Appunti di Algebra Lineare

(già “Appunti di Geometria e Algebra”)

Carlo Petronio

Seconda versione preliminare – autunno 2003

Indice

Capitolo 1

Motivazioni

Lo scopo fondamentale di questo corso è l'introduzione di tecniche di manipolazione di tipo *algebrico* per oggetti di natura non algebrica (come sarebbero, ad esempio, numeri, polinomi, espressioni), bensì *geometrica* (come punti, rette, piani). Svilupperemo un linguaggio astratto e dei metodi che si prestano a trattare in modo unificato (e a risolvere!) problemi apparentemente molto diversi tra loro. Questi problemi hanno tutti importanti motivazioni nel "mondo reale" (ad esempio in questioni provenienti dall'ingegneria), ma noi non avremo tempo di insistere su di esse: lasciamo ai corsi successivi l'illustrazione delle applicazioni della teoria qui descritta.

In questo capitolo anticipiamo alcuni dei temi di cui ci occuperemo.

1.1 Forze applicate

Nella fisica del punto materiale rappresentiamo una forza F applicata a un punto p come una freccia (*vettore*) che parte da p (si veda Fig. 1.1). La freccia indica direzione e verso di F, e la sua lunghezza è proporzionale all'intensità di F. Se due forze sono applicate allo stesso p, l'effetto sul moto di p è quello di una singola forza, detta *risultante* e costruita con la regola del parallelogrammo, come illustrato in Fig. 1.2. Valgono le proprietà:

- $\mathrm{ris}(F_1, F_2) = \mathrm{ris}(F_2, F_1)$;
- $\mathrm{ris}\Big(F_1, \mathrm{ris}(F_2, F_3)\Big) = \mathrm{ris}\Big(\mathrm{ris}(F_1, F_2), F_3\Big)$.

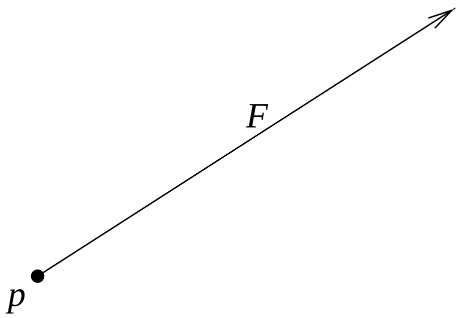

Figura 1.1: Una forza F applicata a un punto p

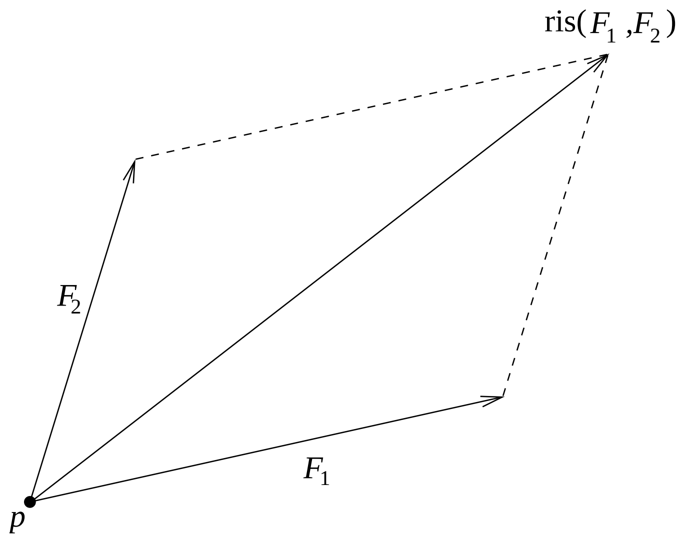

Figura 1.2: Risultante di due forze F_1 e F_2

(La prima è facile; verificare per esercizio la seconda). Inoltre se chiamiamo 0 la forza di intensità nulla applicata a p (della quale non contano direzione e verso, naturalmente) abbiamo anche:

- $\mathrm{ris}(0, F) = F$;
- $\mathrm{ris}(F, \widehat{F}) = 0$ se $\widehat{F}$ è la forza che ha direzione ed intensità uguali a quelle di F, ma verso opposto.

Esaminando le quattro proprietà elencate ci si accorge che sono perfettamente analoghe a quelle dell'operazione "+" (addizione) tra numeri:

- $x + y = y + x$;
- $x + (y + z) = (x + y) + z$;
- $0 + x = x$;
- $x + (-x) = 0$.

Facciamo allora la scommessa di indicare $\mathrm{ris}(F_1, F_2)$ con $F_1 + F_2$, sperando che l'analogia con l'operazione "+" tra numeri dia frutti. Bisogna fare attenzione: scrivendo $F_1 + F_2$ stiamo dando un *nuovo significato* al simbolo "+", cioè stiamo definendo una *nuova operazione*, poiché essa si applica ad oggetti che non sono più numeri (sono forze). Lo stiamo facendo sulla base dell'analogia delle proprietà dell'operazione "risultante" tra forze con quelle dell'operazione "addizione" tra numeri.

Ci sono altre operazioni che possiamo fare con le forze. Ad esempio, data una forza F possiamo raddoppiarne, triplicarne o dimezzarne l'intensità, senza modificare direzione e verso, oppure possiamo cambiarne il verso. È naturale interpretare questo come la moltiplicazione della forza per un fattore 2, 3, 1/2 e -1, rispettivamente. Più in generale è chiaro che senso dare alla forza $\lambda \cdot F$ se λ è un numero. Osserviamo che, come sopra con il "+", abbiamo introdotto una *nuova operazione* "·" che ha come "input" una coppia di oggetti del tipo numero–forza ed ha come "output" una forza. Naturalmente l'uso dello stesso simbolo impiegato per la moltiplicazione tra numeri ha senso se sono analoghe le proprietà algebriche. E di fatto si possono facilmente verificare le identità seguenti:

- $(\lambda_1 \cdot \lambda_2) \cdot F = \lambda_1 \cdot (\lambda_2 \cdot F)$

(si osservi che dei quattro "$\cdot$" che compaiono in questa formula, il primo rappresenta la moltiplicazione tra numeri, mentre gli altri tre rappresentano la nuova operazione introdotta);

- $(\lambda_1 + \lambda_2) \cdot F = \lambda_1 \cdot F + \lambda_2 \cdot F$

(in questo caso il primo "+" è quello tra numeri, mentre l'altro "+" e i tre "$\cdot$" hanno il nuovo significato);

- $\lambda \cdot (F_1 + F_2) = \lambda \cdot F_1 + \lambda \cdot F_2$;

- $\lambda \cdot 0 = 0 \cdot F = 0$

(nell'ultima formula il primo ed il terzo "0" rappresentano la forza di intensità nulla, mentre il secondo è il numero zero). Sulla base di queste proprietà sarà lecito manipolare espressioni contenenti le nuove operazioni introdotte così come si sarebbe fatto per le corrispondenti espressioni algebriche.

1.2 Trasformazioni piane

1.2.1 Traslazioni

Una classe di trasformazioni del piano cartesiano che molti dovrebbero avere incontrato è quella delle traslazioni. Una traslazione T è determinata da un vettore v avente certe componenti (x_0, y_0), come in Fig. 1.3-sinistra. Essa agisce su un generico punto p come indicato in Fig. 1.3-centro. Esaminiamo ora come si esprimano le coordinate (x', y') del punto trasformato $T(p)$ in funzione delle coordinate (x, y) del punto iniziale p. La relazione, che si deduce facilmente da Fig. 1.3-destra, è la seguente:

$$(\spadesuit) \qquad \begin{cases} x' &= x + x_0 \\ y' &= y + y_0. \end{cases}$$

Interpretiamo ora le coordinate di un punto o le componenti di un vettore, che sono una coppia di numeri, come un oggetto unico, che scriviamo come colonna (questa scelta si rivelerà molto utile, come vedremo già in questo primo capitolo) e che indichiamo con il simbolo stesso che denota il punto o il vettore:

$$p' = \begin{pmatrix} x' \\ y' \end{pmatrix}, \qquad p = \begin{pmatrix} x \\ y \end{pmatrix}, \qquad v = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}.$$

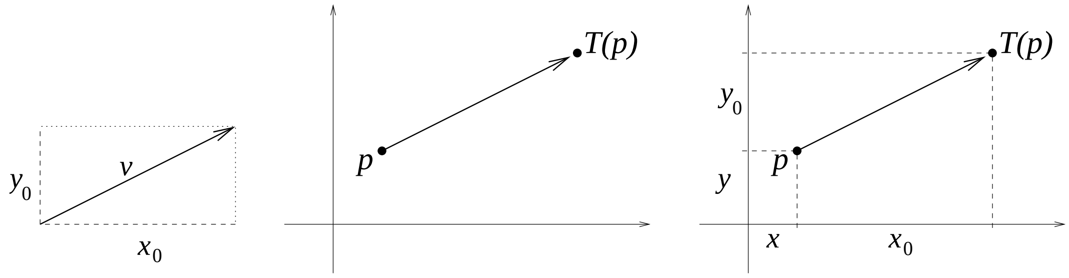

Figura 1.3: Un vettore nel piano, la traslazione ad esso associata, e la corrispondente trasformazione delle coordinate

È allora naturale scrivere la relazione (♠) semplicemente come:

$$p' = p + v.$$

In altre parole stiamo definendo ancora un nuovo significato per il simbolo "+". Ora abbiamo come "input" della nuova operazione due colonne di numeri $\begin{pmatrix} x \\ y \end{pmatrix}$ e $\begin{pmatrix} z \\ w \end{pmatrix}$, e come "output" una nuova colonna $\begin{pmatrix} x+z \\ y+w \end{pmatrix}$. Come sopra, è sensato denotare con "+" la nuova operazione poiché valgono le seguenti proprietà algebriche analoghe a quelle dell'addizione tra numeri:

- $0 + p = p$

dove 0 indica la colonna $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$;

- $p + (-p) = 0$

dove $-p$ indica la colonna $\begin{pmatrix} -x \\ -y \end{pmatrix}$ se $p = \begin{pmatrix} x \\ y \end{pmatrix}$;

- $p_1 + p_2 = p_2 + p_1$;

- $p_1 + (p_2 + p_3) = (p_1 + p_2) + p_3$.

In realtà possiamo ricondurre questa nuova operazione + a quella introdotta sopra tra forze. Se infatti interpretiamo p come la forza applicata all'origine delle coordinate ed avente "testa" nel punto di coordinate p, abbiamo una completa coerenza, come illustrato in Fig. 1.4.

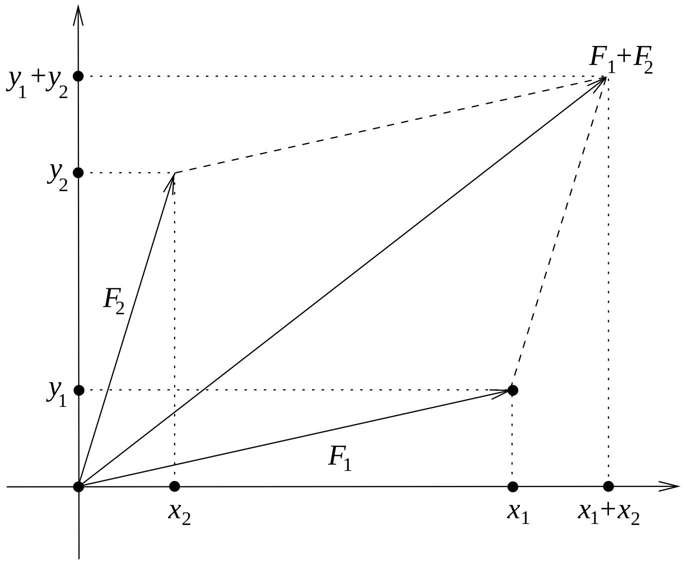

Figura 1.4: Risultante tra forze espressa in coordinate

Per concludere con le traslazioni osserviamo anche che, interpretando sia i punti del piano cartesiano che i vettori come colonne di due numeri, abbiamo di fatto abbandonato la distinzione tra questi tipi di oggetto. La coerenza di questo fatto si spiega con la costruzione appena vista: un punto p determina il vettore che ha "coda" nell'origine degli assi e "testa" in p. Viceversa un vettore v determina un punto se si trasporta la "coda" di v nell'origine e se ne considera la "testa".

1.2.2 Omotetie

Consideriamo ora un'altra operazione elementare sui punti del piano cartesiano, vale a dire l'omotetia di ragione $\lambda \neq 0$ centrata nell'origine O. Geometricamente tale trasformazione mantiene ogni punto p sulla retta che contiene O e p, ma modifica la distanza tra O e p di un fattore $|\lambda|$, riflettendo inoltre rispetto all'origine il punto risultante se $\lambda < 0$. Se $\begin{pmatrix} x \\ y \end{pmatrix}$ sono le coordinate di p, è facile vedere che le coordinate del suo trasformato sono $\begin{pmatrix} \lambda \cdot x \\ \lambda \cdot y \end{pmatrix}$. È

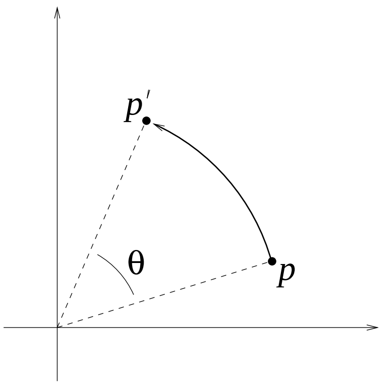

Figura 1.5: La rotazione di angolo θ

ora naturale denotare tale colonna di coordinate come $\lambda \cdot \begin{pmatrix} x \\ y \end{pmatrix}$, introducendo dunque una nuova operazione "$\cdot$" che ha come "input" un numero e una colonna con due coordinate e come "output" un'altra colonna con due coordinate. Come al solito questa scelta è giustificata dalle proprietà algebriche dell'operazione. È anzi facile vedere che essa corrisponde esattamente alla moltiplicazione tra un numero ed una forza, introdotta sopra, interpretando un punto p come il vettore con "coda" nell'origine e "testa" in p.

1.2.3 Rotazioni

Consideriamo ora una nuova classe di trasformazioni del piano cartesiano, quella delle rotazioni intorno all'origine degli assi. Una rotazione è determinata da un angolo θ, ed agisce come suggerito in Fig. 1.5.

Determiniamo come si ricavino le coordinate $\begin{pmatrix} x' \\ y' \end{pmatrix}$ del punto ruotato p' in funzione delle coordinate $\begin{pmatrix} x \\ y \end{pmatrix}$ del punto iniziale p. Si tratta di un esercizio di trigonometria, svolto in Fig. 1.6: sono qui mostrati il triangolo avente vertici in O, in p e nella proiezione di p sull'asse delle ascisse, il ruotato di tale triangolo, e le lunghezze di varî segmenti, dalle quali la conclusione segue facilmente. Si trovano dunque le relazioni seguenti:

$$(\heartsuit) \qquad \begin{cases} x' = \cos\theta \cdot x - \sin\theta \cdot y \\ y' = \sin\theta \cdot x + \cos\theta \cdot y. \end{cases}$$

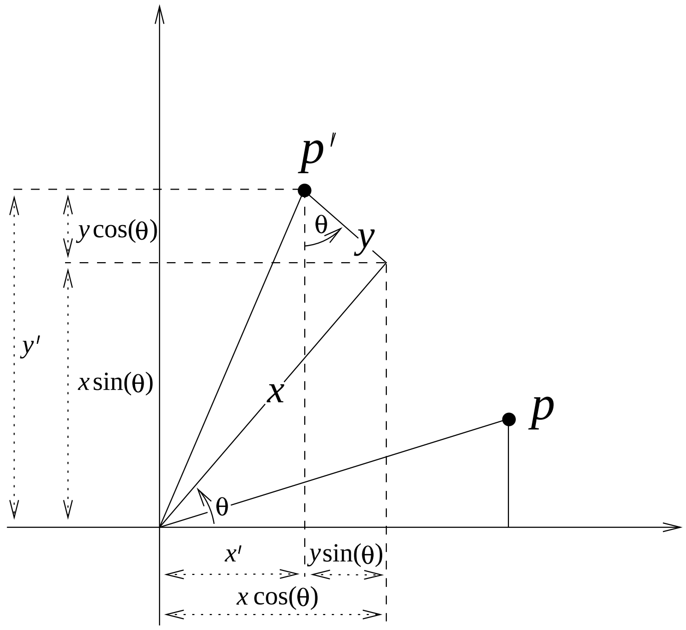

Figura 1.6: Coordinate di un punto ruotato di angolo θ

Avendo interpretato le coordinate come un unico oggetto $\begin{pmatrix} x \\ y \end{pmatrix}$, è naturale tentare di riscrivere le equazioni ($\heartsuit$) come un'unica equazione

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = R_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

dove tanto l'oggetto R_θ che il significato di "$\cdot$" sono da inventare. Per R_θ inventiamo la tabella

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

che rispecchia le posizioni dei coefficienti $\cos\theta$ e $\pm\sin\theta$ nelle equazioni ($\heartsuit$). A questo punto inventiamo la regola di moltiplicazione tra una tabella con due righe e due colonne e una colonna di altezza due in modo che risulti quello che desideriamo:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \cdot x + b \cdot y \\ c \cdot x + d \cdot y \end{pmatrix}.$$

Ancora una volta, ha senso usare il simbolo "$\cdot$" per l'operazione introdotta in virtù delle sue proprietà algebriche, che vedremo oltre.

Illustriamo ora un primo elemento di utilità delle nuove operazioni (che altrimenti potrebbero sembrare pure invenzioni formali, prive di scopo). Ricordiamo che la tabella R_θ l'abbiamo associata alla rotazione di angolo θ, nel senso che la rotazione di un punto di angolo θ si esegue moltiplicando (a sinistra) le coordinate del punto per la R_θ. Se ora consideriamo due angoli θ e φ, possiamo considerare due modi di "moltiplicare" tra loro le corrispondenti R_θ e R_φ. Da un lato, geometricamente, abbiamo le rotazioni di angoli θ e φ, che possiamo comporre, cioè eseguire prima una e poi l'altra, ottenendo la rotazione di angolo $\theta + \varphi$. Dall'altro lato, possiamo facilmente inventare una ragionevole regola di moltiplicazione tra tabelle con due righe e due colonne. Date $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\begin{pmatrix} x & z \\ y & w \end{pmatrix}$, interpretiamo la seconda tabella come la scrittura, una di fianco all'altra, delle due colonne $\begin{pmatrix} x \\ y \end{pmatrix}$ e $\begin{pmatrix} z \\ w \end{pmatrix}$, e decidiamo che moltiplicando a sinistra per $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ si ottengono, una di fianco all'altra, le due colonne $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$ e $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} z \\ w \end{pmatrix}$, ovvero:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & z \\ y & w \end{pmatrix} = \begin{pmatrix} a \cdot x + b \cdot y & a \cdot z + b \cdot w \\ c \cdot x + d \cdot y & c \cdot z + d \cdot w \end{pmatrix}.$$

Con questa regola abbiamo allora:

$$\begin{aligned} R_\theta \cdot R_\varphi &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta \cdot \cos\varphi - \sin\theta \cdot \sin\varphi & -\cos\theta \cdot \sin\varphi - \sin\theta \cdot \cos\varphi \\ \cos\theta \cdot \sin\varphi + \sin\theta \cdot \cos\varphi & \cos\theta \cdot \cos\varphi - \sin\theta \cdot \sin\varphi \end{pmatrix} \end{aligned}$$

mentre avevamo osservato che la composizione di R_θ ed R_φ conduceva a:

$$R_{\theta+\varphi} = \begin{pmatrix} \cos(\theta+\varphi) & -\sin(\theta+\varphi) \\ \sin(\theta+\varphi) & \cos(\theta+\varphi) \end{pmatrix}.$$

Le regole trigonometriche di calcolo per $\cos(\theta+\varphi)$ e $\sin(\theta+\varphi)$ comportano ora che $R_\theta \cdot R_\varphi = R_{\theta+\varphi}$. Dunque abbiamo il fatto notevole che la regola di moltiplicazione algebrica tra tabelle, inventata senza particolare motivazione geometrica, in realtà traduce esattamente la nozione geometrica di composizione delle due rotazioni. Alternativamente, dando per assodata la corrispondenza tra moltiplicazione e composizione, la relazione $R_\theta \cdot R_\varphi = R_{\theta+\varphi}$ ci consente di ricavare in modo facile le regole trigonometriche di calcolo per $\cos(\theta+\varphi)$ e $\sin(\theta+\varphi)$: basta ricordare come si associa R_θ a θ e la moltiplicazione tra tabelle.

Concludiamo osservando che, quando abbiamo parlato della composizione delle due rotazioni di angoli θ e φ, non abbiamo avuto bisogno di specificare quale delle due trasformazioni sia eseguita prima dell'altra, poiché in questo caso l'una scelta o l'altra conducono allo stesso risultato. Si osservi che ciò non è affatto vero per funzioni qualsiasi: ad esempio, se $f(t) = t^2$ e $g(t) = 2t$, si ha $(f \circ g)(t) = 4t^2$ e $(g \circ f)(t) = 2t^2$.

1.3 Intersezione tra rette

Nel piano cartesiano con coordinate x e y, una retta è il luogo definito da una equazione del tipo $ax + by = k$ con a, b, k numeri fissati, purché a e b non siano entrambi nulli (altrimenti viene tutto il piano per $k = 0$ e l'insieme vuoto $\emptyset$ per $c \neq k$). Date due rette di equazioni $ax+by=k$ e $cx+dy=h$, l'operazione geometrica di ricerca della loro intersezione (se esiste) corrisponde algebricamente alla ricerca delle soluzioni del sistema:

$$\begin{cases} ax+by &= k \\ cx+dy &= h. \end{cases}$$

Usando le grafie e le operazioni introdotte in precedenza possiamo ora scrivere questo sistema come una singola equazione

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} k \\ h \end{pmatrix}.$$

Naturalmente il solo fatto di avere scritto le equazioni in maniera più sintetica non aiuta di per sé a risolverle. Vedremo però che al linguaggio introdotto si accompagneranno strumenti molto efficienti per la soluzione di una equazione come quella appena scritta.

1.4 Numeri di Fibonacci

Menzioniamo ora un argomento che non pare a prima vista avere alcuna relazione con le nozioni di natura geometrica (vettori e coordinate) di cui ci si è occupati finora, ma che invece sarà possibile trattare con il linguaggio generale che ci avviamo ad introdurre.

Supponiamo di piantare oggi (all'inizio del mese numero 1) un alberello con un solo ramo, che per tutto il mese cresce senza gettare nuovi rami e poi si sviluppa secondo queste regole:

- nessun ramo muore mai;
- alla metà di ogni nuovo mese, tutti i rami che non siano "neonati" (ovvero che non siano spuntati il mese precedente) gettano un nuovo ramo.

Supponendo che ad ogni mese ogni ramo cresca verso l'alto della stessa altezza, l'aspetto dell'albero al settimo mese sarà quello in Fig. 1.7. Ci chiediamo ora quale sia il numero di rami f_n dell'albero all'inizio del mese n-esimo (tale f_n si chiama n-esimo numero di Fibonacci). Dalla Fig. 1.7 si desume che i

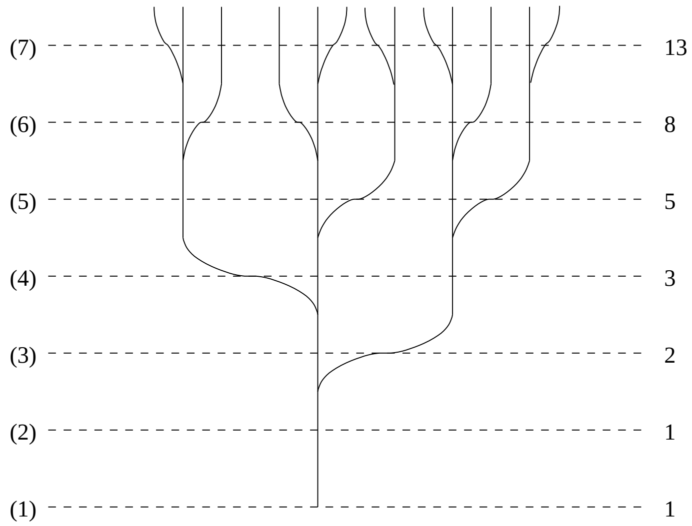

Figura 1.7: Un albero che cresce come la successione di Fibonacci

valori di f_n per $n = 1, \ldots, 7$ sono $1, 1, 2, 3, 5, 8, 13$. Mostriamo ora che vale la seguente formula:

$$(\diamondsuit) \qquad f_n = f_{n-1} + f_{n-2}, \qquad \text{per ogni } n \geqslant 3.$$

Infatti all'inizio del mese n sopravvivono tutti i rami che esistevano all'inizio del mese $n-1$, che sono nel numero di f_{n-1}, ed in più vi sono tutti i rami buttati alla metà del mese $n-1$ dai rami non "neonati", cioè da quelli che esistevano già all'inizio del mese $n-2$. Questi ultimi sono nel numero di f_{n-2}, onde la $(\diamondsuit)$.

La $(\diamondsuit)$ è una formula cosiddetta "ricorsiva", poiché consente di calcolare tutti i valori di f_n ripetendo ricorsivamente la stessa procedura a partire dai termini iniziali $f_1 = 1$ e $f_2 = 1$, ovvero:

$$\begin{array}{rcl} f_1 & = & 1, \\ f_2 & = & 1, \\ f_3 & = & f_2 + f_1 = 1 + 1 = 2, \\ f_4 & = & f_3 + f_2 = 2 + 1 = 3, \\ f_5 & = & f_4 + f_3 = 3 + 2 = 5 \\ & \vdots & . \end{array}$$

In qualsiasi linguaggio di programmazione è molto semplice implementare questa procedura ricorsiva, ma il programma ottenuto è molto dispendioso in termini di tempo, poiché il calcolo di ciascun f_n richiede il calcolo di tutti gli f_m con $m < n$. Esiste tuttavia un metodo alternativo e molto efficiente di calcolo per f_n, basato sulla seguente (sorprendente) identità:

$$(\clubsuit) \qquad f_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

(Già la sola verifica che il termine destro di questa relazione è intero per ogni n non è del tutto banale). Vedremo che la formula ($\clubsuit$) si può non solo dimostrare facilmente, ma anche "spiegare" perfettamente, con il linguaggio che introdurremo a partire dal Capitolo 3.

Capitolo 2

Preliminari algebrici e logici

In questo capitolo richiamiamo le proprietà algebriche delle operazioni sui principali insiemi numerici ed illustriamo, esemplificandole, due tecniche di dimostrazione.

2.1 Numeri

Questa sezione è dedicata gli insiemi dei numeri naturali, degli interi, dei razionali e dei reali.

2.1.1 Numeri naturali ed interi

Useremo (senza definirlo) l'insieme dei numeri *naturali* $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ ed il fatto che sui numeri naturali è definita una operazione di addizione "+" binaria ed interna (cioè che ha come "input" due naturali e come "output" un nuovo naturale), che soddisfa le seguenti proprietà:

1. $0 + n = n$ per ogni n;

3. $n + (m + k) = (n + m) + k$ per ogni n, m, k;

4. $n + m = m + n$ per ogni n, m.

Abbiamo intenzionalmente omesso il numero 2 elencando le proprietà, per una ragione che sarà subito chiara. Se consideriamo, dato $n \in \mathbb{N}$, l'equazione

$$n + x = 0,$$

osserviamo che essa non ha soluzioni $x \in \mathbb{N}$, ad eccezione che nel caso in cui n è 0, nella quale ipotesi si ha la soluzione $x = 0$. Per sopperire a questo inconveniente si estende l'insieme $\mathbb{N}$ dei numeri naturali a quello $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ dei numeri *interi*. Anche su questo insieme è definita una operazione binaria interna di somma, che estende quella su $\mathbb{N}$, e che gode, oltre che delle proprietà (1), (3) e (4) elencate sopra, anche della seguente:

2. Per ogni $n \in \mathbb{Z}$ esiste $(-n) \in \mathbb{Z}$ tale che $n + (-n) = 0$.

Un utile esercizio: usando solo le proprietà elencate, provare che per ogni n l'equazione $n + x = 0$ ha un'*unica* soluzione $x \in \mathbb{Z}$, indicata appunto con $(-n)$.

2.1.2 Numeri razionali e reali

Sull'insieme $\mathbb{Z}$ degli interi, oltre alla somma abbiamo una seconda operazione binaria interna, indicata con "$\cdot$" e detta prodotto, che soddisfa le seguenti proprietà:

5. $1 \cdot n = n$ per ogni n;

7. $n \cdot (m \cdot k) = (n \cdot m) \cdot k$ per ogni n, m, k;

8. $n \cdot m = m \cdot n$ per ogni n, m.

9. $n \cdot (m + k) = n \cdot m + n \cdot k$ per ogni n, m, k;

Di nuovo abbiamo intenzionalmente omesso la proprietà (6). La ragione è che, dato $n \in \mathbb{Z}$, l'equazione

$$n \cdot x = 1$$

non ha soluzioni x in $\mathbb{Z}$, a meno che n non sia $+1$ oppure -1, nel qual caso la soluzione è n. Si passa dunque dall'insieme dei numeri interi a quello $\mathbb{Q}$ dei numeri razionali, ovvero alle frazioni del tipo p/q con $p, q \in \mathbb{Z}$ e $q \neq 0$. In realtà, poiché sappiamo che i numeri razionali si possono scrivere come frazioni in più modi, formalmente si dovrebbe definire $\mathbb{Q}$ come l'insieme delle scritture del tipo p/q come sopra, dove però p/q è identificata a p'/q' quando $p \cdot q' = p' \cdot q$ (il che, naturalmente, corrisponde al fatto che p/q e p'/q' hanno "lo stesso valore"). Analogamente, identifichiamo la frazione $n/1$ all'intero n, deducendo che $\mathbb{Q}$ contiene $\mathbb{Z}$. Inoltre, le operazioni di somma e prodotto definite su $\mathbb{Z}$ si estendono a $\mathbb{Q}$, e soddisfano su $\mathbb{Q}$ le proprietà seguenti:

1. $0 + x = x$ per ogni x;
2. Per ogni x esiste $(-x)$ tale che $x + (-x) = 0$;
3. $x + (y + z) = (x + y) + z$ per ogni x, y, z;
4. $x + y = y + x$ per ogni x, y;
5. $1 \cdot x = x$ per ogni x;
6. Per ogni $x \neq 0$ esiste x^{-1} tale che $x \cdot x^{-1} = 1$;
7. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ per ogni x, y, z;
8. $x \cdot y = y \cdot x$ per ogni x, y;
9. $x \cdot (y + z) = x \cdot y + x \cdot z$ per ogni x, y, z.

Nella proprietà (6) è necessario ipotizzare $x \neq 0$ perché dalle altre proprietà è possibile dedurre che $0 \cdot y = 0$ per ogni y.

Estendiamo ora ulteriormente l'insieme $\mathbb{Q}$ dei razionali all'insieme, indicato con $\mathbb{R}$, dei numeri reali. La motivazione dell'estensione è questa volta di natura geometrico-analitica, piuttosto che algebrica come per i passaggi da $\mathbb{N}$ a $\mathbb{Z}$ e poi da $\mathbb{Z}$ a $\mathbb{Q}$. Per spiegarla, consideriamo una retta e fissiamo su questa retta due punti distinti che facciamo corrispondere ai numeri razionali 0 e 1. Possiamo allora estendere questa corrispondenza, associando ad ogni numero un punto. Ad esempio il numero $-3/2$ corrisponderà al punto che sta dalla parte opposta di 1 rispetto a 0 e che ha distanza da 0 una volta e mezza quella che 1 ha da 0. La funzione così definita da $\mathbb{Q}$ alla retta risulta allora iniettiva (cioè numeri diversi danno punti diversi). Essa non è però surgettiva, ovvero ci sono punti che non corrispondono ad alcun numero razionale. Un esempio è il punto x costruito nella Fig. 2.1, la cui distanza da 0 è uguale alla lunghezza della diagonale del quadrato unitario. Per il Teorema di Pitagora, se x corrispondesse ad un numero razionale esso dovrebbe soddisfare l'identità $x^2 = 2$, mentre è possibile vedere (lo faremo più avanti in questo capitolo) che l'equazione $x^2 = 2$ non ha soluzioni in $\mathbb{Q}$.

Avendo scoperto che $\mathbb{Q}$ rappresenta alcuni ma non tutti i punti della retta, definiamo $\mathbb{R}$ semplicemente come l'insieme dei punti della retta, ed usiamo (senza dimostrarlo), il fatto che le operazioni "+" e "·" definite su $\mathbb{Q}$ si estendono a $\mathbb{R}$ e continuano a soddisfare le proprietà (1)-(9) che abbiamo elencato sopra per $\mathbb{Q}$.

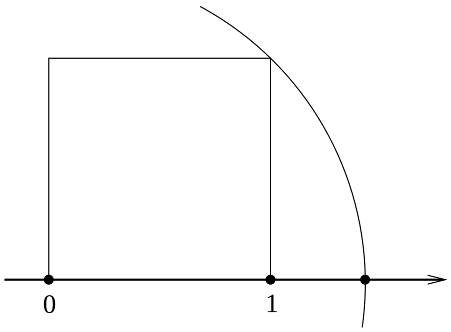

Figura 2.1: Un punto non razionale della retta

2.1.3 Campi e gruppi commutativi

Avendo incontrato due insiemi (cioè $\mathbb{Q}$ e $\mathbb{R}$) che possiedono due operazioni soddisfacenti lo stesso lungo elenco di proprietà, introduciamo ora un singolo termine, quello di *campo*, per indicare un insieme siffatto. Nel Capitolo 8 incontreremo un altro esempio di campo, quello $\mathbb{C}$ dei numeri complessi. Osservando inoltre che le proprietà (1)-(4) della definizione di campo riguardano la sola operazione "+", mentre le (5)-(8) riguardano solo "·" e sono formalmente pressoché analoghe alle (1)-(4), introduciamo ora un'altra nuova terminologia. Chiamiamo *gruppo commutativo* un insieme sul quale è definita una operazione (binaria ed interna) tale che esiste un elemento neutro, ogni elemento ammette un opposto, e valgono le proprietà associativa e commutativa. Notiamo che, per essere del tutto precisi, un gruppo commutativo non è il solo insieme, bensì la terna insieme–operazione–elemento neutro. Dalla discussione sugli insiemi numerici fin qui svolta segue allora che possediamo già i seguenti esempi di gruppo commutativo:

- $(\mathbb{Z}, +, 0)$;
- $(\mathbb{Q}, +, 0)$;
- $(\mathbb{R}, +, 0)$;
- $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$, mentre, è importante osservarlo, non è un gruppo commutativo l'insieme $(\mathbb{Q}, \cdot, 1)$, poiché l'elemento 0 non ammette "opposto rispetto alla moltiplicazione" (cioè, non ammette inverso); è questa l'u-

nica ma sostanziale differenza tra la proprietà (6) e la (2) tra quelle di campo;

- $(\mathbb{R} \setminus \{0\}, \cdot, 1)$.

2.2 Polinomi

Avremo spesso a che fare con i polinomi, ovvero con le scritture del tipo $a_0+a_1\cdot x+a_2\cdot x^2+\ldots+a_k\cdot x^k$, dove $k \in \mathbb{N}$, $a_0, \ldots, a_k \in \mathbb{R}$, e x è un simbolo che non appartiene a $\mathbb{R}$ (detto *indeterminata*). Sottolineiamo che un polinomio per noi è una espressione del tipo $a_0+a_1\cdot x+a_2\cdot x^2+\ldots+a_k\cdot x^k$, non la funzione polinomiale da $\mathbb{R}$ a $\mathbb{R}$ che eventualmente gli si può associare. Definiamo ora $\mathbb{R}[x]$ come l'insieme di tutti i polinomi, ovvero delle espressioni del tipo appena descritto, avendo però una piccola accortezza che ora illustriamo. Notiamo che formalmente l'espressione $1/2 - 7x^2$ non è del tipo descritto, mentre $1/2 + 0 \cdot x - 7x^2$ lo è. Inoltre, entrambe le espressioni $3/4 + 2x$ e $3/4+2x+0\cdot x^2$ sono del tipo descritto, e sono diverse. Tuttavia noi certamente vogliamo considerare $1/2-7x^2$ un polinomio, e vogliamo considerare $3/4+2x$ e $3/4 + 2x + 0 \cdot x^2$ uguali tra loro. Adottiamo quindi la convenzione che nella scrittura di un polinomio è possibile introdurre o cancellare a piacimento monomi del tipo $0 \cdot x^h$.

Ad un polinomio $p(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_k \cdot x^k$ che non sia il polinomio nullo si associa un intero $\deg(p(x))$, detto *grado*, definito come

$$\deg(p(x)) = \max\{h : \ a_h \neq 0\}.$$

Al polinomio nullo si può convenzionalmente assegnare il grado $-\infty$, oppure -1, oppure nessun grado.

Anche sull'insieme dei polinomi sono definite due operazioni naturali "+" e "·". Per descriverle in termini generali conviene introdurre una ulteriore convenzione. Osserviamo intanto che una espressione $a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_k \cdot x^k$ può essere descritta dalla sommatoria $\sum_{n=0}^{k} a_n \cdot x^n$. Inoltre, se $h \geqslant k$ e si pone $a_n = 0$ per $n = k+1, \ldots, h$, la stessa espressione è uguale a $\sum_{n=0}^{h} a_n \cdot x^n$. Poiché nell'ultima sommatoria il valore di h è arbitrariamente grande, è ragionevole ora convenire che un polinomio è una espressione del tipo $\sum\limits_{n=0}^{\infty} a_n \cdot x^n$, dove i coefficienti a_n sono tutti nulli ad eccezione che per un numero finito di indici n. Le formule per la somma ed il prodotto di polinomi sono allora date da:

$$\begin{aligned}
\left(\sum_{n=0}^{\infty} a_n \cdot x^n\right) + \left(\sum_{n=0}^{\infty} b_n \cdot x^n\right) &= \sum_{n=0}^{\infty}(a_n + b_n) \cdot x^n, \\
\left(\sum_{n=0}^{\infty} a_n \cdot x^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n \cdot x^n\right) &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right) \cdot x^n.
\end{aligned}$$

Si può verificare per esercizio che queste operazioni soddisfano le proprietà (1)-(5) e (7)-(9) della definizione di campo, ma non la (6).

2.3 Dimostrazioni

Illustriamo ed esemplifichiamo in questa sezione due tecniche dimostrative alle quali faremo spesso ricorso nel seguito.

2.3.1 Principio di induzione

Questo principio è utile quando si voglia dimostrare che una certa proposizione $\mathcal{P}(n)$, relativa ad un numero naturale n, vale per ogni $n \in \mathbb{N}$. A questo fine è sufficiente dimostrare che:

- (passo base) vale la $\mathcal{P}(0)$, ovvero la proposizione $\mathcal{P}(n)$ per $n = 0$;

- (passo induttivo) se vale la proposizione $\mathcal{P}(n)$ per un generico $n \in \mathbb{N}$ (ipotesi induttiva), allora vale anche la $\mathcal{P}(n + 1)$.

È facile convincersi che questo davvero è sufficiente: vale infatti la $\mathcal{P}(0)$ per il passo base; applicando allora il passo induttivo per $n = 0$ si trova che vale $\mathcal{P}(1)$; di nuovo per il passo induttivo, ora con $n = 1$, si ha la $\mathcal{P}(2)$, e si procede deducendo che $\mathcal{P}(n)$ vale per ogni n. È importante osservare che nel passo induttivo la validità di $\mathcal{P}(n)$ è una *ipotesi*, ovvero non bisogna dimostrarla. Quello che bisogna fornire è un argomento che sia valido per ogni generico n e che consenta di far discendere la $\mathcal{P}(n + 1)$ dalla $\mathcal{P}(n)$. Un esempio di questo ragionamento è il seguente:

Proposizione 2.3.1. $\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \qquad \forall\, n \in \mathbb{N}.$

Dimostrazione. Chiamiamo $\mathcal{P}(n)$ l'affermazione che $\sum_{k=0}^{n} k$ vale $n(n+1)/2$, e dimostriamola per induzione su n. Il passo base dell'induzione, ovvero $\mathcal{P}(0)$, è certamente valido, poiché i due numeri di cui bisogna verificare l'uguaglianza sono entrambi nulli.

Sia dunque $n \in \mathbb{N}$ generico, e *supponiamo* che $\mathcal{P}(n)$ sia vera, cioè che $\sum_{k=0}^{n} k$ valga $n(n+1)/2$. Vogliamo dedurne che è vera la $\mathcal{P}(n+1)$, cioè che $\sum_{k=0}^{n+1} k$ vale $(n+1)((n+1)+1)/2$, ovvero $(n+1)(n+2)/2$. Infatti $\sum_{k=0}^{n+1} k$ vale $\left(\sum_{k=0}^{n} k\right) + (n+1)$, e per ipotesi induttiva il primo addendo di questa somma vale $n(n+1)/2$. Si conclude ora semplicemente con un calcolo: $n(n+1)/2 + (n+1) = (n+1)(n+2)/2$. $\square$

2.3.2 Dimostrazioni per assurdo

Un'altra tecnica che capita spesso di usare è la seguente. Volendo dimostrare, sotto opportune ipotesi, una proposizione $\mathcal{P}$, si suppone che $\mathcal{P}$ sia falsa (*ipotesi dell'assurdo*) e, usando le ipotesi e fatti noti, si sviluppa un argomento che conduca alla negazione di una delle ipotesi o di un altro fatto noto (*contraddizione*). Dimostriamo ad esempio il fatto già annunciato sopra:

Proposizione 2.3.2. *L'equazione $x^2 = 2$ non ha soluzioni $x \in \mathbb{Q}$.*

Dimostrazione. Supponiamo per assurdo che una soluzione x esista. Utilizziamo ora il fatto noto che x, appartenendo a $\mathbb{Q}$, può essere scritto come una frazione n/m dove n, m sono interi privi di fattori comuni (e $m \neq 0$). Per l'ipotesi dell'assurdo abbiamo allora $(n/m)^2 = 2$, dunque $n^2 = 2m^2$. Ora, se n fosse dispari, anche n^2 sarebbe dispari, mentre $2m^2$ è pari, perciò n è pari, ovvero $n = 2k$ con k intero. Sostituendo nell'identità $n^2 = 2m^2$ e semplificando un 2 troviamo allora $m^2 = 2k^2$. Per lo stesso argomento appena esposto, ne deduciamo che anche m è pari. Questo però è assurdo, perché n e m li avevamo supposti privi di fattori comuni, mentre avrebbero in comune il fattore 2. $\square$