come $D(A^1, ..., A^n)$, dove $A^1, ..., A^n$ sono le colonne della matrice.

Teorema: il determinante soddisfa le seguenti proprietà:

1) è lineare nelle sue colonne:

$$D(A^1, ..., B+C, ..., A^n) = D(A^1, ...B, ..., A^n) + D(A^1, ..., C, ..., A^n) \tag{11.5}$$
$$D(A^1, ..., tB, ..., A^n) = tD(A^1, ..., B, ..., A^n), \quad t \in K \tag{11.6}$$

Similmente è lineare nelle sue righe.

2) si ha $D(A^1, ..., B, B, ..., A^n) = 0$. Cioè se una matrice ha due colonne adiacenti uguali, il suo determinante è nullo. Idem per le righe.

3) $\det I = 1$

Dimostrazione: per induzione. Si suppongono vere le proprietà 1),2),3) per determinanti di matrici $(n-1)\times(n-1)$, e si dimostra che valgono nel caso $n\times n$.

1) consideriamo $D(A^1, ...A^k, ...A^n)$ come funzione della colonna k-esima. Il termine j-esimo nella somma in (11.3) è $(-1)^{i+j} A_{ij} \det \widetilde{A}_{ij}$, e se $j \neq k$ allora A_{ij} non dipende da A^k, e $\det \widetilde{A}_{ij}$ dipende linearmente dalla colonna k-esima (per ipotesi di induzione). Se invece $j = k$, allora A_{ij} dipende linearmente dalla k-esima colonna, mentre $\det \widetilde{A}_{ij}$ non dipende dalla k-esima colonna. Poichè $\det A$ è una somma di questi termini, dipende linearmente dalla k-esima colonna. □

2) Supponiamo che siano uguali le colonne A^k e A^{k+1}, e sia j un indice diverso da k e da $k+1$. Allora la matrice $\widetilde{A}_{ij}$ ha due colonne adiacenti uguali e quindi il suo determinante è nullo. Quindi sono nulli tutti i termini nella somma (11.3) tranne due:

$$(-1)^{i+k} A_{ik} \det \widetilde{A}_{ik} + (-1)^{i+k+1} A_{i,k+1} \det \widetilde{A}_{i,k+1} \tag{11.7}$$

Le due matrici $\widetilde{A}_{ik}$ e $\widetilde{A}_{i,k+1}$ sono uguali poichè la colonna k-esima di A è uguale alla colonna $k+1$-esima. Similmente gli elementi di matrice A_{ik} e $A_{i,k+1}$ sono uguali, e

i due termini nell' espressione di sopra si cancellano perchè hanno segno opposto. □

3) Se $A = I$, gli unici elementi di A diversi da zero sono quelli diagonali, tutti uguali a 1: $A_{ii} = 1$. Allora la somma in (11.3) si riduce al solo termine:

$$(-)^{i+i} A_{ii} \det \widetilde{A}_{ii} \tag{11.8}$$

che è uguale a 1, poichè $(-)^{2i} = 1$, $A_{ii} = 1$ e $\widetilde{A}_{ii}$ è la matrice identità $(n-1)\times(n-1)$. □

Da queste tre proprietà segue che

4) il valore del determinante non cambia se a una colonna si aggiunge un multiplo di un' altra colonna. Idem per le righe.

5) se si scambiano due colonne (o due righe) il valore del determinante cambia segno.

6) se i vettori colonna A^1,...A^n della matrice A sono linearmente dipendenti si ha $\det A = 0$. Idem per i vettori riga.

Dimostrazione: dalla 2) si deduce che lo scambio di due colonne adiacenti provoca un cambio di segno nel determinante. Infatti si ha

$$0 = D(A^1, ..., B + C, B + C...A^n) = D(A^1, ..., B, C...A^n) + D(A^1, ..., C, B...A^n) \tag{11.9}$$

Ma allora si ha anche

$$D(A^1, ..., B, ..., B, ...A^n) = 0 \tag{11.10}$$

cioè il determinante è nullo anche se due colonne, non necessariamente adiacenti, sono uguali. Infatti basta avvicinare una delle due colonne B all' altra mediante scambi con colonne vicine, (ogni scambio comporta un cambio di segno del determinante) fino a renderle adiacenti. Ora con lo stesso ragionamento di sopra si vede che il determinante cambia segno sotto scambio di due colonne anche non adiacenti. Abbiamo così dimostrato la proprietà 5). Dalla (11.10) e dalla linearità del determinante segue la 4). Finalmente la proprietà 6) discende dal fatto che se $A^1, ..., A^n$ sono vettori colonna linearmente dipendenti, si può esprimere uno di questi come combinazione lineare degli altri, e per linearità il determinante di A diventa la somma di determinanti di matrici con due colonne uguali, ognuno dei quali è nullo. □

11.3 Regola di Cramer

Le proprietà dei determinanti discusse nella Sezione precedente ci permettono di dimostrare la *regola di Cramer* per la risoluzione di sistemi di equazioni lineari.

Teorema (Regola di Cramer): Siano $A^1, ..., A^n$ vettori colonna con n componenti tali che $D(A^1, ..., A^n) \neq 0$. Sia B un vettore colonna. Consideriamo il sistema di n equazioni lineari:

$$x_1 A^1 + \cdots + x_n A^n = B \tag{11.11}$$

dove $x_1, ...x_n \in K$ sono le incognite da determinare. Allora si ha, per ogni $j = 1, ...n$:

$$\boxed{x_j = \frac{D(A^1, ..., B, ..., A^n)}{D(A^1, ..., A^n)}} \tag{11.12}$$

dove B sostituisce la colonna A^j.

Dimostrazione: si ha

$$\begin{aligned} D(A^1, ..., B, ..., A^n) &= D(A^1, ..., \ x_1 A^1 + \cdots + x_n A^n, ..., A^n) = \\ &= D(A^1, ..., \ x_j A^j, ..., A^n) = \\ &= x_j D(A^1, ..., A^j, ..., A^n) = \\ &= x_j D(A^1, ..., A^n) \end{aligned} \tag{11.13}$$

□

11.4 Matrice triangolare

Se A è una matrice $n \times n$, tramite due tipi di operazioni sulle colonne può essere trasformata in una matrice triangolare

$$B = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}.$$

Le due operazioni sono: 1) aggiunta a una colonna di multipli di altre colonne; 2) scambio di colonne. L' operazione 1) non cambia il determinante, mentre l' operazione 2) ne cambia il segno. Il determinante della matrice triangolare è dato semplicemente dal prodotto dei suoi elementi diagonali, e si capisce allora che rendere una matrice triangolare può essere un metodo pratico per calcolarne il determinante. Notiamo anche che le operazioni 1) e 2) non cambiano il rango della matrice, e quindi rango A = rango B.

La dimostrazione che A può sempre essere trasformata in B tramite le operazioni 1) e 2) procede per induzione su n. Per $n = 1$ non c'è niente da dimostrare. Per $n > 1$, se tutti gli elementi della prima riga di A sono 0, allora si applica l' ipotesi di induzione alla sottomatrice $\widetilde{A}_{11}$, e si ottiene B. Se qualche elemento della prima riga è diverso da 0, tramite scambio di colonne possiamo supporre $A_{11} \neq 0$. Aggiungendo

multipli della prima colonna alle altre colonne si può costruire una matrice B tale che tutti gli elementi della prima riga, tranne il primo, siano nulli. A questo punto si applica l' ipotesi di induzione alla sottomatrice $\widetilde{A}_{11}$. □

Nella Sezione 11.2 abbiamo dimostrato la proprietà 6) dei determinanti: se n vettori in K^n sono linearmente dipendenti, la matrice che ha per colonne questi vettori ha determinante nullo. Il seguente teorema estende questa proprietà con un "se e solo se".

Teorema: sia A una matrice $n \times n$. Le colonne $A^1, ..., A^n$ sono vettori di K^n linearmente indipendenti se e solo se $\det A \neq 0$, o equivalentemente, le colonne $A^1, ..., A^n$ sono linearmente dipendenti se e solo se $\det A = 0$.

Dimostrazione: triangolarizzando la matrice si ottiene una matrice B con $\det B$ dato dal prodotto degli elementi diagonali. Come per l' esercizio 2 della Sezione 9.3, è facile verificare che le colonne della matrice B sono linearmente indipendenti (e quindi anche le colonne della matrice A sono linearmente indipendenti, poichè rango$A$ = rango$B$) se e solo se tutti gli elementi sulla diagonale sono diversi da 0, cioè se e solo se $\det B \neq 0$ (e quindi $\det A \neq 0$). □

11.5 Determinanti e permutazioni

Osservazione: Siano $X^1, ...X^n$ vettori in uno spazio vettoriale di dimensione n sul campo K, B una matrice $n \times n$ con elementi in K, e poniamo:

$$\begin{aligned} A^1 &= B_{11}X^1 + ... + B_{n1}X^n \\ \vdots \quad & \quad \vdots \quad \quad \vdots \\ A^n &= B_{1n}X^1 + ... + B_{nn}X^n \end{aligned} \tag{11.14}$$

Allora si ha

$$\begin{aligned} D(A^1, ..., A^n) &= D(B_{11}X^1 + ... + B_{n1}X^n, ..., B_{1n}X^1 + ... + B_{nn}X^n) = \\ &= \sum_\sigma B_{\sigma(1),1} \cdots B_{\sigma(n),n} D(X^{\sigma(1)}, ..., X^{\sigma(n)}) \end{aligned} \tag{11.15}$$

dove σ è un' applicazione che assegna un intero dell' intervallo $[1, ..., n]$ a ogni intero dello stesso intervallo, e $\sum_\sigma$ è la somma su tutte le possibili assegnazioni σ. Per arrivare all' espressione di sopra si è usata la linearità nelle colonne del determinante D. Per convincersi della validità dell' espressione di sopra è utile verificarla nel caso $n = 3$. Notiamo poi che $D(X^{\sigma(1)}, ..., X^{\sigma(n)})$ è nullo se due colonne $X^{\sigma(i)}$ e $X^{\sigma(j)}$ sono uguali, e quindi se $\sigma(i) = \sigma(j)$, per $i \neq j$. Dunque nella somma su σ possiamo considerare solo le assegnazioni per le quali $\sigma(i) = \sigma(j)$, per $i \neq j$, cioè le applicazioni iniettive dell' insieme $\{1, ...n\}$ in se stesso, quindi le biiezioni. Queste sono le permutazioni, discusse nella Sezione 7.8.

Usando la proprietà di antisimmetria del determinante per scambio di colonne, si arriva all' espressione

$$D(A^1, ..., A^n) = \sum_\sigma \mathrm{sgn}(\sigma) B_{\sigma(1),1} \cdots B_{\sigma(n),n} D(X^1, ..., X^n) \tag{11.16}$$

dove $\mathrm{sgn}(\sigma)$ è la segnatura della permutazione.

Scegliendo infine per $X^1, ..., X^n$ la base standard $E^1, ...E^n$ di K^n si ha che A^i diventa uguale al vettore $(B_{1i}, ..B_{ni})$, e quindi $D(A^1, ...A^n)$ diventa uguale a $\det B$. Si trova quindi l' espressione per il determinante della matrice B:

$$\det B = \sum_\sigma \mathrm{sgn}(\sigma) B_{\sigma(1),1} \cdots B_{\sigma(n),n} \tag{11.17}$$

avendo usato $D(E^1, ..., E^n) = \det I = 1$. Notiamo che le tre proprietà 1),2),3) (vedi Sezione 11.2) determinano univocamente il determinante, dato dall' espressione di sopra. Ne consegue che questa espressione dà lo stesso risultato dell' espressione (11.3) della Sezione 11.2.

Teorema: $\det(AB) = \det A \det B$.

Dimostrazione: siano A, B matrici $n \times n$. Se $C = AB$ si ha per definizione di prodotto righe per colonne:

$$C^k = B_{1k} A^1 + \cdots + B_{nk} A^n \tag{11.18}$$

da cui segue

$$\begin{aligned} \det(AB) &= D(C^1, ..., C^n) = \\ &= D(B_{11} A^1 + \cdots + B_{n1} A^n, ..., B_{1n} A^1 + \cdots + B_{nn} A^n) \\ &= \sum_\sigma B_{\sigma(1),1} \cdots B_{\sigma(n),n} D(A^{\sigma(1)}, ..., A^{\sigma(n)}) \\ &= \sum_\sigma sgn(\sigma) B_{\sigma(1),1} \cdots B_{\sigma(n),n} D(A^1, ..., A^n) \\ &= \det B \det A \end{aligned} \tag{11.19}$$

□

Esercizio: provare che $\det A^{-1} = (\det A)^{-1}$.

Teorema: il determinante di una matrice è uguale al determinante della matrice trasposta, i.e. $\det A = \det A^T$.

Dimostrazione:

$$\begin{aligned}\det A &= \sum_\sigma \mathrm{sgn}(\sigma) A_{\sigma(1),1} \cdots A_{\sigma(n),n} \\ &= \sum_\sigma \mathrm{sgn}(\sigma^{-1}) A_{1,\sigma^{-1}(1)} \cdots A_{n,\sigma^{-1}(n)} \\ &= \sum_\sigma \mathrm{sgn}(\sigma) A_{1,\sigma(1)} \cdots A_{n,\sigma(n)} \\ &= \sum_\sigma \mathrm{sgn}(\sigma) A^T_{\sigma(1),1} \cdots A^T_{\sigma(n),n} \\ &= \det A^T \end{aligned} \tag{11.20}$$

dove si è usato $\mathrm{sgn}(\sigma)$=$\mathrm{sgn}(\sigma^{-1})$ e l' uguaglianza dei prodotti $A_{\sigma(1),1} \cdots A_{\sigma(n),n}$ e $A_{1,\sigma^{-1}(1)} \cdots A_{n,\sigma^{-1}(n)}$. Inoltre la somma sulle permutazioni inverse coincide con la somma sulle permutazioni (l' insieme delle permutazioni comprende anche le permutazioni inverse).

Nota: dalla proprietà $\det(AB) = \det A \det B$ segue che il determinante di una matrice non cambia sotto trasformazione di similitudine $A \to SAS^{-1}$. Infatti $\det(SAS^{-1}) = \det S \det A \det S^{-1} = \det S \det A (\det S)^{-1} = \det A$. Si può quindi parlare di *determinante di un' applicazione lineare*, senza riferirsi a una base, dato che le sue rappresentazioni matriciali su basi diverse hanno tutte lo stesso determinante.

11.6 Matrice inversa

Sia A una matrice $n \times n$ con $\det A \neq 0$. Allora esiste l' inverso A^{-1} dato da

$$(A^{-1})_{ij} = \frac{D(A^1, ..., E^j, ..., A^n)}{\det A} \tag{11.21}$$

dove in $D(A^1, ..., E^j, ..., A^n)$ il vettore colonna E^j sostituisce la colonna i-esima della matrice A.

Dimostrazione: sia X una matrice incognita tale che $AX = I$. Per definizione si ha allora

$$E^j = x_{1j} A^1 + \cdots + x_{nj} A^n \tag{11.22}$$

Questo è un sistema di equazioni lineari, di cui esiste una sola soluzione data dalla regola di Cramer, e coincide con l' espressione (11.21). Per provare che vale anche $XA = I$, si nota che $\det A^T \neq 0$, e si può allora trovare con la procedura di sopra una matrice Y tale che $A^T Y = I$. Prendendo le trasposte di ambo i membri si ha $Y^T A = I$ e quindi $I = Y^T AXA = XA$ $\square$.

Se si espande il determinante al numeratore della formula di inversione (11.21) secondo la colonna i-esima, un solo termine è diverso da zero, e si ottiene il numer-

atore come determinante della sottomatrice $\widetilde{A}_{ji}$:

$$\boxed{(A^{-1})_{ij} = \frac{(-1)^{i+j} \det \widetilde{A}_{ji}}{\det A}} \tag{11.23}$$

Notare l' inversione degli indici ij.

11.7 Rango di una matrice e sottodeterminanti

Sia A una matrice $n \times n$. Abbiamo visto che le sue colonne sono vettori linearmente indipendenti se e solo se $\det A \neq 0$. Il determinante fornisce quindi uno strumento per studiare l' indipendenza lineare di un insieme di vettori.

Se $\det A = 0$, quindi rango$A < n$, ci possiamo chiedere come determinare il rango di A. Per questo basta calcolare il determinante di tutte le sottomatrici $(n-1) \times (n-1)$ di A. Se una di queste ha determinante non nullo, il rango di A è $n-1$, altrimenti si procede a calcolare il determinante delle sottomatrici $(n-2) \times (n-2)$ e così via.

Teorema: Il rango di A è la dimensione massima della sottomatrice con determinante non nullo. Questo rimane vero anche per una matrice $m \times n$ con $m \neq n$.

Illustriamo il Teorema su un semplice esempio, da cui si può trarre la dimostrazione nel caso generale.

Esempio: sia data la matrice

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & -1 \\ 4 & 3 & 1 \end{pmatrix} \tag{11.24}$$

Si ha $\det A = 0$ (la terza riga è somma delle prime due) , e quindi rango$A < 3$. Il determinante della sottomatrice 2×2 dell' angolo superiore sinistro di A ha determinante non nullo. Dal Teorema si ha che rango$A = 2$.

Verifichiamo che effettivamente A ha due righe linearmente indipendenti, e quindi che rango$A = 2$. Per esempio le due prime righe formano la matrice B:

$$B = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & -1 \end{pmatrix} \tag{11.25}$$

Sono linearmente indipendenti ? Le prime due colonne sono linearmente indipendenti, infatti formano una matrice 2×2 il cui determinante è diverso da 0. Allora il rango della matrice B è 2, ed è anche il numero massimo di righe linearmente indipendenti (vedi Sez. 10.2). Allora le due prime righe di A sono linearmente indipendenti, e così il rango di A è 2. □

12 Operatori hermitiani, unitari, normali. Autovalori e autovettori

12.1 Operatore aggiunto

• Dato un operatore lineare $A : V \to V$, dove lo spazio vettoriale V sia definito sul campo dei numeri complessi $\mathbb{C}$, si definisce il suo **aggiunto** $A^\dagger$ come segue:

$$\langle v, Aw\rangle \equiv \langle A^\dagger v, w\rangle \quad \forall v, w, \in V \tag{12.1}$$

Su una base ortonormale la sua matrice rappresentativa soddisfa:

$$A^\dagger_{ij} = A^*_{ji} \tag{12.2}$$

ed è quindi la **trasposta coniugata** della matrice che rappresenta A sulla stessa base. Infatti

$$A_{ij} = \langle u_i, Au_j\rangle = \langle A^\dagger u_i, u_j\rangle = \langle u_j, A^\dagger u_i\rangle^* = (A^\dagger_{ji})^* \tag{12.3}$$

usando la definizione di aggiunto, e la proprietà $\langle v, w\rangle = \langle w, v\rangle^*$ del prodotto scalare in campo complesso. Prendendo il complesso coniugato di ambo i membri si arriva all' asserto.

Osservazione 1: dalla definizione di operatore aggiunto segue che $(zA)^\dagger = z^* A^\dagger$, con $z \in \mathbb{C}$. Per esempio $(iA)^\dagger = -iA^\dagger$.

Osservazione 2: $(A^\dagger)^\dagger = A$, cioè l' aggiunto dell' aggiunto di A coincide con A.

Esercizio: dimostrare che l' aggiunto di un prodotto è uguale al prodotto degli aggiunti in ordine inverso:

$$(AB)^\dagger = B^\dagger A^\dagger \tag{12.4}$$

Nota: se lo spazio vettoriale V è definito sul campo dei numeri reali $\mathbb{R}$, l' aggiunto di A è rappresentato dalla trasposta della matrice che rappresenta A (la coniugazione non ha effetto su numeri reali): $A^\dagger = A^T$.

12.2 Operatori hermitiani

Gli operatori hermitiani sono definiti da

$$A^\dagger = A \tag{12.5}$$

In questo caso la matrice rappresentativa di A (chiamata anch'essa matrice hermitiana) coincide con la sua trasposta complessa coniugata, cf. (12.2). Dalla definizione di operatore aggiunto e dalla proprietà di $*$-commutazione del prodotto scalare, segue che un operatore A è hermitiano se e solo se

$$\langle v, Aw\rangle = \langle w, Av\rangle^* \qquad \forall v, w \in V \tag{12.6}$$

Gli operatori *antihermitiani* sono definiti da $A^\dagger = -A$. Se A è hermitiano, iA è antihermitiano e viceversa.

Nota : se A e B sono hermitiani, il loro commutatore $[A, B]$ è antihermitiano.

12.3 Operatori unitari

Gli operatori unitari sono definiti da

$$A^\dagger = A^{-1} \tag{12.7}$$

o equivalentemente $A^\dagger A = I = AA^\dagger$. Gli operatori unitari hanno l' importante proprietà di *conservare i prodotti scalari*: se A è un operatore unitario si ha

$$\langle Av, Aw\rangle = \langle v, w\rangle \quad \forall v, w \in V \tag{12.8}$$

come si dimostra immediatamente dalla definizione (12.7).

Osservazione: due basi ortonormali diverse $\{u_i\}$ e $\{u'_i\}$ sono collegate da una trasformazione S, cf. eq. (9.29), che deve essere *unitaria*, così che $\langle u_i, u_j\rangle = \langle u'_i, u'_j\rangle = \delta_{ij}$.

Esercizio: dimostrare che il prodotto di due operatori unitari è un operatore unitario.

Gli operatori unitari, in uno spazio vettoriale di dimensione n sul campo dei numeri complessi, formano un gruppo rispetto alla composizione, denotato $U(n)$. Se lo spazio vettoriale è definito sui numeri reali, la condizione di unitarietà diventa

$$A^T = A^{-1} \tag{12.9}$$

o equivalentemente $A^T A = I = AA^T$. L' operatore A in tal caso si dice **ortogonale**. Gli operatori ortogonali in uno spazio vettoriale reale di dimensione n formano un gruppo, denotato $O(n)$.

12.4 Autovalori e autovettori

Un vettore v è un **autovettore** di un operatore A, corrispondente all' autovalore λ, se soddisfa all' equazione (*equazione agli autovalori per l' operatore A*):

$$Av = \lambda v \tag{12.10}$$

Si esclude il caso banale $v = 0$. Gli autovettori di A vengono trasformati da A in vettori ad essi proporzionali, e la costante di proporzionalità prende il nome di **autovalore**. A volte si usa indicare l' autovettore corrispondente a un autovalore λ con una notazione che richiami l' autovalore, per esempio v_λ.

12.5 Equazione caratteristica

Il problema di trovare tutti gli autovalori e autovettori di un operatore è detto *problema spettrale* [6] . In genere è un problema difficile. Gli autovalori si trovano risolvendo per λ *l' equazione caratteristica*

$$\boxed{\det(A - \lambda I) = 0} \tag{12.11}$$

Dimostrazione: dalla (12.10) si ha $(A - \lambda I)v = 0$ con $v \neq 0$. Se esistesse l' inverso dell' operatore $A - \lambda I$ si potrebbe applicarlo all' equazione di sopra, ottenendo $(A - \lambda I)^{-1}(A - \lambda I)v = v = 0$, contrariamente all' ipotesi $v \neq 0$. Quindi $A - \lambda I$ non deve essere invertibile $\Rightarrow \det(A - \lambda I) = 0$. L' espressione $\det(A - \lambda I)$ è un polinomio in λ, di grado n (dimensione dello spazio vettoriale), e ha quindi n radici in $\mathbb{C}$. E' chiamato *polinomio caratteristico* della matrice A,

Una volta trovate le radici λ_i, si sostituiscono nell' equazione $Av = \lambda_i v$. Per ogni autovalore λ_i, questa diventa un sistema lineare per le componenti dell' autovettore incognito v corrispondente, di facile risoluzione. La parte difficile del procedimento è la prima, cioè trovare gli autovalori. Per indicare che v è l' autovettore corrispondente all' autovalore λ_i, possiamo indicarlo con v_i.

E' evidente che se v è autovettore con autovalore λ, anche av con $a \in K$ è autovettore con lo stesso autovalore, e quindi gli autovettori possono sempre essere normalizzati dividendoli per la loro norma. A un particolare autovalore λ_i possono corrispondere più autovettori linearmente indipendenti. Il numero g_i di questi autovettori si dice *degenerazione* dell' autovalore λ_i, e gli autovettori vengono denotati con un ulteriore indice che li distingua:

$$v_i^{(\alpha)}, \quad \alpha = 1, ...g_i \tag{12.12}$$

Questi autovettori, tutti con autovalore λ, generano uno spazio vettoriale, chiamato **autosottospazio** di A corrispondente all' autovalore λ_i. Ogni vettore di questo sottospazio (cioè ogni combinazione lineare dei $v_i^{(\alpha)}$) è sempre autovettore di A con autovalore λ_i

12.6 Diagonalizzazione di un operatore normale

Si definisce operatore **normale** un operatore lineare A che commuta col suo aggiunto, $[A, A^\dagger] = 0$. Si ha allora l' importante teorema:

Teorema sugli operatori normali: se $A : V \to V$ è un operatore normale, A ammette n autovettori ortonormali v_i , con $n =$ dimensione dello spazio vettoriale V. Quindi questi autovettori formano una base ortonormale $\{v_i\}$ di V. Inoltre la degenerazione di λ è data dalla *molteplicità* della radice λ del polinomio caratteristico $det(A - \lambda I)$.

[6] e l' insieme degli autovalori di A è detto *spettro* di A.

Se si rappresenta l' operatore A sulla base dei suoi autovettori, si ottiene una matrice diagonale, con elementi della diagonale uguali agli autovalori λ_i :

$$A_{ij} = \langle v_i, Av_j \rangle = \langle v_i, \lambda_j v_j \rangle = \lambda_j \langle v_i, v_j \rangle = \lambda_j \delta_{ij} \tag{12.13}$$

dove si è usata l' ortonormalità della base di autovettori v_i. Una matrice A corrispondente ad un operatore normale si chiama *matrice normale* e può quindi essere *diagonalizzata*, nel senso che si può sempre trovare una matrice S di cambiamento di base, che collega la base di partenza alla nuova base formata dagli autovettori della matrice, tale che $A' = SAS^{-1}$ sia diagonale, cf. (9.29).

Gli operatori hermitiani e gli operatori unitari sono operatori normali, com'è immediato verificare, e quindi sono diagonalizzabili.

Teorema: gli autovalori di un operatore hermitiano A sono reali.

Dimostrazione: immediata se si considera la matrice rappresentativa di A sulla base dei suoi autovettori: è una matrice diagonale, con elementi sulla diagonale che soddisfano alla condizione di hermiticità $A_{ii} = (A_{ii})^*$ (la trasposizione non ha effetto sugli elementi diagonali). Ma gli elementi sulla diagonale sono gli autovalori di A, e sono quindi reali. □

Teorema: gli autovalori di un operatore unitario A sono numeri complessi di modulo 1.

Dimostrazione: con lo stesso metodo usato nella dimostrazione del Teorema precedente, si considera la matrice che rappresenta l' operatore unitario A su una base dei suoi autovettori. La condizione di unitarietà $A^\dagger A = I$ sugli elementi diagonali diventa $A^*_{ii} A_{ii} = 1$ e cioè $|A_{ii}|^2 = 1$. □

Esempio: alla matrice

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} \tag{12.14}$$

corrisponde il polinomio caratteristico $(\lambda-1)^2\lambda$ le cui radici ($\lambda = 2$ con molteplicità 2, e $\lambda = 0$) individuano gli autovalori di A. I corrispondenti autovettori $v_\lambda = (x, y, z)$ si trovano risolvendo il sistema lineare

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{12.15}$$

con $\lambda = 0$ e $\lambda = 2$. Dal teorema sugli operatori normali sappiamo che ci devono essere due autovettori $v_{\lambda=2}$, $v'_{\lambda=2}$ linearmente indipendenti corrispondenti all' autovalore $\lambda = 2$ (di degenerazione 2), e un autovettore $v_{\lambda=0}$ corrispondente a $\lambda = 0$

(autovalore non degenere). Si trova:

$$v_{\lambda=0} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad v_{\lambda=2} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad v'_{\lambda=2} = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \tag{12.16}$$

e si può verificare che formano una base ortonormale per $\mathbb{R}^3$.

Esercizio 1: trovare autovalori e autovettori della matrice

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{12.17}$$

Verificare che A è unitaria, e che rappresenta una rotazione di un angolo θ in $\mathbb{R}^2$. Determinare anche gli autovalori complessi.

Esercizio 2: trovare autovalori e autovettori della matrice

$$A = \begin{pmatrix} 4 & 1 \\ -1 & 2 \end{pmatrix} \tag{12.18}$$

Verificare che A non è normale.

References

[1] A. Facchini, "Algebra e matematica discreta", Zanichelli 2018.

[2] S. Lang, "Algebra lineare", Boringhieri 1970.