Algebra 1

Stefano Montaldo

Università degli Studi di Cagliari
A.A. 2024-2025

Lo sfondo riprende un particolare della copertina dell'album *Lemma* di John Zorn

Indice

Introduzione

Questi appunti costituiscono una sintesi delle lezioni del corso di Algebra 1 presso il Corso di Studi in Matematica dell'Università di Cagliari, tenute negli anni accademici dal 2015 al 2022.

L'insegnamento di Algebra 1 riveste un'importanza fondamentale nel percorso di studi in Matematica sia per i contenuti trattati che per la forma mentis matematica che gli studenti sviluppano durante il suo studio. Il corso affronta temi apparentemente familiari sin dalle scuole medie, ma li esamina da una prospettiva e con un livello di approfondimento diversi rispetto a quanto solitamente affrontato nelle scuole superiori. È importante sottolineare che questo testo rappresenta solo uno schema generale delle lezioni, e l'uso esclusivo di esso non può sostituire l'esperienza delle lezioni frontali. Durante queste ultime, il docente può dedicare maggiore attenzione ai dettagli, stabilire connessioni cruciali tra le diverse sezioni del programma e valutare se alcuni concetti richiedono ulteriori approfondimenti, concedendo loro quindi più tempo. Tutti questi aspetti sono parte integrante della vera essenza dell'Università, e solo attraverso il dialogo e il confronto continuo è possibile acquisire una conoscenza approfondita della disciplina.

Questo testo è stato redatto con l'intento di assistere gli studenti del primo anno durante l'anno accademico 2020-21, un periodo particolare a causa dell'emergenza COVID-19. Tuttavia, è fondamentale sottolineare che l'uso esclusivo degli appunti non è consigliato, poiché non incentiva gli studenti a consultare altre fonti. Tale pratica non deve essere assolutamente abbandonata; gli studenti sono fortemente incoraggiati a consultare anche altri testi per approfondire gli argomenti trattati.

Infine, desidero informare il lettore che, essendo stati redatti in un breve lasso di tempo a causa dell'emergenza COVID-19, gli appunti attuali contengono numerosi errori. Mi scuso anticipatamente per questo inconveniente e invito gli studenti a segnalare eventuali errori tramite email. Questa collaborazione contribuirà a migliorare gli appunti e sarà di grande aiuto per le generazioni future di studenti.

1. Cenni sulla teoria degli insiemi

1.1 Due parole di logica

Iniziamo con la seguente definizione.

Definizione 1.1 Una *proposizione* (*enunciato*) P è un'affermazione "sensata" alla quale è possibile attribuire un valore di verità : vero (V) o falso (F).

Come vedremo più avanti la vera difficoltà sta proprio nel definire cosa si intenda per "sensata" e per "verità" in matematica. In questo paragrafo ci accontentiamo di affidarci al buon senso del lettore e nel prossimo paragrafo faremo un'analisi più dettagliata del concetto di verità di un'affermazione in matematica.

▪ **Esempio 1.1 — di proposizioni.** Negli esempi seguenti si farà uso di nozioni già note al lettore anche se, più avanti nel testo, alcune di queste saranno riprese e ridefinite.

1. 6 è un numero primo;
2. nel piano esistono coppie di rette parallele;
3. 24 è la somma di due numeri primi;
4. ogni numero pari maggiore di 2 è la somma di due primi (non necessariamente distinti). Questa proposizione è una *congettura*[1] dovuta a *Goldbach* (1742) della quale non si conosce ancora il valore di verità anche se è ragionevole che sia vera o falsa.

▪

▪ **Esempio 1.2 — di non proposizioni.**

(a) come stai?
(b) $1/10$ è un numero piccolo;
(c) l'affermazione al punto (c) dell'Esempio 1.2 è falsa.
Provate è vi accorgerete che se è vera allora è falsa e se è falsa allora è vera.

▪

Proposizioni più complesse possono essere ottenute mediante l'uso dei cosiddetti *connettivi logici*, che elenchiamo di seguito ponendo, per ognuno di essi, il suo significato:

$\neg$	non	negazione
$\wedge$	e	congiunzione
$\vee$	oppure	disgiunzione
$\Rightarrow$	implica	implicazione semplice
$\Leftrightarrow$	se e solo se	doppia implicazione

[1] Una congettura è una proposizione ritenuta vera, ma non ancora rigorosamente dimostrata

Se una proposizione complessa P è ottenuta mediante l'uso dei connettivi logici, a partire da proposizioni $P_1 \dots P_n$, è naturale chiedersi quale sia il suo valore di verità in funzione dei valori di verità delle proposizioni $P_1 \dots P_n$ mediante le quali essa è costruita. Il punto di partenza è dato dalle *tavole di verità* mostrate nelle tabelle seguenti

P	$\neg P$
V	F
F	V

P_1	P_2	$P_1 \wedge P_2$
V	V	V
V	F	F
F	V	F
F	F	F

P_1	P_2	$P_1 \vee P_2$
V	V	V
V	F	V
F	V	V
F	F	F

P_1	P_2	$P_1 \Rightarrow P_2$
V	V	V
V	F	F
F	V	V
F	F	V

P_1	P_2	$P_1 \Leftrightarrow P_2$
V	V	V
V	F	F
F	V	F
F	F	V

Queste tavole di verità hanno un significato intuitivamente molto chiaro: ad esempio, nessuno dovrebbe meravigliarsi, leggendo la seconda tabella, del fatto che $P_1 \wedge P_2$ risulta vera se, e solo se, entrambe P_1 e P_2 sono vere. Solo la quarta tabella potrebbe generare qualche perplessità nel lettore, per cui ora la discutiamo brevemente.
Definiamo le seguenti proposizioni

P_1 : c'è il sole
P_2 : faccio una passeggiata

La proposizione

$P_1 \Rightarrow P_2$ (se c'è il sole, allora faccio una passeggiata)

è *falsa solo se c'è il sole e non faccio una passeggiata*; cioè, $P_1 \Rightarrow P_2$ è falsa solo se P_1 è vera e P_2 è falsa. In parole, se non c'è il sole, il fatto che io faccia la passeggiata o meno non cambia il valore di verità dell'implicazione $P_1 \Rightarrow P_2$, che è V in entrambi i casi.

La confusione nasce dal fatto che si è abituati a pensare che $P_1 \Rightarrow P_2$ sia equivalente a dimostrare che P_2 è vera. In realtà quello che si fa è il seguente ragionamento noto come *Modus Ponens*: se P_1 è vera e $(P_1 \Rightarrow P_2)$ è vera allora P_2 è vera (si veda la tavola di verità dell'implicazione semplice per convincersi di quanto asserito). Ora, concentrandosi un momento, si può anche riconoscere che il *Modus Ponens* è equivalente al fatto che la proposizione (1.1) sotto è una *tautologia* (dove tautologia significa proposizione vera sempre, indipendentemente dai valori di verità delle proposizioni usate per costruirla):

$$P_1 \wedge (P_1 \Rightarrow P_2) \Rightarrow P_2 \,. \tag{1.1}$$

Diciamo che due proposizioni P_1 e P_2 sono *logicamente equivalenti* se hanno la stessa tavola di verità. In tal caso scriviamo $P_1 \equiv P_2$.

Esercizio 1.1 Verificare le seguenti equivalenze logiche

$$\begin{array}{lrcll} 1. & P_1 \Rightarrow P_2 & \equiv & \neg P_1 \vee P_2 & \\ 2. & \neg(P_1 \Rightarrow P_2) & \equiv & P_1 \wedge \neg P_2 & \text{(negazione)} \\ 3. & P_2 \Rightarrow P_1 & \equiv & P_1 \vee \neg P_2 & \text{(inversa)} \\ 4. & \neg P_2 \Rightarrow \neg P_1 & \equiv & P_1 \Rightarrow P_2 & \text{(contronominale)} \end{array}$$

La contronominale è piuttosto utile nella pratica. A titolo di esempio, la proposizione

$P_1 \Rightarrow P_2$ (se n è pari allora 2 divide n)

è equivalente alla sua contronominale

$\neg P_2 \Rightarrow \neg P_1$ (se 2 non divide n allora n non è pari).

Definizione 1.2 Un *predicato* è una proposizione contenente una o più variabili.

■ **Esempio 1.3 — Predicati.**

$P_1(x)$: x è un numero primo.
$P_2(x,y)$: le rette x e y sono incidenti.
$P_3(x,y)$: $x > y$.

■

Se si fissano i valori delle variabili un predicato diventa una proposizione. Ad esempio, con riferimento ai predicati dell'esempio precedente si hanno le seguenti proposizioni:

$P_1(4)$: 4 è un numero primo.

$P_3(5,3)$: $5 > 3$.

Un predicato si può trasformare in una proposizione mediante l'uso dei seguenti *quantificatori*:

(a) il quantificatore *universale* $\forall$ – che si legge "per ogni";

(b) il quantificatore *esistenziale* $\exists$ – che si legge "esiste".

■ **Esempio 1.4 — Uso dei quantificatori.** Se il predicato è

$P_1(x)$: x è un numero primo,

questo si può rendere una proposizione nel modo seguente:

$\exists$ un x: $P_1(x)$ – esiste un x tale che $P_1(x)$ sia vera, cioè esiste almeno un numero primo.

Per il predicato

$P_2(x,y)$: le rette x e y sono incidenti,

una proposizione può essere:

$\forall\, x\, \exists\, y : P_2(x,y)$ – per ogni data retta x esiste almeno una retta y incidente la retta x. ■

Quando si usano i quantificatori in una proposizione la negazione di questa scambia l'utilizzo del quantificatore universale con quello esistenziale e viceversa. Ad esempio, la negazione della proposizione

$\forall\, x$ si ha $x \geq 2$

diventa

$\exists\, x$ tale che $x < 2$.

1.2 Problemi proposti

Problema 1.1 Mostrare che

$$(p \wedge (p \Rightarrow q)) \Rightarrow q$$

è una tautologia, cioè una proposizione vera qualunque siano i valori di verità di p e q. Questa tautologia prende il nome di *principio del modus ponens*.

Problema 1.2 Dimostrare le seguenti equivalenze logiche

- $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- $\neg(A \vee B) \equiv \neg A \wedge \neg B$
- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

Problema 1.3 Mostrare che

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$$

è una tautologia.

Problema 1.4 Siano P, Q ed R proposizioni. Si provi che $(P \vee Q) \Rightarrow R$ e $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ sono logicamente equivalenti.

Problema 1.5 Siano P e Q proposizioni. Si scriva la tavola di verità della proposizione

$$(P \wedge \neg Q) \Rightarrow (Q \vee \neg P)$$

Si sostituiscano quindi P e Q con affermazioni di carattere matematico, scelte in modo che la proposizione risultante sia effettivamente falsa.

Problema 1.6 Siano P e Q proposizioni. Se $P \Rightarrow Q$ è vera e Q è vera, si può concludere che P è vera?

1.3 Il concetto di verità in matematica - facoltativo

Prima di esporre il sistema assiomatico della teoria degli insiemi è utile che il lettore si interroghi sul concetto di verità in matematica. È stata proprio la ricerca di dare senso alla frase *quand'è che un'affermazione è vera in matematica* ad aver condotto gli studiosi a formulare le teorie assiomatiche. Per accompagnare il lettore lungo tale percorso mi son permesso di rielaborare una nota di Luigi Cerlienco proprio dal titolo *Il concetto di verità in matematica* che nel seguito vi propongo.

Per chiarire il concetto di verità in matematica — come pure per tante altre questioni ancora attuali — occorre partire da molto lontano, e cioè almeno dai filosofi greci. Cos'altro erano infatti i *paradossi* di *Zenone di Elea* (V sec. a.C.) se non un interrogarsi sul concetto di verità e metterne in evidenza le ambiguità?
Permettetemi di ricordarli brevemente. Uno era quello di *Achille e la tartaruga*. Zenone immagina che la tartaruga sfidi il piè-veloce Achille ad una gara di corsa. Questi, un po' divertito, accetta, concedendole anzi un congruo vantaggio iniziale, poniamo uno stadio. Resterà però scornato, sostiene Zenone, perchè non la raggiungerà mai. Argomenta infatti che — detto A il punto di partenza di Achille e T quello della tartaruga e ammesso che Achille sia (tanto per fissare le idee) dieci volte più veloce della tartaruga — quando Achille avrà raggiunto il punto T la tartaruga avrà percorso un decimo di stadio e sarà arrivata ad un punto T', quando poi Achille avrà raggiunto il punto T' la tartaruga sarà nel punto T'', più avanti di T' di un centesimo di stadio; e così di seguito. Achille quindi si avvicinerà sempre più alla tartaruga però senza mai raggiungerla.
Analogo è il *paradosso della freccia* che non raggiungerà mai il suo bersaglio, giacché prima di questo dovrà passare per il punto C situato a metà strada tra l'arco A e il bersaglio B, e prima ancora per il punto medio C' del segmento AC, ma prima di questo per il punto medio C'' di AC' ... e così via all'infinito.
Più tardi *Eubulide di Mileto* (IV sec. a.C.) propose altri paradossi. Quello del *sorìte* (=mucchio) che pone il problema dell'uso di termini di significato ambiguo: un chicco di grano non costituisce un mucchio; per ottenerlo si dovrà aggiungere un altro chicco, e poi un altro ancora, e così di seguito; ma a che punto esattamente avrò formato un mucchio?
Più famosa ancora, e molto più profonda, è l'*antinomia del mentitore*: il quale dice *Io mento*[2]. Ma è vero o è falso che lui menta? Ammesso che sia vero, allora è vero che mente e quindi ciò che dice è falso, in contraddizione con l'assunto. Viceversa, se ciò che afferma è falso allora non è vero che mente e quindi ciò che dice è vero, altra contraddizione. Insomma, ciò che dice è vero se e solo se è falso. Il che è ovviamente un'assurdità.
Neppure *Aristotele* (384-322 a.C.) — che pure, affrontando i paradossi di Zenone, aveva introdotto la fondamentale distinzione tra *infinito attuale* e *infinito potenziale* — era riuscito a risolverli. Bisognerà infatti attendere il XVIII secolo per arrivare a capire, con l'uso della teoria delle serie dell'analisi infinitesimale, che Achille raggiungerà la tartaruga in un tempo finito.
Invece l'antinomia del mentitore sarà chiarita solo negli anni trenta del novecento allorché il logico-matematico polacco *Alfred Tarki* (1902-1983) introdurrà la distinzione tra *linguaggio oggetto* e *meta-linguaggio*.

Lo strumento principale di cui si è dotata la matematica per affrontare il problema della verità è il *metodo assiomatico*. Possiamo anche indicarne l'inventore: *Euclide*, il periodo della scoperta: circa il 300 A.C., ed il primo e principale riferimento bibliografico: gli *Elementi*. Alla base di una *teoria assiomatica* Euclide pose alcuni concetti (detti *nozioni primitive*), il cui significato giudicava chiaro ed evidente, ed alcune affermazioni (detti appunto *assiomi della teoria*) la cui verità reputava altrettanto chiara ed evidente per tutti. Poiché in particolare si occupava di geometria i primi erano i concetti di *punto*, *retta*, *piano*, *angolo*, etc. mentre tra i secondi vi era ad es. l'affermazione per cui *dati due punti distinti per essi passa una ed una sola retta*, ed altri altrettanto semplici[3]. Ciò posto la teoria in questione consisteva poi di tutti i concetti che via via potevano essere definiti facendo uso, in ultima analisi, esclusivamente delle nozioni primitive e di tutte le affermazioni (*teoremi*) che si sarebbero successivamente dedotti dagli assiomi sfruttando le usuali regole d'inferenza logica. Ad esempio il concetto di *triangolo* — definibile come *la figura formata da tre punti non allineati e dalle tre rette che li congiungono a due a due* — o il teorema secondo cui *la somma degli angoli interni di un triangolo qualunque è pari ad un angolo piatto.*

[2] Esistono molte altre versioni dell'antinomia del mentitore. Una, ad esempio, è la seguente: "L'affermazione tra virgolette della nota 1) di questa pagina è falsa". Si provi che questa affermazione è vera se e solo se è falsa.

[3] Gli altri quattro garantiscono: 2) la possibilità di prolungare indefinitamente un segmento, 3) la possibilità di tracciare una circonferenza di dati centro e raggio, 4) il fatto che tutti gli angoli retti sono uguali e infine 5) l'esistenza di una ed una sola retta parallela ad una retta assegnata e passante per un dato punto esterno a questa.

In tale contesto la prova della verità di un'affermazione A è ricondotta alla sua dimostrazione all'interno di una teoria assiomatica nel cui ambito A abbia diritto di cittadinanza.

Tale concezione ha retto fino all'inizio dell'ottocento (Kant compreso quindi) allorché la scoperta delle *geometrie non-euclidee*[4] ne ha messo in evidenza un punto debole. Si tratta di quel "chiaro ed evidente" relativo sia alle nozioni primitive che agli assiomi. Si è cioè capito che quando si parla ad esempio di punti e rette ci si può riferire altrettanto legittimamente a più cose tra loro diverse. Similmente è altrettanto lecito costruire, accanto ad una data teoria assiomatica $\mathscr{T}$, un'altra teoria $\mathscr{T}'$ in cui uno degli assiomi di $\mathscr{T}$ sia stato sostituito dalla sua negazione. E quale delle due è quella *vera*? Dal punto di vista matematico hanno entrambe gli stessi diritti (oltreché gli stessi doveri) per cui questa domanda risulta addirittura priva di senso. Al fine di superare questa crisi *David Hilbert* (1862-1943) ha proposto una nuova concezione, secondo la quale gli assiomi vanno semplicemente accettati — e ciò esclusivamente nell'ambito della teoria assiomatica che si fonda su di essi e sempreché siano tra loro non contraddittori — mentre alle nozioni primitive non va attribuito alcun particolare significato se non quello *implicitamente* definito dagli assiomi. Ad es. non bisogna chiedersi quale sia il significato della parola "punto" o di "retta" o dell'"appartenenza di punto a retta" ma accettare che, qualunque cosa questi termini significhino, ciò deve essere in accordo con l'assioma che afferma che *dati due punti distinti per essi passa una ed una sola retta*.
Questa concezione non solo ha permesso di superare le difficoltà di quella euclidea ma ha anche fornito un quadro generale nel quale trovavano corretta collocazione le teorie astratte (algebriche, topologiche, etc) che caratterizzano la matematica attuale. Hilbert era convinto che il metodo assiomatico fosse finalmente lo strumento affidabile e autosufficiente che avrebbe consentito sia di eliminare ogni ambiguità del concetto di verità che di pervenire, almeno in linea di principio, ad accertare la verità o la falsità di ogni affermazione matematica. Più precisamente:

a) un'affermazione A di una teoria assiomatica $\mathscr{T}$ sarà da considerarsi *vera* — nell'ambito della teoria — se risulta essere vera in ogni *modello* della teoria, cioè in ogni situazione concreta[5] nella quale siano interpretabili le nozioni primitive di $\mathscr{T}$ e siano verificati gli assiomi di $\mathscr{T}$;
b) lo strumento per accertare la verità di un'affermazione A è ancora la dimostrazione formale (vale a dire assolutamente rigorosa e controllabile) di A a partire dagli assiomi di $\mathscr{T}$. Ciò che peraltro valeva anche per Euclide; si ha però ora una maggior consapevolezza di tutto l'apparato logico-formale che sostiene tale concezione.

Se da un lato, come è facile vedere, ogni teorema è un'affermazione vera (nel senso precisato in a)) — giacché gli assiomi sono ovviamente veri (ancora, insisto, nel senso precisato in a)) e le deduzioni logiche fanno passare da affermazioni vere ad affermazioni vere — d'altro lato Hilbert era convinto che, viceversa, ogni affermazione vera della teoria fosse anche dimostrabile, cioè, come suol dirsi, che una teoria assiomatica fosse anche *completa*. Per dirla altrimenti: che il complesso dei teoremi[6] esaurisse tutte le affermazioni vere. Purtroppo proprio quest'ultimo aspetto doveva rivelarsi irrealizzabile (se non in casi particolarmente semplici). Ci riferiamo ad uno dei più famosi risultati della logica-matematica novecentesca, il *Teorema di incompletezza di Gödel*.
Molti hanno visto in questo risultato un colpo mortale al programma di Hilbert. Ma che ne pensa il matematico militante? Tutto ciò lo scoraggia al punto da fargli dire: *non vale la pena d'affannarsi per dimostrare un nuovo teorema sapendo che potrebbe proprio essere una di quelle verità indimostrabili di cui parla Gödel*? Ovviamente no! Anzi, per dirla tutta, generalmente gliene importa poco o niente. Non pochi, tra i matematici, nascono, vivono e muoiono — nel mondo matematico, intendo — senza aver mai prestato attenzione al signor Gödel ed al suo terribile teorema. In effetti sono più interessati ad esso i logici e gli epistemologi. La cosa non è senza giustificazione. Le molteplici ragioni di ciò, possono, a mio parere, essere condensate nelle due considerazioni seguenti.

[4] Scoperta fatta, indipendentemente l'uno dall'altro, da tre matematici: il tedesco *Carl Friedrich Gauß* (1777–1855), il russo *Nicolai Ivanovic Lobačevskij* (1792–1856) ed il magiaro *János Bólyai* (1802–1860). Essi capirono che si possono costruire teorie diverse dalla geometria euclidea ma altrettanto rigorose (e, si capirà poi con la teoria della relatività, non prive di importanti applicazioni) conservando i primi quattro assiomi euclidei ma sostituendo il quinto con una sua negazione: o quella che postula infinite rette parallele alla retta data (*geometria iperbolica*) o quella che le esclude del tutto (*geometria ellittica o riemanniana*).

[5] La nozione di *situazione concreta* qui utilizzata va intesa nella sua accezione intuitiva e relativa ad altra situazione al confronto più astratta. Pertanto una situazione concreta in un contesto può poi essere ritenuta astratta, anche all'interno dello stesso discorso, se il contesto di riferimento è cambiato.

[6] Ivi compresi quelli futuri. Ricordiamo che un teorema è, per definizione, un'affermazione che sia stata dimostrata.

La prima è che la dimostrazione di Gödel, pur geniale, si sviluppa tuttavia lungo linee assai lontane da quelle individuabili nelle usuali dimostrazioni di matematica. Essa si produce, in effetti, in una sorta di circolo vizioso — in qualche modo analogo all'*antinomia del mentitore*, come è stato osservato — in cui si ha spesso l'impressione di muoversi su un terreno sdrucciolevole posto in cima a un pendio senza poter capire se si sta per scivolare dolcemente verso una tranquilla valle in cui tutto si chiarisce o viceversa precipitare nel baratro del non-senso assoluto.
Capita di chiedersi: *ma sono solo io che non capisco ciò che per molti altri è perfettamente chiaro?* È possibile che la risposta debba essere affermativa, giacché nei moltissimi lavori specialistici dedicati al teorema di incompletezza e ad una sua corretta interpretazione è difficile trovare i dubbi espressi più sopra. Anzi quasi sempre, in apparenza, l'autore del lavoro in questione dà mostra di aver perfettamente inteso e l'uno e l'altra. Solo che, contestualmente, la sua visione non di rado si contrappone, in modo più o meno esplicito, a quella di qualche altro studioso. E allora al comune matematico viene da pensare che sia meglio tenersi lontano da queste diatribe, lasciandole agli specialisti del settore. Anche perché — e qui veniamo alla seconda considerazione — l'affermazione esibita da Gödel come vera ma indimostrabile è essa stessa (e non solo la sua dimostrazione) così lontana dalle usuali affermazioni della matematica che, compiendo un atto di fede (ne sia consentito uno anche ai matematici!), viene spontaneo ritenere queste ultime esenti dal "morbo di Gödel" cioè dalla patologia genetica che le candida ad essere sia indimostrabili che inconfutabili.

Forti di quanto detto sino ad ora introduciamo nel prossimo paragrafo la teoria assiomatica degli insiemi. Nell'enunciare gli assiomi useremo un linguaggio non completamente formale. Sviluppare in modo strettamente formale la teoria assiomatica degli insiemi richiede un lavoro notevole, e per questo rimandiamo a un corso di Logica Matematica.

1.4 Il sistema assiomatico di Zermelo-Fraenkel

La costruzione assiomatica degli insiemi si indica con con la sigla ZF. La scelta della sigla ricorda che la teoria assiomatica degli insiemi è il risultato del lavoro di *Thoralf Skolem* del 1922 il quale si basa su lavori precedenti di *Abraham Fraenkel* e sul sistema assiomatico sviluppato da *Ernst Zermelo* nel 1908 (teoria degli insiemi di Zermelo). Si indica invece con la sigla ZFC il sistema assiomatico dato dagli assiomi di Zermelo-Fraenkel con l'aggiunta dell'*assioma della scelta* del quale parleremo più avanti in questo testo.

Nel sistema assiomatico ZF vi è un unico concetto primitivo, *l'insieme* e un'unica relazione primitiva fra insiemi, *l'appartenenza*. Per dire che un insieme appartiene ad un altro si scrive

$$X \in Y$$

che si legge "X appartiene ad Y" oppure "X è un elemento di Y". Di solito siamo abituati a distinguere fra *insiemi* ed *elementi*, anche se in realtà basta un solo concetto primitivo.

In seguito, quando sarà utile per aiutare il lettore, indicheremo con le lettere maiuscole $X, Y, Z, \ldots$ gli insiemi e con lettere minuscole $x, y, z, \ldots$ gli elementi di un insieme. Si tenga comunque a mente che gli elementi di un insieme possono essi stessi essere degli insiemi.

Elenchiamo adesso gli assiomi.

ZF 1 — Assioma dell'estensione. Due insiemi X e Y sono uguali se e solo se ogni elemento dell'insieme X è un elemento dell'insieme Y e ogni elemento dell'insieme Y è un elemento dell'insieme X.

Se ogni elemento di X è un elemento di Y scriviamo $X \subseteq Y$ e leggiamo "X è un sottoinsieme di Y".

Segue, dall'assioma dell'estensione, che due insiemi X e Y sono uguali se e solo se $X \subseteq Y$ e $Y \subseteq X$.

ZF 2 — Assioma dell'insieme vuoto. Esiste un insieme che non contiene elementi.

Osserviamo che, se indichiamo un insieme che non contiene elementi con $\varnothing$, allora

$$\varnothing \subseteq X \quad \forall X \text{ insieme}$$

cioè l'insieme vuoto è un sottoinsieme di qualunque insieme X. Ha quindi senso scrivere $\varnothing \subseteq \varnothing$. Dall'assioma di estensione segue che l'insieme vuoto è unico. Si noti che l'assioma dell'insieme vuoto è necessario per garantire l'esistenza di almeno un insieme.

ZF 3 — Assioma della coppia. Per ogni due insiemi X e Y esiste un insieme Z i cui elementi sono solo X e Y.

Questo insieme si denota con $Z = \{X, Y\}$. Osserviamo che X e Y non sono necessariamente distinti, e si ha allora $\{X, X\} = \{X\}$. Dunque, dato un insieme X, l'assioma della coppia afferma, in particolare, l'esistenza di un insieme $\{X\}$ che ha come unico elemento X.

■ **Esempio 1.5** Se $X = \varnothing$ allora $\{X\} = \{\varnothing\}$ è un nuovo insieme che contiene l'insieme vuoto come suo unico elemento. In particolare, $\{\varnothing\} \neq \varnothing$ poiché contiene un elemento. ■

Più avanti mostreremo che nella teoria ZF, per ogni insieme X, $X \notin X$. Segue che, per ogni insieme X, $X \neq \{X\}$. Ugualmente, $\{X\} \neq \{\{X\}\}$, il primo è l'insieme che contiene X come elemento mentre il secondo è l'insieme che contiene come elemento l'insieme che contiene X.

A partire dall'esistenza della coppia si può definire la *coppia ordinata* di due insiemi, indicata con (X, Y), ponendo, per definizione

$$(X, Y) = \{\{X\}, \{X, Y\}\}.$$

Proposizione 1.1 Due coppie ordinate (X, Y) e (X', Y') sono uguali se e solo se $X = X'$ e $Y = Y'$.

Dimostrazione. Se $X = X'$ e $Y = Y'$ allora da ZF 1 $\{X\} = \{X'\}$ e $\{X, Y\} = \{X', Y'\}$. Sempre da ZF 1 $(X, Y) = \{\{X\}, \{X, Y\}\} = \{\{X'\}, \{X', Y'\}\} = (X', Y')$.
Viceversa, supponiamo che $\{\{X\}, \{X, Y\}\} = \{\{X'\}, \{X', Y'\}\}$. Distinguiamo due casi.
Se $X = Y$ segue che $\{\{X\}, \{X, Y\}\} = \{\{X\}, \{X\}\} = \{\{X\}\}$, da cui $\{\{X\}\} = \{\{X'\}, \{X', Y'\}\}$ e quest'ultima implica, sempre per ZF 1, che $\{X', Y'\} = \{X'\} = \{X\}$, cioè $X' = Y' = X$.
Se $X \neq Y$, allora $\{\{X\}, \{X, Y\}\} = \{\{X'\}, \{X', Y'\}\}$ implica che

$$\begin{cases} \{X\} = \{X'\} \\ \{X, Y\} = \{X', Y'\} \end{cases} \quad \vee \quad \begin{cases} \{X\} = \{X', Y'\} \\ \{X, Y\} = \{X'\} \end{cases}$$

Nel primo caso si ottiene, dalla prima condizione, $X = X'$ e la seconda, diventando $\{X, Y\} = \{X, Y'\}$, implica $Y = Y'$. Nel secondo caso la seconda condizione restituisce $X = Y = X'$ contro l'ipotesi che $X \neq Y$ e quindi va scartata. ■

ZF 4 — Assioma dell'unione. Per ogni insieme X esiste un insieme Y (insieme unione degli insiemi che costituiscono X) tale che un insieme T è un elemento di Y se e solo se T è elemento di un elemento di X.

■ **Esempio 1.6** Se $X = \{\{a, b, c\}, \{x, y\}\}$ allora $Y = \{a, b, c, x, y\}$ e si denota usualmente come $Y = \{a, b, c\} \cup \{x, y\}$. ■

■ **Esempio 1.7** Se $X = \{A,B,C,D,E\}$ è un insieme i cui elementi sono un certo numero di insiemi A,B,C,D,E, allora l'insieme unione è

$$Y = \bigcup_{Z\in X} Z = A\cup B\cup C\cup D\cup E.$$

Un elemento $x \in \bigcup_{Z\in X} Z = A\cup B\cup C\cup D\cup E$ se esiste un elemento $Z \in X$ tale che $x \in Z$, cioè se x appartiene ad almeno uno degli insiemi A,B,C,D,E. ■

ZF 5 — Assioma dell'insieme potenza. Per ogni insieme X esiste un insieme Y i cui elementi sono tutti e soli i sottoinsiemi di X.

L'insieme Y, chiamato *insieme delle parti di X* (o insieme potenza), si denota con $\mathscr{P}(X)$.

■ **Esempio 1.8** Se $X = \{a,b,c\}$ allora

$$\mathscr{P}(X) = \{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}.$$

■

■ **Esempio 1.9** Se $X = \{\{a,b,c\},\{x,y\}\}$ allora

$$\mathscr{P}(X) = \{\varnothing,\{\{a,b,c\}\},\{\{x,y\}\},\{\{a,b,c\},\{x,y\}\}\}.$$

■

Vediamo adesso quali insiemi possiamo costruire a partire dagli assiomi descritti sino a questo momento. L'assioma dell'insieme vuoto garantisce l'esistenza di almeno un insieme, $\varnothing$, e usando l'assioma dell'insieme potenza (o della coppia) si ottiene l'insieme $\mathscr{P}(\varnothing) = \{\varnothing\}$ il quale contiene un elemento, per l'appunto $\varnothing$. Applicando adesso l'assioma della coppia agli insieme $\varnothing$ e $\{\varnothing\}$ si ottiene l'insieme $\{\varnothing,\{\varnothing\}\} = \{\varnothing\}\cup\{\{\varnothing\}\}$ che contiene due elementi. Continuando questo processo possiamo costruire la seguente sequenza di insiemi:

$$\varnothing,\quad \{\varnothing\},\quad \{\varnothing,\{\varnothing\}\},\quad \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\},\quad \ldots$$

dove il primo insieme non contiene alcun elemento, il secondo contiene un elemento, il terzo due elementi, il quarto tre elementi e così via. Incredibilmente, dall'insieme vuoto, cioè privo di elementi, siamo in grado di costruire un insieme con un numero qualsiasi (comunque "finito") di elementi!
Se vogliamo parlare di insiemi infiniti, argomento che affronteremo in dettaglio nel seguito, dobbiamo avere un assioma apposito. A tal scopo, definiamo la seguente nozione: se X è un insieme, *l'insieme seguente* è $S(X) = X\cup\{X\}$. Per esempio,

$$S(\varnothing) = \varnothing\cup\{\varnothing\} = \{\varnothing\},\quad S(S(\varnothing)) = \{\varnothing\}\cup\{\{\varnothing\}\} = \{\varnothing,\{\varnothing\}\},$$

$$S(S(S(\varnothing))) = \{\varnothing,\{\varnothing\}\}\cup\{\{\varnothing,\{\varnothing\}\}\} = \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$$

ZF 6 — Assioma dell'infinito. Esiste un insieme X che ha $\varnothing$ come elemento e per ogni $Y \in X$ anche $S(Y) \in X$.

Mostreremo in seguito che l'assioma dell'infinito è equivalente all'assioma di Peano e che entrambi garantiscono l'esistenza dei *numeri naturali* i quali formano un insieme che contiene una *infinità attuale* di elementi, cioè tale che i suoi infiniti elementi possano essere considerati contemporaneamente, e non solo uno dopo l'altro.

Ora che abbiamo un buon numero di insiemi possiamo costruire altri insiemi come *sottoinsiemi* di insiemi già noti.

ZF 7 — Assioma di comprensione. Per ogni insieme X e per ogni proprietà P di insiemi, esiste un insieme Y tale che $Z \in Y$ se e solo se $Z \in X$ e Z gode della proprietà P.

Di solito si scrive $Y = \{Z \in X : P(Z)\}$.

Nella formulazione di questo assioma è evidente l'incertezza di significato dell'espressione *proprietà di insiemi*. Formulare con precisione tale significato è molto difficile nel linguaggio naturale che stiamo usando; diciamo solo che una proprietà di insiemi è espressa mediante una *frase* che contiene solo simboli per rappresentare insiemi, i connettivi (a parole o in simboli), i quantificatori (a parole o in simboli), loro sinonimi, e che sia costruita *regolarmente*. Proprio dire quando una frase è costruita regolarmente presenta le difficoltà maggiori e necessita l'introduzione di un linguaggio formale e la nozione di correttezza sintattica. Rimandiamo ad un corso di logica per una trattazione più completa. In questo paragrafo, piuttosto che tentare di definire con precisione cosa sia una proprietà di insiemi, vediamone almeno alcune, che corrispondono a costruzioni ben note.

■ **Esempio 1.10 — Intersezione di insiemi.** Siano X, Y due insiemi. Se $P(Z)$ è la proprietà $Z \in Y$, allora l'assioma di comprensione garantisce l'esistenza *dell'intersezione*

$$X \cap Y = \{Z \in X : Z \in Y\} = \{Z \in Y : Z \in X\}.$$

Se $\mathscr{F} \subseteq \mathscr{P}(X)$ è un insieme i cui elementi sono sottoinsiemi di X allora si ha

$$\bigcap_{A \in \mathscr{F}} A = \{x \in X : x \in A \ \forall A \in \mathscr{F}\}.$$

■

Esercizio 1.2 Verificare che valgono le seguenti proprietà:

1. $X \cap X = X \quad \wedge \quad X \cup X = X$ idempotenza;
2. $X \cap Y = Y \cap X \quad \wedge \quad X \cup Y = Y \cup X$ commutativa;
3. $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ associativa;
4. $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ associativa;
5. $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ distributiva;
6. $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ distributiva.

■ **Esempio 1.11 — Differenza tra insiemi.** Siano X, Y due insiemi. Se $P(Z)$ è la proprietà $Z \notin Y$ allora si definisce la *differenza tra insiemi*

$$X \setminus Y = \{Z \in X : Z \notin Y\}.$$

Nel caso particolare in cui $Y \subseteq X$ denotiamo $X \setminus Y$ con $C_X(Y)$ che si legge "il complementare di Y in X" . ■

Esercizio 1.3 Verificare che

$$X \setminus Y = \varnothing \quad \Leftrightarrow \quad X \subseteq Y.$$

Proposizione 1.2 — Formule di De Morgan. Sia X un insieme e sia $\mathscr{F} \subseteq P(X)$ un sottoinsieme dell'insieme delle parti di X. Allora se $Y \subseteq X$ è un sottoinsieme di X valgono le seguenti uguaglianze tra insiemi:

$$\text{(a)} \quad Y \setminus \bigcup_{B \in \mathscr{F}} B = \bigcap_{B \in \mathscr{F}} (Y \setminus B), \qquad \text{(b)} \quad Y \setminus \bigcap_{B \in \mathscr{F}} B = \bigcup_{B \in \mathscr{F}} (Y \setminus B)$$

Dimostrazione. Dimostriamo la (b) e lasciamo la (a) come esercizio. Dovendo dimostrare l'uguaglianza tra due insiemi procediamo dimostrando che valgono le due inclusioni

$$Y \setminus \bigcap_{B\in\mathscr{F}} B \subseteq \bigcup_{B\in\mathscr{F}} (Y\setminus B) \qquad \bigcup_{B\in\mathscr{F}} (Y\setminus B) \subseteq Y \setminus \bigcap_{B\in\mathscr{F}} B$$

Per la prima, se $x \in Y \setminus \bigcap_{B\in\mathscr{F}} B \;\Rightarrow\; x \in Y \wedge x \notin \bigcap_{B\in\mathscr{F}} B \;\Rightarrow\; x \in Y \wedge \exists B_0 \in \mathscr{F} : x \notin B_0 \;\Rightarrow\; x \in (Y \setminus B_0) \;\Rightarrow\; x \in \bigcup_{B\in\mathscr{F}} (Y\setminus B)$.

Per la seconda se $x \in \bigcup_{B\in\mathscr{F}} (Y\setminus B) \;\Rightarrow\; \exists B_0 \in \mathscr{F} : x \in (Y\setminus B_0) \;\Rightarrow\; x \in Y \wedge x \notin B_0 \;\Rightarrow\; x \in Y \wedge x \notin \bigcap_{B\in\mathscr{F}} B \;\Rightarrow\; x \in Y \setminus \bigcap_{B\in\mathscr{F}} B$. ■

Definizione 1.3 Sia X un insieme e sia $\mathscr{F} \subseteq \mathscr{P}(X)$ una famiglia di sottoinsiemi di X. Diciamo che $\mathscr{F}$ è una *partizione* di X se valgono le seguenti proprietà:
(a) $\forall A \in \mathscr{F}, \quad A \neq \varnothing$
(b) $X = \bigcup_{A\in\mathscr{F}} A$;
(c) $\forall A, B \in \mathscr{F}, \quad A \neq B$ se e solo se $A \cap B = \varnothing$.

■ **Esempio 1.12** Se $X = \{a,b,c,d\}$, allora due esempi di partizione sono

$$\mathscr{F}_1 = \{\{a\},\{b,c\},\{d\}\}, \quad \mathscr{F}_2 = \{\{a\},\{b,c,d\}\}.$$

■

Per enunciare con precisione il prossimo assioma, ricordiamo la definizione di prodotto cartesiano di insiemi X e Y che, intuitivamente, è l'insieme di tutte le coppie ordinate il cui primo elemento appartiene a X e il secondo a Y. Per dare la definizione formale, osserviamo che se $x \in X$ e $y \in Y$, allora $\{x\},\{x,y\} \in \mathscr{P}(X \cup Y)$ e $(x,y) = \{\{x\},\{x,y\}\} \in \mathscr{P}(\mathscr{P}(X \cup Y))$.

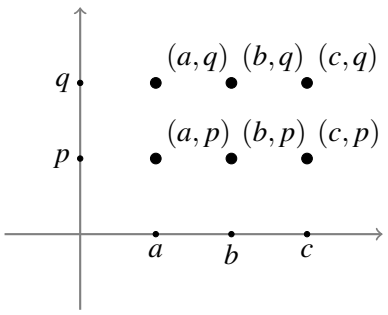
Definizione 1.4 Dati due insiemi X e Y, il *prodotto cartesiano* è definito come l'insieme

$$X \times Y = \{Z \in \mathscr{P}(\mathscr{P}(X \cup Y)) : \exists x \in X \wedge \exists y \in Y \text{ con } Z = (x,y)\}$$

■ **Esempio 1.13** Se $X = \{a,b,c\}$ e $Y = \{p,q\}$ il prodotto cartesiano di X e Y è

$$X \times Y = \{\{a,p\},\{a,q\},\{b,p\},\{b,q\},\{c,p\},\{c,q\}\}$$

il quale si può rappresentare graficamente come (il grafico seguente deve essere visto solo come una rappresentazione astratta del prodotto cartesiano)

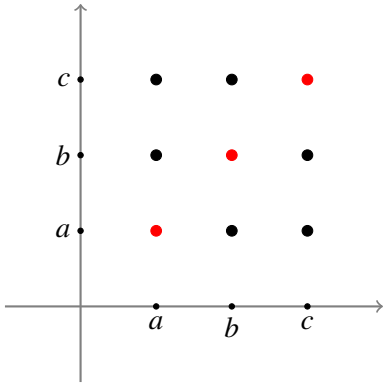


■

■ **Esempio 1.14** Se $X = Y$ scriviamo $X \times X = X^2$. In questo caso chiamiamo il sottoinsieme

$$\Delta_X = \{(x,x) : x \in X\} \subseteq X \times X$$

la *diagonale* di $X \times X$. La rappresentazione grafica di Δ_X ricorda proprio la diagonale del quadrato. Per esempio se $X = \{a,b,c\}$ la diagonale Δ_X nel diagramma seguente è rappresentata dai punti in rosso:



■

Esercizio 1.4 Verificare le seguenti proprietà:
1. $X \times \varnothing = \varnothing \times Y = \varnothing$;
2. Se $X, Y \neq \varnothing \quad \Rightarrow \quad X \times Y = Y \times X \quad \Leftrightarrow \quad X = Y$;
3. Se $X' \subseteq X \ \wedge \ Y' \subseteq Y \quad \Rightarrow \quad X' \times Y' \subseteq X \times Y$;
4. $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$;
5. $(X \cap T) \times (Y \cap Z) = (X \times Y) \cap (T \times Z)$.

ZF 8 — Assioma del rimpiazzamento. Sia P una proprietà definita sulle coppie ordinate di insiemi, tale che: per ogni elemento x di un insieme X e per ogni coppia di elementi y_1 e y_2 appartenenti a un insieme Y, se le coppie (x, y_1) e (x, y_2) soddisfano la proprietà P, allora $y_1 = y_2$. Allora esiste un sottoinsieme $Y' \subseteq Y$ contenente tutti gli elementi $y' \in Y$ per i quali esiste un $x \in X$ tale che la coppia (x, y') soddisfi la proprietà P, cioè

$$Y' = \{y' \in Y : \exists x \in X \quad \wedge \quad P(x, y')\}$$

Il significato è utilizzo di questo assioma sarà spiegato nel seguito della trattazione, in particolare, quando si tratteranno le relazioni e le funzioni tra insiemi.

Osserviamo, infine, che l'assioma di comprensione garantisce l'esistenza di un insieme per ogni proprietà, ossia per ogni formula *sintatticamente corretta*, ma solo come sottoinsieme di un insieme già dato. Ci si può dunque chiedere se questo assioma possa essere ampliato, ovvero se, data una proprietà P, sia possibile postulare l'esistenza di un insieme costituito da tutti gli insiemi che soddisfano P. Questa era l'idea originaria di Cantor e Frege, secondo cui "insieme = proprietà". Tuttavia, il paradosso di Russell dimostrò che non basta che la formula che definisce P sia sintatticamente corretta.
Il paradosso di Russell deriva dal fatto che secondo l'idea di Cantor e Frege $X = \{Z : Z \notin Z\}$ sarebbe un insieme. Ma questo porta ad una contraddizione: infatti, supponendo che $X \in X$, si dedurrebbe che $X \notin X$; d'altra parte, assumendo che $X \notin X$, si arriverebbe alla conclusione che $X \in X$. In entrambi i casi, sia $X \in X$ che $X \notin X$ portano a una contraddizione.
Una possibile soluzione a questo paradosso consiste nell'impedire che un insieme possa appartenere a sé stesso. A tale scopo, viene introdotto il seguente assioma.

ZF 9 — Assioma della fondazione. Sia P una proprietà degli insiemi, e supponiamo che esista un insieme Y che gode di P. Allora esiste un insieme X che gode di P e tale che ogni suo elemento non gode di P.

L'assioma della fondazione permette di dimostrare che un insieme non può essere elemento di se stesso.

Proposizione 1.3 Per ogni insieme X si ha

$$X \notin X\,.$$

Dimostrazione. Sia $P(U)$ la proprietà $U \in U$. Supponiamo, per assurdo, che esista un insieme Y tale che $P(Y)$, cioè $Y \in Y$. Per l'assioma della fondazione esiste un altro insieme X tale che

(i) $X \in X$, cioè $P(X)$ è vera;

(ii) per ogni $Z \in X$, $Z \notin Z$, cioè per ogni $Z \in X$, $P(Z)$ è falsa.

Dalla (i) si ha che $X \in X$, di conseguenza, dalla (ii), si deve avere $X \notin X$ che fornisce una contraddizione. Dunque non può esistere alcun insieme Y tale che $Y \in Y$. ■

La Proposizione 1.3 implica che il "candidato ad essere un insieme" nel sopracitato paradosso di Russel, cioè

$$X = \{Z\colon Z \notin Z\}\,,$$

è la totalità di **tutti** gli insiemi dell'universo di Zermelo–Fraenkel. Se X fosse un insieme, contenendo tutti gli insiemi, si avrebbe $X \in X$, in contraddizione con la Proposizione 1.3. Quindi $X = \{Z\colon Z \notin Z\}$ non è un insieme e si evita il paradosso di Russell.

Nulla vieta che, nella teoria ZF, ci siano altri paradossi meno immediati e non ancora scoperti, ma per ora (in poco più di cento anni) non ne sono stati trovati.

L'ultimo assioma, l'assioma della scelta, sarà enunciato in seguito.

Per proseguire con lo studio è utile, in questa fase, riflettere con attenzione principalmente sugli assiomi ZF 1, ZF 2, ZF 3, ZF 4, ZF 5 e ZF 7. I restanti assiomi saranno richiamati all'occorrenza e discussi nel contesto appropriato.

1.5 Problemi proposti

Problema 1.7 Dire quali delle seguenti affermazioni sono vere

- $\varnothing \in \{\varnothing, 2\}$
- $\varnothing \subseteq \{\varnothing, \{\varnothing\}\}$
- $\{\varnothing\} = \{\varnothing, \{\varnothing\}\}$
- $\{1\} \in \{1,2\}$
- $\{\{1\}\} \subseteq \{1,2\}$
- $\{\varnothing\} = \{\varnothing, \{\varnothing\}\}$
- $\varnothing = \{x\colon \{1,x\} = \{1,2,3\}\}$

Problema 1.8 Descrivere l'insieme $P(\{1,2,3,4\})$.

Problema 1.9 Siano A e B due insiemi. Provare che

$$\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B) \quad \text{e} \quad \mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$$

Problema 1.10 Siano A e B due insiemi. Provare che $A \subseteq B$ se e solo se $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

Problema 1.11 Siano X, Y, Z insiemi. Dimostrare le seguenti proprietà dell'unione e dell'intersezione tra insiemi.

- $X \cup Y = Y \cup X$
- $(X \cup Y) \cup Z = X \cup (Y \cup Z)$
- $X \cup X = X$
- $X \cap Y = Y \cap X$
- $(X \cap Y) \cap Z = X \cap (Y \cap Z)$
- $X \cap X = X$

Problema 1.12 Siano A, B, C insiemi. Dimostrare le seguenti uguaglianze (proprietà distributiva):

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

Problema 1.13 Siano A, B e C insiemi. Si provi che $(A \cup B) \cap C = A \cup (B \cap C)$ se e solo se $A \subseteq C$.

Problema 1.14 Definiamo la *differenza simmetrica* $A\Delta B$ di due insiemi A e B nel modo seguente:

$$A\Delta B = (A \setminus B) \cup (B \setminus A)$$

Si provino le seguenti proprietà della differenza simmetrica

- $A\Delta A = \varnothing$
- $A\Delta\varnothing = A$
- $A\Delta B = (A \cup B) \setminus (A \cap B)$
- $A\Delta B = B\Delta A$
- $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$

Vale anche la proprietà associativa $(A\Delta B)\Delta C = A\Delta(B\Delta C)$ la cui dimostrazione utilizza una costruzione che vedremo più avanti nel corso. Se lo desiderate provate già da adesso ma è piuttosto laboriosa.

Come mai non compare la proprietà $A \cup (B\Delta C) = (A \cup B)\Delta(A \cup C)$?

Problema 1.15 Siano A, B e C insiemi. Si provi che

- $A \setminus B = A \setminus C$ se e solo se $A \cap B = A \cap C$
- $A\Delta(B \cup C) \subseteq (A\Delta B) \cup C$
- $A\Delta(B \cup C) = (A\Delta B) \cup C$ se e solo se $A \cap C = \varnothing$

2. Relazioni binarie e funzioni

2.1 Relazioni e funzioni

Iniziamo con la seguente

Definizione 2.1 Siano X e Y due insiemi non vuoti. Una *relazione binaria* di X in Y è un sottoinsieme $R \subseteq X \times Y$. Se $X = Y$ chiamiamo una relazione binaria $R \subseteq X \times X$ semplicemente una relazione su X.

■ **Esempio 2.1** Se $X = \{a,b,c,d\}$ e $Y = \{p,q,r\}$ allora i seguenti sottoinsiemi di $X \times Y$ rappresentano relazioni binarie di X in Y.

1. $R_1 = \{(a,p),(a,q),(b,q),(c,q),(d,r)\}$
2. $R_2 = \{(a,p),(c,q),(d,r)\}$
3. $R_3 = \{(a,p),(b,q),(c,q),(d,r)\}$

■

Tra tutte le relazioni di un insieme in un altro insieme hanno un ruolo fondamentale quelle che definiscono le funzioni tra due insiemi.

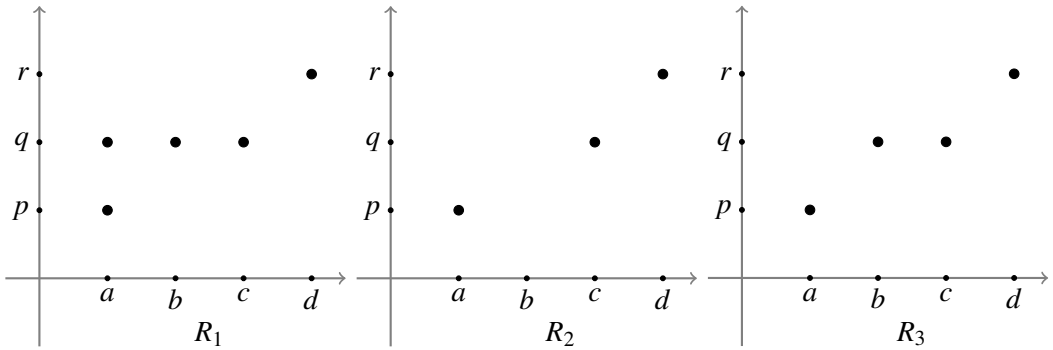
Definizione 2.2 Siano X e Y due insiemi non vuoti. Una *relazione binaria* $R \subseteq X \times Y$ definisce una *funzione* se valgono le seguenti proprietà:

(a) per ogni $x \in X$ esiste un $y \in Y$ tale che $(x,y) \in R$;
(b) se $(x,y),(x,y') \in R$ allora $y = y'$.

■ **Esempio 2.2** Con riferimento all'Esempio 2.1 si ha che

1. R_1 non è una funzione poiché $(a,p),(a,q) \in R_1$ ma $p \neq q$;
2. R_2 non è una funzione poiché per $b \in X$ non esiste alcun elemto $y \in Y$ con $(b,y) \in R_2$;
3. R_3 definisce invece una funzione.

È utile rappresentare graficamente le relazioni R_1, R_2 e R_3. Si trova



Dall'analisi dei grafici sopra si evince immediatamente che R_1 non è una funzione poiché vi sono due punti in corrispondenza di a mentre R_2 non è una funzione poiché non vi è alcun punto in corrispondenza di b. ∎

Data una funzione $R \subseteq X \times Y$ si può costruire una corrispondenza tra gli elementi di X e quelli di Y nel modo seguente:

ad ogni $x \in X$ si fa corrispondere l'unico elemento $y \in Y$ tale che $(x,y) \in R$.

La corrispondenza descritta sopra si indica con il seguente diagramma

$$X \to Y$$
$$x \mapsto y = \text{l'unico elemento di } Y \text{ tale che } (x,y) \in R$$

ed, in aggiunta, si indica la corrispondenza che ad x associa y con una lettera f, g, h etc. Si scrive quindi

$$f : X \to Y$$
$$x \mapsto f(x) = y = \text{l'unico elemento di } Y \text{ tale che } (x,y) \in R\,.$$

Diamo adesso alcune definizioni. Sia $f : X \to Y$ una funzione.

- L'insieme X è chiamato *dominio* della funzione.
- L'insieme Y è chiamato *codominio* della funzione.
- Se $x \in X$, chiamiamo *immagine* di x l'elemento $f(x) \in Y$.
- Se $A \subseteq X$, chiamiamo immagine dell'insieme A in Y

$$f(A) = \{y \in Y : \exists\, x \in A \text{ con } f(x) = y\}.$$

- Se $A = X$, chiamiamo $f(X)$ *immagine della funzione*.
- Se $y \in Y$ chiamiamo $f^{-1}(y) = \{x \in X : f(x) = y\} \subseteq X$ la *controimmagine* dell'elemento $y \in Y$.
- Se $B \subseteq Y$ chiamiamo $f^{-1}(B) = \{x \in X : f(x) \in B\} \subseteq X$ la controimmagine dell'insieme B.

Esercizio 2.1 Utilizzare ZF8 per dimostrare che data una funzione $f : X \to Y$, $f(X)$ è un insieme.

■ **Esempio 2.3** Sia X un insieme e sia $\mathscr{P}(X)$ l'insieme delle parti. Allora la relazione

$$R = \{(x,\{x\}) : x \in X\} \subseteq X \times \mathscr{P}(X)$$

definisce la funzione

$$f : X \to \mathscr{P}(X)$$
$$x \mapsto \{x\}$$

∎

■ **Esempio 2.4** Sia X un insieme. Allora la diagonale di X

$$\Delta_X = \{(x,x) : x \in X\} \subseteq X \times X$$

definisce la funzione

$$\mathrm{Id}_X : X \to X$$
$$x \mapsto x$$

che prende il nome di *funzione identità*. ∎

■ **Esempio 2.5** Siano X e Y due insiemi. Allora la relazione

$$R = \{((x,y),x) : x \in X \wedge y \in Y\} \subseteq (X \times Y) \times X$$

definisce la funzione

$$Pr_1 : X \times Y \to X$$
$$(x,y) \mapsto x$$

che prende il nome di *proiezione* sul primo fattore. ■

■ **Esempio 2.6** Sia X un insieme e sia $A \subseteq X$ un sottoinsieme. Allora la relazione

$$R = \{(x,x) : x \in A\} \subseteq A \times X$$

definisce la funzione

$$i_A : A \to X$$
$$x \mapsto x$$

che prende il nome di *inclusione*. ■

■ **Esempio 2.7** Siano X e Y due insiemi e sia $f : X \to Y$ una funzione. Sia $A \subseteq X$ un sottoinsieme. Allora la relazione

$$R = \{(x,y) : x \in A \wedge y = f(x)\} \subseteq A \times Y$$

definisce la funzione

$$f_{|_A} : A \to Y$$
$$x \mapsto f(x)$$

che prende il nome di *restrizione* di f ad A. ■

Osservazione 2.1 Se $f : X \to Y$ è una funzione, allora la relazione

$$R = \{(x,y) \in X \times Y : y = f(x)\}$$

che la definisce prende anche il nome di *grafico* della funzione.

Esercizio 2.2 Sia $f : X \to Y$ una funzione. Verificare che $\left\{f^{-1}(y)\right\}_{y \in Y}$ definisce una partizione di X.

Definizione 2.3 Siano $X, Y \neq \varnothing$ due insiemi. Denotiamo con

$$Y^X = \{f : X \to Y : f \text{ funzione}\}$$

l'insieme di tutte le funzioni da X in Y.

■ **Esempio 2.8** Se $Y = \{0,1\}$ è un insieme formato da due elementi indichiamo con 2^X l'insieme Y^X. ■

Definizione 2.4 Una funzione $f : X \to Y$ si dice:
(a) *iniettiva* se: $\forall x_1, x_2 \in X \quad f(x_1) = f(x_2) \quad \Rightarrow \quad x_1 = x_2$;
(b) *suriettiva* se: $\forall y \in Y \quad \exists x \in X$ tale che $f(x) = y$;

(c) *biettiva* se è sia iniettiva che suriettiva.

■ **Esempio 2.9** Se $X = \{a,b,c,d\}$ e $Y = \{p,q,r\}$ allora i seguenti sottoinsiemi di $X \times Y$ definiscono una funzione da X in Y:

1) $R_1 = \{(a,p),(b,q),(c,q),(d,p)\}$
2) $R_2 = \{(a,p),(b,q),(c,q),(d,r)\}$

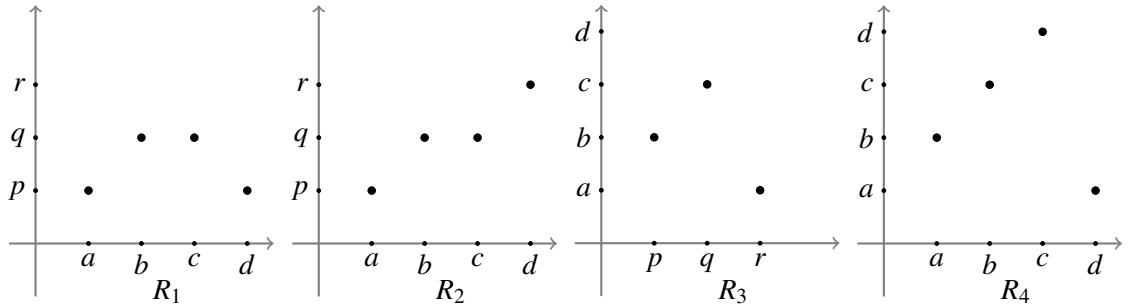
il seguente sottoinsieme di $Y \times X$ definisce una funzione da Y in X:

3) $R_3 = \{(p,b),(q,c),(r,a)\}$

ed infine il seguente sottoinsieme di $X \times X$ definisce una funzione da X in X:

4) $R_4 = \{(a,b),(b,c),(c,d),(d,a)\}$

La rappresentazione grafica delle funzioni sopra descritte è:



Si deduce immediatamente che: R_1 definisce una funzione né iniettiva ($f_1(a) = f_1(d) \wedge f_1(b) = f_1(c)$) né suriettiva ($r \in Y$ non è immagine di alcun elemento di X); R_2 definisce una funzione non iniettiva ($f_2(b) = f_2(c)$) ma suriettiva; R_3 definisce una funzione iniettiva ma non suriettiva ($d \in X$ non è immagine di alcun elemento di Y); R_4 definisce una funzione sia iniettiva che suriettiva. ■

■ **Esempio 2.10** La funzione $\mathrm{Id}_X : X \to X$ definisce una funzione biettiva. La funzione inclusione $i_A : A \to X$, $A \subseteq X$, definisce una funzione iniettiva la quale, se $A \neq X$, non è suriettiva. ■

Osservazione 2.2 Applicando la contronominale alla definizione di funzione iniettiva si ottiene che $f : X \to Y$ è iniettiva se $\forall x_1, x_2 \in X \quad x_1 \neq x_2 \quad \Rightarrow \quad f(x_1) \neq f(x_2)$. Invece, una funzione $f : X \to Y$ è suriettiva se e solo se $f(X) = Y$, cioè se l'immagine di f coincide con il codominio.

Vale l'importante teorema

Teorema 2.1 — Teorema di Cantor. Sia $X \neq \varnothing$ un insieme. Allora, non esiste una funzione suriettiva $f : X \to \mathscr{P}(X)$.

Dimostrazione. Supponiamo, per assurdo, che esista una funzione $f : X \to \mathscr{P}(X)$ suriettiva. Sia

$$A = \{x \in X : x \notin f(x)\}.$$

Siccome f è suriettiva e $A \in \mathscr{P}(X)$, esiste $x_0 \in X$ con $f(x_0) = A$. Ci chiediamo se $x_0 \in A$. Se $x_0 \in A$ allora, per definizione di A, $x_0 \notin f(x_0) = A$, quindi assurdo. Supponiamo allora che $x_0 \notin A$. Ma allora, sempre per la definizione di A, segue che $x_0 \in f(x_0) = A$ che conduce nuovamente ad un assurdo. Siamo quindi pervenuti all'assurdo, ipotizzando che f fosse suriettiva, che l'elemento x_0 non può né appartenere né non appartenere ad A. Concludiamo che f non può essere suriettiva. ■

Se esiste una funzione biettiva tra due insiemi X e Y diciamo che i due insiemi sono in *corrispondenza biunivoca*. Siamo soliti indicare le corrispondenze biunivoche con la doppia freccia $X \leftrightarrow Y$.

Osservazione 2.3 Siano X, Y due insiemi e siano $f, g : X \to Y$ due funzioni. Allora le due funzioni coincidono, cioè $f \equiv g$, se e solo se $\forall x \in X$ si ha $f(x) = g(x)$.

Proposizione 2.1 Sia X un insieme, sia $\mathscr{P}(X)$ il corrispondente insieme delle parti e sia $2^X = \{f : X \to \{0,1\} : f \text{ funzione}\}$. Allora esiste una corrispondenza biunivoca tra $\mathscr{P}(X)$ e 2^X.

Dimostrazione. Sia $A \subseteq X$ un sottoinsieme di X. Definiamo la *funzione caratteristica* di A come

$$\begin{aligned} &\mathscr{X}_A : X \to \{0,1\} \\ &\qquad x \longmapsto \mathscr{X}_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases} \end{aligned} \tag{2.1}$$

Per costruzione $\mathscr{X}_A \in 2^X$. Definiamo quindi la seguente funzione:

$$\begin{aligned} \varphi : \mathscr{P}(X) &\to 2^X \\ A &\mapsto \varphi(A) = \mathscr{X}_A \end{aligned}$$

Mostriamo che φ è iniettiva e suriettiva. Per l'iniettività, siano $A, B \subseteq X$ tali che $\varphi(A) = \varphi(B)$ e mostriamo che $A = B$, cioè che $A \subseteq B$ e $B \subseteq A$. Per $A \subseteq B$, sia $x \in A$ allora

$$1 = \mathscr{X}_A(x) = \varphi(A)(x) = \varphi(B)(x) = \mathscr{X}_B(x).$$

Quindi $\mathscr{X}_B(x) = 1$ da cui segue che $x \in B$. Allo stesso modo si dimostra che $B \subseteq A$. Per la suriettività, sia $f \in 2^X$ una qualsiasi funzione $f : X \to \{0,1\}$ e sia $A = f^{-1}(1) = \{x \in X : f(x) = 1\}$. Si verifica facilmente che $\mathscr{X}_A = f$ da cui $\varphi(A) = \mathscr{X}_A = f$, cioè $\forall f \in 2^X \quad \exists A = f^{-1}(1) \in \mathscr{P}(X) : \varphi(A) = f$. ■

2.2 Funzioni composte

Definizione 2.5 — Funzione composta. Siano X, Y, Z tre insieme e siano $f : X \to Y$, $g : Y \to Z$ due funzioni. Definiamo la *funzione composta* $g \circ f : X \to Z$ nel modo seguente: $\forall x \in X \quad g \circ f(x) := g(f(x))$.

Si veda il seguente diagramma che illustra com'è definita la funzione composta

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \\ x & \mapsto & f(x) & \mapsto & g(f(x)) \end{array}$$

Nei prossimi esempi useremo sia l'insieme dei numeri naturali che quello dei numeri interi e saranno denotati, rispettivamente, con le lettere $\mathbb{N}$ e $\mathbb{Z}$. Non diamo adesso la costruzione formale di questi due insiemi numerici (tale costruzione costituisce una parte importante di questo corso) ma ci affidiamo alla consapevolezza che il lettore abbia un'idea, almeno intuitiva, di chi siano i numeri naturali $\{0,1,2,3,4,\ldots\}$ e i numeri interi $\{\ldots,-4,-3,-2,-1,0,1,2,3,4,\ldots\}$.

■ **Esempio 2.11** Date le due funzioni

$$\begin{array}{rccc} f: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & n^2 \end{array} \qquad \begin{array}{rccc} g: & \mathbb{N} & \to & \mathbb{Z} \\ & n & \mapsto & -n \end{array}$$

la funzione composta $g \circ f$ è

$$\begin{array}{ccccc} \mathbb{N} & \xrightarrow{f} & \mathbb{N} & \xrightarrow{g} & \mathbb{Z} \\ n & \mapsto & n^2 & \mapsto & -n^2 \end{array}$$

■

■ **Esempio 2.12** Date le due funzioni

$$\begin{array}{rccc} f: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & n+1 \end{array} \qquad \begin{array}{rccc} g: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & n^2 \end{array}$$

la funzione composta $g \circ f$ è

$$\begin{array}{ccccc} \mathbb{N} & \xrightarrow{f} & \mathbb{N} & \xrightarrow{g} & \mathbb{N} \\ n & \mapsto & n+1 & \mapsto & (n+1)^2 \end{array}$$

■

! Si osservi che nell'Esempio 2.11 la composizione $f \circ g$ non ha senso poichè f non è definita per i numeri relativi. L'Esempio 2.12 mostra che anche quando sia possibile commutare l'ordine nella composizione di due funzioni le funzioni composte ottenute sono differenti. Infatti, sempre con riferimento all'Esempio 2.12, si trova:

$$\begin{array}{rccc} g \circ f: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & (n+1)^2 \end{array} \qquad \begin{array}{rccc} f \circ g: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & n^2+1 \end{array}$$

Proposizione 2.2 Siano X, Y, Z tre insieme e siano $f : X \to Y$, $g : Y \to Z$ due funzioni.
(a) Se f e g sono iniettive allora $g \circ f$ è iniettiva;
(b) Se f e g sono suriettive allora $g \circ f$ è suriettiva;
(c) Se $g \circ f$ è iniettiva allora f e iniettive;
(d) Se $g \circ f$ è suriettiva allora g e suriettiva.

Dimostrazione.

(a) Siano $x, y \in X$. Mostriamo che se $g \circ f(x) = g \circ f(y)$ allora $x = y$. Si ha

$$g \circ f(x) = g \circ f(y) \xrightarrow{\text{def. composizione}} g(f(x)) = g(f(y)) \xrightarrow{g \text{ iniettiva}} f(x) = f(y) \xrightarrow{f \text{ iniettiva}} x = y.$$

(b) Mostriamo che per ogni $z \in Z$ esiste $x \in X$ con $g \circ f(x) = z$. Poiché g è suriettiva $\forall z \in Z\ \exists y \in Y : g(y) = z$. Poiché f è suriettiva $\exists x \in X : f(x) = y$. Segue che $g \circ f(x) = g(f(x)) = g(y) = z$.

(c) Siano $x_1, x_2 \in X$ e supponiamo che $f(x_1) = f(x_2)$. Allora, $g(f(x_1)) = g(f(x_2))$ da cui $g \circ f(x_1) = g \circ f(x_2) \xrightarrow{g \circ f \text{ iniettiva}} x_1 = x_2$.

(d) Sia $z \in Z$. Dalla suriettività di $g \circ f$ segue che $\exists x \in X : g \circ f(x) = z \quad \Rightarrow \quad g(f(x)) = z$. Siccome $f(x) \in Y$ segue che $\forall z \in Z$ esiste $f(x) \in Y$ con $g(f(x)) = z$, cioè g è suriettiva. ■

■ **Esempio 2.13** Definiamo la funzione *valore assoluto* in $\mathbb{Z}$ nel modo seguente

$$\begin{array}{rccc} |\,|: & \mathbb{Z} & \to & \mathbb{N} \\ & z & \mapsto & |z| = \begin{cases} z & \text{se } z \geq 0 \\ -z & \text{se } z < 0 \end{cases} \end{array}$$

la quale è suriettiva ma non iniettiva. Sia adesso $i_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ la funzione inclusione la quale è iniettiva ma non suriettiva. La composizione

$$\begin{array}{ccccc} \mathbb{N} & \xrightarrow{i_{\mathbb{N}}} & \mathbb{Z} & \xrightarrow{|\,|} & \mathbb{N} \\ n & \mapsto & n & \mapsto & |n| = n \end{array}$$

della funzione $i_{\mathbb{N}}$ seguita dalla funzione $|\,|$ restituisce la funzione identità, cioè $|\,|\circ i_{\mathbb{N}} = \mathrm{Id}_{\mathbb{N}}$. Quindi $|\,|\circ i_{\mathbb{N}}$ è sia iniettiva che suriettiva nonostante la funzione $i_{\mathbb{N}}$ non è suriettiva e la funzione $|\,|$ non è iniettiva. Questo esempio, come tanti altri facilmente costruibili, mostra che se la composizione di due funzioni è suriettiva (iniettiva) non si può concludere che le due funzioni composte siano entrambe suriettive (iniettive). ∎

2.3 Inversa destra e inversa sinistra

Prima di descrivere l'argomento di questo paragrafo introduciamo l'ultimo assioma della Teoria ZFC degli Insiemi, ovvero l'assioma della scelta.

Definizione 2.6 Sia I un insieme e sia $\mathscr{A} = \{A_i\}_{i\in I}$ una famiglia di insiemi, uno per ogni elemento $i \in I$. Una *funzione di scelta* è una funzione $\varphi : I \to \bigcup_{i\in I} A_i$ tale che $\varphi(i) \in A_i\ \forall i \in I$.

ZFC 1 — Assioma della Scelta. Sia $\mathscr{A} = \{A_i\}_{i\in I}$ una famiglia non vuota di insiemi non vuoti. Allora esiste una funzione di scelta.

Proposizione 2.3 Sia $f : X \to Y$ una funzione. Allora f è suriettiva se e solo se esiste una funzione $g : Y \to X$ iniettiva tale che $f \circ g = \mathrm{Id}_Y$.

Dimostrazione.
"⇐" Se esiste $g : Y \to X$ iniettiva tale che $f \circ g = \mathrm{Id}_Y$ allora dalla Proposizione 2.2–*(d)* f è suriettiva.
"⇒" Sia $f : X \to Y$ una funzione suriettiva e si consideri la famiglia di insiemi

$$\mathscr{A} = \{f^{-1}(y)\}_{y\in Y}$$

Essendo $Y \neq \varnothing$ esiste almeno un elemento $y \in Y$. Inoltre, dalla suriettività di f, segue che $f^{-1}(y) \neq \varnothing\ \forall y \in Y$. Quindi $\mathscr{A}$ è una famiglia non vuota di insiemi non vuoti. Dall'assioma della scelta esiste una funzione $\varphi : Y \to \bigcup_{y\in Y} f^{-1}(y) = X$ tale che $\varphi(y) \in f^{-1}(y)\ \forall y \in Y$. Possiamo quindi definire $g = \varphi$. Verifichiamo che $f \circ g = \mathrm{Id}_Y$. Infatti, se $y \in Y$, $f \circ g(y) = f(g(y))$ con $g(y) \in f^{-1}(y)$ e, per definizione di controimmagine, concludiamo che $f(g(y)) = y$, da cui $f \circ g = \mathrm{Id}_Y$. Infine, dalla Proposizione 2.2–*(c)*, essendo $f \circ g = \mathrm{Id}_Y$ iniettiva, segue che g è iniettiva. ∎

Proposizione 2.4 Sia $f : X \to Y$ una funzione. Allora f è iniettiva se e solo se esiste una funzione $g : Y \to X$ suriettiva tale che $g \circ f = \mathrm{Id}_X$.

Dimostrazione.
"⇐" Se esiste $g : Y \to X$ suriettiva tale che $g \circ f = \mathrm{Id}_X$ allora dalla Proposizione 2.2–*(c)* f è iniettiva.
"⇒" Sia $f : X \to Y$ una funzione iniettiva. Allora per ogni $y \in f(X) \subseteq Y$ esiste un unico $x \in X$ tale che $f(x) = y$. Siccome $X \neq \varnothing$ esiste un elemento $x_0 \in X$. Definiamo una funzione g nel modo seguente

$$\begin{array}{rccl} g: & Y & \to & X \\ & y & \mapsto & g(y) = \begin{cases} x & \text{se } y = f(x) \in f(X) \\ x_0 & \text{se } y \in Y \setminus f(X) \end{cases} \end{array}$$

Mostriamo che $g \circ f = \mathrm{Id}_X$. Se $x \in X$ si ha $g \circ f(x) = g(f(x)) = x$. Infine, dalla Proposizione 2.2–*(d)*, essendo $g \circ f = \mathrm{Id}_X$ suriettiva, segue che g è suriettiva.

∎

Osservazione 2.4 La funzione g nella Proposizione 2.3 si chiama una *inversa destra* della funzione suriettiva f, mentre la funzione g nella Proposizione 2.4 si chiama una *inversa sinistra*

della funzione iniettiva f. Si noti che né l'inversa destra che l'inversa sinistra sono, in genere, uniche.

Esercizio 2.3 Determinare due inverse destre della funzione valore assoluto $|\ |:\mathbb{Z}\to\mathbb{N}$ e due inverse sinistre della funzione inclusione $i_{\mathbb{N}}:\mathbb{N}\to\mathbb{Z}$.

■ **Esempio 2.14** Sia $f:\{a,b\}\to\{p,q,r\}$ la funzione definita da

$$f(a)=p,\quad f(b)=q.$$

Si considerino adesso le due funzioni $h_1,h_2:\{p,q,r\}\to\{p,q,r\}$ definite da

$$h_1(p)=p,\quad h_1(q)=q,\quad h_1(r)=r$$

$$h_2(p)=p,\quad h_2(q)=q,\quad h_2(r)=p.$$

Chiaramente $h_1\neq h_2$ mentre $h_1\circ f=h_2\circ f$. Quindi, la condizione $h_1\circ f=h_2\circ f$ non implica, almeno in questo esempio, che $h_1=h_2$. ■

L'esempio precedente suggerisce l'introduzione della seguente definizione.

Definizione 2.7 Siano X,Y,Z tre insiemi non vuoti.

(a) Una funzione $f:X\to Y$ è *cancellabile a destra* se

$$\forall\, h_1,h_2:Y\to Z\quad h_1\circ f=h_2\circ f\quad\Rightarrow\quad h_1=h_2$$

(b) Una funzione $f:X\to Y$ è *cancellabile a sinistra* se

$$\forall\, h_1,h_2:Z\to X\quad f\circ h_1=f\circ h_2\quad\Rightarrow\quad h_1=h_2$$

Proposizione 2.5

(a) Una funzione è cancellabile a destra se e solo se è suriettiva.

(b) Una funzione è cancellabile a sinistra se e solo se è iniettiva.

Dimostrazione.

(a) Dimostriamo le due implicazioni separatamente.

"$\Leftarrow$" Sia $f:X\to Y$ una funzione suriettiva. Supponiamo che $h_1\circ f=h_2\circ f$ con $h_1,h_2:Y\to Z$. Dobbiamo dimostrare che $h_1=h_2$, cioè che $h_1(y)=h_2(y)\ \forall y\in Y$. Sia quindi $y\in Y$, dalla suriettività di f esiste $x\in X$ con $f(x)=y$. Segue che $h_1\circ f(x)=h_2\circ f(x)\quad\Rightarrow\quad h_1(f(x))=h_2(f(x))\quad\Rightarrow\quad h_1(y)=h_2(y)$.

"$\Rightarrow$" Dimostriamo la contronominale: se $f:X\to Y$ è una funzione non suriettiva allora f non è cancellabile a destra. Se $f:X\to Y$ non è suriettiva esiste un elemento $y_0\in Y\setminus f(X)$. Per dimostrare che f non è cancellabile a destra costruiamo due funzioni $h_1,h_2:Y\to Y$ diverse tali che $h_1\circ f=h_2\circ f$. A tal scopo, sia $h_1=\mathrm{Id}_Y$ e sia h_2 la funzione così definita

$$h_2(y)=\begin{cases}y & \text{se } y\in f(X)\\ y' & \text{se } y\in Y\setminus f(X)\end{cases}$$

dove $y'\in f(X)$ è un fissato elemento dell'immagine di f. Mostriamo che $h_1\circ f=h_2\circ f$:

$$\forall x\in X\quad h_1\circ f(x)=h_1(f(x))=f(x)=h_2(f(x))=h_2\circ f(x)\,.$$

Tuttavia, $h_1(y_0) = y_0 \neq y' = h_2(y_0)$ e quindi $h_1 \neq h_2$.

(b) Dimostriamo le due implicazioni separatamente.

"$\Leftarrow$" Sia $f : X \to Y$ una funzione iniettiva. Supponiamo che $f \circ h_1 = f \circ h_2$ con $h_1, h_2 : Z \to X$. Dobbiamo dimostrare che $h_1 = h_2$, cioè che $h_1(z) = h_2(z)\ \forall z \in Z$. Sia $z \in Z$, si ha $f \circ h_1(z) = f \circ h_2(z) \quad \Rightarrow \quad f(h_1(z)) = f(h_2(z)) \xRightarrow{f \text{ iniettiva}} h_1(z) = h_2(z)$.

"$\Rightarrow$" Dimostriamo anche in questo caso la contronominale: se $f : X \to Y$ è una funzione non iniettiva allora f non è cancellabile a sinistra. Se $f : X \to Y$ non è iniettiva esistono due elementi $x_1, x_2 \in X, x_1 \neq x_2$, tali che $f(x_1) = f(x_2)$. Per dimostrare che f non è cancellabile a sinistra costruiamo due funzioni $h_1, h_2 : Z \to X$ distinte tali che $f \circ h_1 = f \circ h_2$. A tal scopo, scegliamo $Z = \{z\}$ un insieme formato da un solo elemento e definiamo

$$\begin{array}{rccc} h_1: & \{z\} & \to & X \\ & z & \mapsto & x_1 \end{array} \qquad \begin{array}{rccc} h_2: & \{z\} & \to & X \\ & z & \mapsto & x_2 \end{array}$$

Le funzioni h_1 e h_2 sono distinte per costruzione mentre $f \circ h_1(z) = f(h_1(z)) = f(x_1) = f(x_2) = f(h_2(z)) = f \circ h_2(z)$.

■

Definizione 2.8 Una funzione $f : X \to Y$ si dice *invertibile* se esiste una funzione $g : Y \to X$ tale che $g \circ f = \mathrm{Id}_X$ e $f \circ g = \mathrm{Id}_Y$.

Proposizione 2.6 Una funzione $f : X \to Y$ è invertibile se e solo se è biettiva. Inoltre la funzione $g : Y \to X$ è unica e si denota con f^{-1}.

Dimostrazione.

"$\Rightarrow$" Se f è invertibile esiste $g : Y \to X$ tale che $g \circ f = \mathrm{Id}_X$ e $f \circ g = \mathrm{Id}_Y$. Da $g \circ f = \mathrm{Id}_X$ segue che f è iniettiva mentre $f \circ g = \mathrm{Id}_Y$ implica che f è suriettiva.

"$\Leftarrow$" Sia $f : X \to Y$ biettiva. Allora per la suriettività di f per ogni $y \in Y$ esiste un $x \in X$ con $f(x) = y$ mentre per l'iniettività di f tale x è unico. Segue che la funzione

$$\begin{array}{rccc} g: & Y & \to & X \\ & y & \mapsto & \text{l'unico } x\text{: } f(x) = y \end{array}$$

è un'inversa di f. Dimostriamo adesso che l'inversa è unica. Se esistessero due inverse $g, g' : Y \to X$ si avrebbe $g' \circ f = \mathrm{Id}_X = g \circ f \xRightarrow{f \text{ suriettiva}} g' = g$. ■

■ **Esempio 2.15** La funzione

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & z & \mapsto & z-1 \end{array}$$

è biettiva (verificare). Per determinare la funzione inversa si scriva $z' = z - 1$ e si ricavi z in funzione di z'. Si ottiene $z = z' + 1$, segue che la funzione

$$\begin{array}{rccc} f^{-1}: & \mathbb{Z} & \to & \mathbb{Z} \\ & z & \mapsto & z+1 \end{array}$$

è l'inversa di f. ■

2.4 Problemi proposti

In questi problemi si utilizzeranno i numeri naturali, interi e razionali. Qui lo studente deve utilizzare le proprietà che già conosce di questi numeri.

Problema 2.1 Data la funzione $f : \mathbb{Z} \to \mathbb{N}$ definita da $f(x) = x^2$, si determini $f^{-1}(Y)$ nei seguenti casi:

- $Y = \{4\}$
- $Y = \{3,5,8\}$
- $Y = \{0,1,2,3\}$
- $Y = \{\text{numeri primi}\}$

Problema 2.2

- Una funzione $f : X \to Y$ è iniettiva se e solo se $\forall\, T \subseteq X$ si ha che $f(X \setminus T) \subseteq Y \setminus f(T)$.
- Una funzione $f : X \to Y$ è suriettiva se e solo se $\forall\, T \subseteq X$ si ha che $f(X \setminus T) \supseteq Y \setminus f(T)$.

Problema 2.3 Sia X un insieme e sia $\mathscr{P}(X)$ l'insieme delle parti. Dimostrare che la funzione $f : \mathscr{P}(X) \to \mathscr{P}(X)$ defina da $A \mapsto X \setminus A$ è biettiva.

Problema 2.4 Dimostrare che la funzione $f : \mathbb{N} \to \mathbb{Z}$ definita da

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari} \\ 0 & \text{se } n = 0 \end{cases}$$

è biettiva.

Problema 2.5 Dato un insieme X per ogni $A \in \mathscr{P}(X)$ definiamo la funzione caratteristica $\mathscr{X}_A : X \to \{0,1\}$ di A come

$$\mathscr{X}_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A\,. \end{cases}$$

- Dimostrare che valgono le seguenti:
  1. $\mathscr{X}_A = \mathscr{X}_B$ se e solo se $A = B$
  2. $\mathscr{X}_{A\cap B} = \mathscr{X}_A\,\mathscr{X}_B$
  3. $\mathscr{X}_{C(A)} = 1 - \mathscr{X}_A$
  4. $\mathscr{X}_{A\cup B} = \mathscr{X}_A + \mathscr{X}_B - \mathscr{X}_{A\cap B}$

- Dimostrare che

$$(*) \qquad \mathscr{X}_{A\Delta B} = \mathscr{X}_A + \mathscr{X}_B - 2\mathscr{X}_{A\cap B}$$

  dove Δ indica la differenza simmetrica.
- Usando la $(*)$ dimostrare che la differenza simmetrica gode della proproietà associativa.

Problema 2.6 Sia X un insieme non vuoto e sia Y un sottoinsime fissato di X. Definiamo un'applicazione $\varphi : P(X) \to P(X)$, ponendo, per ogni $A \in P(X) : \varphi(A) = A\Delta Y$. Dimostrare che $\varphi^2 = \varphi \circ \varphi = \mathrm{Id}$. Dedurre, argomentando, che φ è biettiva.

Problema 2.7 Sia $\mathbb{Q}$ l'insieme dei numeri razionali (per ora potete pensare $\mathbb{Q} = \{\frac{m}{n} : m,n \in \mathbb{Z}, n \neq 0\}$). Sia $f : \mathbb{Q} \to \mathbb{Q}$ l'applicazione definita da, per ogni $x \in \mathbb{Q}$,

$$f(x) = \frac{2x}{|x|+1}$$

Si dica se f è iniettiva e/o suriettiva.

Problema 2.8 Siano A,B e C insiemi non vuoti, e $f : A \to B$ una funzione fissata. Sia C^B l'insieme di tutte le funzioni da B in C, e C^A quello di tutte le funzioni da A in C. Sia $\varphi : C^B \to C^A$ l'applicazione definita da $\varphi(g) = g \circ f$ per ogni $g \in C^B$. Si provi che se f è suriettiva (iniettiva), allora φ è iniettiva (suriettiva).

Problema 2.9 Sia $f : A \to B$ una funzione, e siano $S, T \subseteq A$. Si provi che
(1) $f(S \cup T) = f(S) \cup f(T)$
(2) $f(S \cap T) \subseteq f(S) \cap f(T)$
(3) $f(S) \setminus f(T) \subseteq f(S \setminus T)$
e si mostri, mediante opportuni esempi che le inclusioni ai punti (2), (3) possono essere proprie.

Problema 2.10 Sia $f : A \to B$ una funzione. Si provi che f è iniettiva se e soltanto se $f(S \cap T) = f(S) \cap f(T)$ per ogni $S, T \subseteq A$

Problema 2.11 Sia $f : A \to B$ una funzione, e siano $S, T \subseteq B$. Si provi che
(1) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$
(2) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$
(3) $f^{-1}(S \setminus T) = f^{-1}(S) \setminus f^{-1}(T)$

Problema 2.12 Dimostrare che la composizione di funzioni gode della proprietà associativa.

Problema 2.13 Siano $f, g : \mathbb{N} \to \mathbb{N}$ definite da, per ogni $n \in \mathbb{N}$:

$$f(n) = \begin{cases} n+10 & \text{se } n \leq 9 \\ n-10 & \text{se } n \geq 10 \end{cases} \quad , \qquad g(n) = n+10$$

- Si descrivano le funzioni $f \circ g$ e $g \circ f$
- Si dica se esiste $h : \mathbb{N} \to \mathbb{N}$ tale che $h \circ f = \mathrm{Id}_{\mathbb{N}}$

Problema 2.14 Sia $f : \mathbb{Q} \to \mathbb{Q}$ definita da, per ogni $x \in \mathbb{Q}$, $f(x) = 2x - 1$. Verificare che f è biettiva e determinare la sua inversa.

Problema 2.15 Sia $f : \mathbb{Q} \setminus \{1\} \to \mathbb{Q} \setminus \{1\}$ definita da, per ogni $x \in \mathbb{Q} \setminus \{1\}$, $f(x) = (x+1)/(x-1)$. Verificare che f è biettiva e determinare la sua inversa.

Problema 2.16 Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni invertibili. Dimostrare che:

- f^{-1} è invertibile e $(f^{-1})^{-1} = f$
- $g \circ f$ è invertibile e $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

3. I numeri naturali

3.1 Costruzione dei numeri naturali

In questo capitolo introduciamo, facendo uso esclusivamente della teoria degli insiemi, i numeri naturali. Vi sono diversi modi per costruire i numeri naturali per via assiomatica. Qui faremo vedere che l'assioma dell'infinito garantisce l'esistenza dei numeri naturali.
Iniziamo con la seguente definizione

Definizione 3.1 Un *Sistema di Peano* è una terna (N,s,a) dove N è un insieme e tale che:
(P_1) $a \in N$
(P_2) $s : N \to N$ è una funzione
(P_3) $s(n) \neq a$ per ogni $n \in N$
(P_4) s è iniettiva
(P_5) se $E \subseteq N$ con $a \in E$ e $s(E) \subseteq E$ allora $E = N$

L'elemento a è di fatto unico. Infatti, sia $s(N) \subseteq N$ l'immagine di s e si consideri l'insieme $E = s(N) \cup \{a\}$. Allora $a \in E$ e, per costruzione, $s(E) \subseteq E$. Segue da (P_5) che $E = s(N) \cup \{a\} = N$ da cui $\{a\} = N \setminus s(N)$ risulta univocamente determinato. In pratica s è una funzione non suriettiva per la quale l'unico elemento che non appartiene all'immagine è a.

Proposizione 3.1 Esiste un sistema di Peano.

Dimostrazione. L'assioma dell'infinito **ZF** 6 garantisce che esiste un insieme X che ha $\varnothing$ come elemento e per ogni $x \in X$ anche il seguente $x \cup \{x\} \in X$. Indichiamo con

$$\mathscr{A} = \{A \in \mathscr{P}(X) : \varnothing \in A \text{ e } x \cup \{x\} \in A \ \forall x \in A\}$$

e sia

$$N = \bigcap_{A \in \mathscr{A}} A$$

L'insieme vuoto appartiene ad ogni $A \in \mathscr{A}$, quindi $\varnothing \in N$. Poiché il seguente di un elemento $x \in N$ appartiene ad N, possiamo definire la funzione

$$\begin{array}{rccc} s: & N & \to & N \\ & x & \mapsto & x \cup \{x\} \end{array}$$

Mostriamo che la terna (N,a,s), $a = \varnothing$, è un sistema di Peano. Attenzione che dimostreremo prima (P_5) e poi, utilizzando (P_5), (P_4).
(P_1) $a \in N$ per costruzione di N.

(P_2) $s : N \to N$ è una funzione.
(P_3) $\forall x \in N\ s(x) = x \cup \{x\} \neq \varnothing$ quindi $a = \varnothing$ non appartiene all'immagine di s.
(P_5) Sia $E \subseteq N$ con $a \in E$ e $s(E) \subseteq E$, cioè per ogni $x \in E$ si ha che $x \cup \{x\} \in E$. Allora E soddisfa l'assioma dell'infinito da cui $E \in \mathscr{A}$. Essendo $N = \bigcap_{A \in \mathscr{A}} A$ segue che $N \subseteq A\ \forall A \in \mathscr{A}$, in particolare $N \subseteq E$.
(P_4) Sia

$$S = \{y \in N : x \in y \quad \Rightarrow \quad x \subseteq y\} \subseteq N$$

Allora $\varnothing \in S$, inoltre se $y \in S$ anche $s(y) \in S$. Infatti, se $x \in y \cup \{y\}$ si ha $x = y \vee x \in y$. Se $x = y$ allora $x \subseteq y \cup \{y\}$. Mentre se $x \in y$ si trova, poiché $y \in S, x \subseteq y \subseteq y \cup \{y\}$. Segue da ($P_5$) che $S = N$.
Mostriamo adesso che s è iniettiva. Se $s(x) = s(y)$ allora $x \cup \{x\} = y \cup \{y\}$ e si presentano due casi

$$x = y \quad \vee \quad (x \in y \wedge y \in x).$$

Se $x = y$ abbiamo finito. Se $x \neq y$, allora $x \in y \wedge y \in x$ da cui segue, poiché $S = N$, che $x \subseteq y \wedge y \subseteq x$ la quale conduce all'assurdo $x = y$.

■

! In alcuni testi invece di invocare l'assioma dell'infinito si assume l'esistenza di un sistema di Peano come assioma.

Appurato che esiste almeno un sistema di Peano ci si chiede se è possibile costruire più sistemi di Peano che siano fondamentalmente distinti. In realtà un sistema di Peano è, in qualche modo, unico, come mostra la seguente proposizione

Proposizione 3.2 Siano (N, s, a) e (N', s', a') due sistemi di Peano. Allora esiste una biezione $f : N \to N'$ tale che
(a) $a' = f(a)$
(b) $\forall x \in N \quad f(s(x)) = s'(f(x))$

Dimostrazione. Si rimanda al libro di testo. ■

Una funzione f che soddisfa (a), (b) della Proposizione 3.2 si chiama *isomorfismo di sistemi di Peano*. Quindi, a meno di isomorfismi di sistemi di Peano, un sistema di Peano è unico.

Definizione 3.2 Denotiamo con $\mathbb{N}$ l'insieme N dell'unico sistema di Peano (N, a, s) e lo chiamiamo insieme dei *numeri naturali*. Poniamo

$$0 = a \qquad 1 = s(a) = s(0) \qquad 2 = s(1) \qquad 3 = s(2) \quad \cdots$$

La funzione s si chiama *funzione successore*.

Ci sono proposizioni il cui enunciato dipende da un numero naturale. Ad esempio: $2n$ *è un numero pari per ogni* $n \in \mathbb{N}$. Per dimostrare che tali proposizioni sono vere per tutti i numeri naturali non è sufficiente far vedere che sono vere per i primi 10 o 100 numeri naturali. Non è neanche possibile verificarle per tutti i numeri naturali poiché dato un numero naturale n, $s(n)$ è un altro numero naturale diverso dai precedenti e così via. Il metodo dimostrativo che si utilizza si basa sul seguente principio di induzione.

Proposizione 3.3 — Induzione debole. Sia $P(n)$ una proposizione che dipende da un numero naturale $n \in \mathbb{N}$. Supponiamo di aver dimostrato che
(a) $P(0)$ è vera;
(b) se $P(n)$ è vera allora $P(s(n))$ è vera.

Allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Dimostrazione. Sia $E = \{n \in \mathbb{N} : P(n) \text{ è vera}\}$. Allora (a) implica che $0 \in E$ mentre (b) garantisce che $s(E) \subseteq E$. Segue da (P_5) che $E = \mathbb{N}$ e quindi $P(n)$ è vera per ogni $n \in \mathbb{N}$. ■

Lo stesso principio di induzione si può utilizzare per formulare una *definizione per induzione* secondo il seguente schema

Si vuole definire l'espressione $D(n)$.
Passo 1. Si definisce $D(0)$.
Passo 2. Supponendo che $D(n)$ sia definita si definisce $D(s(n))$.
Segue, sempre per (P_5), che $D(n)$ è definita per ogni $n \in \mathbb{N}$.

Definizione 3.3 — Potenza di una funzione. Sia $f : X \to X$ una funzione. Definiamo la potenza di f, f^n, per induzione su n nel modo seguente:
Poniamo $f^0 = \mathrm{Id}_X$.
Se f^n è definita poniamo $f^{s(n)} = f \circ f^n$.

▪ **Esempio 3.1** Dimostriamo per induzione che $s^n(0) = n$ per ogni $n \in \mathbb{N}$.
Passo 1. Per $n = 0 \quad s^0(0) = \mathrm{Id}_{\mathbb{N}}(0) = 0 \quad$ quindi verificata;
Passo 2. Supponiamo che sia vera per n, cioè che $s^n(0) = n$ e dimostriamo la proposizione per $s(n)$. Per definizione di potenza di funzione si ha $s^{s(n)}(0) = s \circ s^n(0) = s(s^n(0)) \overset{\text{ip.ind.}}{=} s(n)$.
■

▪ **Esempio 3.2** Dimostriamo per induzione che $s \circ s^n = s^n \circ s$ per ogni $n \in \mathbb{N}$.
Passo 1. Per $n = 0 \quad s \circ s^0 = s \circ \mathrm{Id}_{\mathbb{N}} = s = \mathrm{Id}_{\mathbb{N}} \circ s = s^0 \circ s \quad$ quindi verificata;
Passo 2. Supponiamo che sia vera per n, cioè che $s \circ s^n = s^n \circ s$ e dimostriamo la proposizione per $s(n)$. Per definizione di potenza di funzione ed usando che la composizione di funzioni gode della proprietà associativa (Problema 2.12) si ha

$$s^{s(n)} \circ s = (s \circ s^n) \circ s = s \circ (s^n \circ s) \overset{\text{ip.ind.}}{=} s \circ (s \circ s^n) = s \circ s^{s(n)}.$$

■

3.2 Operazioni nei numeri naturali

Definizione 3.4 — Operazione di somma. L'operazione di *somma* in $\mathbb{N}$ è un'operazione binaria, cioè una funzione $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definita nel modo seguente:

$$(m,n) \mapsto m+n = s^n(m).$$

Quindi $m+0 = s^0(m) = \mathrm{Id}_{\mathbb{N}}(m) = m$ mentre $m+1 = s(m)$.

Proposizione 3.4 Valgono le seguenti proprietà, $\forall m,n,k \in \mathbb{N}$,

(a) $s(m+n) = s(m)+n$;
(b) $s(m+n) = m+s(n)$;
(c) $0+n = n$;
(d) $m+(n+k) = (m+n)+k$ (associativa)
(e) $m+n = n+m$ (commutativa)
(f) $m+k = n+k \quad \Rightarrow \quad m = n$ (legge di cancellazione)

Dimostrazione.

(a) $\quad s(m+n) \overset{\text{def. somma}}{=} s(s^n(m)) = s \circ s^n(m) \overset{\text{Esempio 3.2}}{=} s^n \circ s(m) = s^n(s(m)) = s(m)+n.$

(b) $s(m+n) \overset{\text{def. somma}}{=} s(s^n(m)) = s \circ s^n(m) \overset{\text{def. potenza}}{=} s^{s(n)}(m) = m + s(n)$.

(c) $0+n \overset{\text{def. somma}}{=} s^n(0) \overset{\text{Esempio 3.1}}{=} n$.

(d) Fissiamo n e k e dimostriamola per induzione su m (il lettore dovrebbe poi dimostrarla per induzione su n fissando m e k).

Passo 1. Per $m = 0$

$$0 + (n+k) \overset{(c)}{=} n+k \quad \wedge \quad (0+n)+k \overset{(c)}{=} n+k$$

quindi verificata.

Passo 2. Supponiamo che sia vera per m, cioè che

$$m + (n+k) = (m+n)+k$$

e dimostriamo la proposizione per $s(m)$. Si ha

$$s(m) + (n+k) \overset{(a)}{=} s(m+(n+k)) \overset{\text{ip.ind.}}{=} s((m+n)+k) \overset{(a)}{=} s(m+n)+k \overset{(a)}{=} (s(m)+n)+k.$$

(e) Fissiamo n e dimostriamola per induzione su m.

Passo 1. Per $m = 0$: $\quad 0+n \overset{(c)}{=} n \quad \wedge \quad n+0 = n$ quindi verificata;

Passo 2. Supponiamo che sia vera per m, cioè che

$$m+n = n+m$$

e dimostriamo la proposizione per $s(m)$. Si ha

$$s(m)+n \overset{(a)}{=} s(m+n) \overset{\text{ip.ind.}}{=} s(n+m) \overset{(b)}{=} n+s(m).$$

(f) $m+k = n+k \overset{\text{def. somma}}{\Rightarrow} s^k(m) = s^k(n) \overset{s^k \text{ iniettiva}}{\Rightarrow} m = n$. ■

Esercizio 3.1 Dimostrare che, $\forall m, n \in \mathbb{N}$,

$$m+n = 0 \quad \Leftrightarrow \quad m = 0 \quad \wedge \quad n = 0\,.$$

Osservazione 3.1 Utilizzando le proprietà dei numeri naturali, se $a_1, a_2, \ldots, a_n$ sono dei numeri naturali ha senso considerare somme del tipo

$$a_1 + a_2 + \cdots + a_n$$

che sintetizziamo con la scrittura

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

Definizione 3.5 Un numero $n \in \mathbb{N}$ si dice:
(a) *pari* se esiste $k \in \mathbb{N}$ con $n = s^k(k) = k+k$;
(b) *dispari* se esiste $k \in \mathbb{N}$ con $n = s^{s(k)}(k) = k + s(k)$.

Definizione 3.6 — Operazione di prodotto. L'operazione di *prodotto* in $\mathbb{N}$ è un'operazione binaria

$$\begin{array}{rccc} \cdot : & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ & (m,n) & \mapsto & m\cdot n \end{array}$$

definita per induzione su m nel modo seguente:

$0\cdot n = 0$

se $m\cdot n$ è definito $\quad\Rightarrow\quad s(m)\cdot n = m\cdot n + n$.

Esercizio 3.2 Dimostrare per induzione su $m\in\mathbb{N}$ che,

$$m\cdot s(n) = m\cdot n + m\,.$$

Proposizione 3.5 Valgono le seguenti proprietà, $\forall m,n,k\in\mathbb{N}$,

(a) $m\cdot 0 = 0$

(b) $m\cdot n = 0 \quad\Leftrightarrow\quad m=0 \quad\vee\quad n=0$

(c) $m\cdot(n+k) = m\cdot n + m\cdot k$ (distributiva)

(d) $m\cdot(n\cdot k) = (m\cdot n)\cdot k$ (associativa)

(e) $m\cdot n = n\cdot m$ (commutativa)

Dimostrazione.

(a) Esercizio per induzione su m.

(b) Chiaramente $m=0\vee n=0 \quad\Rightarrow\quad m\cdot n=0$. Dimostriamo il viceversa. Sia $m\cdot n=0$ e supponiamo che $m\neq 0\wedge n\neq 0$. Allora $m=s(m')$ per qualche $m'\in\mathbb{N}$ e $0=m\cdot n=s(m')\cdot n=m'\cdot n+n$. Segue, dall'Esercizio 3.1, che $m'\cdot n=0\wedge n=0$ contro l'ipotesi che $n\neq 0$.

(c) Fissiamo n e k e dimostriamola per induzione su m (il lettore dovrebbe poi dimostrarla per induzione su n fissando m e k).

Passo 1. Per $m=0$

$$0\cdot(n+k) = 0 \quad\wedge\quad (0\cdot n)+(0\cdot k) = 0+0 = 0$$

quindi verificata;

Passo 2. Supponiamo che sia vera per m, cioè che

$$m\cdot(n+k) = m\cdot n + m\cdot k$$

e dimostriamo la proposizione per $s(m)$. Si ha

$$\begin{array}{rcl} s(m)\cdot(n+k) & \overset{\text{def.prod.}}{=} & m\cdot(n+k)+(n+k) \overset{\text{ip.ind.}}{=} m\cdot n+m\cdot k+(n+k) \\ & = & m\cdot n+n+m\cdot k+k = s(m)\cdot n+s(m)\cdot k. \end{array}$$

(d) Esercizio per induzione.

(e) Fissiamo n e dimostriamola per induzione su m.

Passo 1. Per $m=0 \quad 0\cdot n=0 \quad\wedge\quad n\cdot 0=0$ quindi verificata;

Passo 2. Supponiamo che sia vera per m, cioè che $m\cdot n=n\cdot m$ e dimostriamo la proposizione per $s(m)$. Si ha

$$s(m)\cdot n \overset{\text{def.prod.}}{=} m\cdot n+n \overset{\text{ip.ind.}}{=} n\cdot m+n \overset{\text{Esercizio 3.2}}{=} n\cdot s(m).$$

■

Definizione 3.7 — Relazione d'ordine. Siano $m,n \in \mathbb{N}$. Diciamo che $m \leq n$ se esiste un $k \in \mathbb{N}$ tale che $n = m+k$. Se $k \neq 0$ diciamo che $m < n$.

Si noti che $n < s(n) \quad \forall n \in \mathbb{N}$.

Proposizione 3.6 La relazione d'ordine $\leq$ definita su $\mathbb{N}$ soddisfa le seguenti proprietà, $\forall m,n,k \in \mathbb{N}$,

(a) $m \leq m$ (riflessiva)
(b) $m \leq n \quad \wedge \quad n \leq m \quad \Leftrightarrow \quad m = n$ (antisimmetrica)
(c) $m \leq n \quad \wedge \quad n \leq k \quad \Rightarrow \quad m \leq k$ (transitiva)
(d) $m \leq n \quad \vee \quad n \leq m$ (dicotomia)
(e) $m \leq n \quad \Leftrightarrow \quad m+k \leq n+k$
(f) $m \leq n \quad \Rightarrow \quad m \cdot k \leq n \cdot k$

Dimostrazione.

(a) $\forall m \in \mathbb{N} \quad m = m+0 \quad \Rightarrow \quad m \leq m$.

(b) se $m = n$ allora dalla riflessiva si ha l'implicazione "$\Leftarrow$". Viceversa

$$m \leq n \quad \wedge \quad n \leq m \quad \Rightarrow \quad \exists\, k,q \in \mathbb{N} \colon n = m+k \quad \wedge \quad m = n+q\,.$$

Segue che

$$m+n = m+n+k+q \quad \Rightarrow \quad k+q = 0 \overset{\text{Esercizio 3.1}}{\Rightarrow} k = 0 \quad \wedge \quad q = 0 \quad \Rightarrow \quad m = n\,.$$

(c) $m \leq n \quad \wedge \quad n \leq k \quad \Rightarrow \quad \exists\, q,r \in \mathbb{N} \colon n = m+q \quad \wedge \quad k = n+r$. Segue che

$$k = m+(q+r) \quad \Rightarrow \quad m \leq k\,.$$

(d) Bisogna dimostrare che per ogni coppia di numeri naturali m,n si ha che

$$m \leq n \quad \vee \quad n \leq m\,.$$

Fissiamo n e dimostriamola per induzione su m.

Passo 1. Per $m = 0 \quad n = 0+n \quad \Rightarrow \quad 0 \leq n \quad \forall n \in \mathbb{N}$, quindi verificata;

Passo 2. Supponiamo che sia vera per m, cioè che $m \leq n \quad \vee \quad n \leq m$ e dimostriamo la proposizione per $s(m)$. Distinguiamo due casi.

Caso 1. Se $m \leq n \quad \Rightarrow \quad n = m+k$. Ci sono due sotto casi

- Se $k = 0 \quad \Rightarrow \quad n = m \quad \Rightarrow \quad s(n) = s(m) \quad \Rightarrow \quad n < s(n) = s(m)$.
- Se $k \neq 0 \quad \Rightarrow \quad k = s(k') \quad \Rightarrow \quad n = m+s(k') = s(m)+k' \quad \Rightarrow \quad s(m) \leq n$.

Caso 2. Se $n \leq m \quad \Rightarrow \quad n \leq m < s(m)$.

(e) Esercizio.

(f) Esercizio.

■

Da ora in poi non useremo più la notazione $m \cdot n$ ma scriveremo semplicemente mn.

Osservazione 3.2 Se $n \leq m$ allora esiste $k \in \mathbb{N}$ con $m = n+k$. Poniamo, per definizione, $m-n = k$.

Osservazione 3.3 Può accadere che una proposizione sia vera per tutti i numeri naturali maggiori o uguali di un dato numero naturale n_0. In tali condizioni il principio di induzione diventa

Sia $n_0 \in \mathbb{N}$ e sia $P(n)$ una proposizione che soddisfa alle seguenti due condizioni:
(a) $P(n_0)$ è vera;
(b) se per $n \geq n_0$ $P(n)$ è vera $\Rightarrow$ $P(n+1)$ è vera.
Allora $P(n)$ è vera per ogni $n \geq n_0$.

Per convincersi basta applicare l'induzione alla proposizione $P(n+n_0)$.

3.3 Problemi proposti

Problema 3.1 Siano $m,n \in \mathbb{N}$. Dimostrare che se $m < n$ allora $m+1 \leq n$.
Problema 3.2 Dimostrare per induzione che $\sum_{i=1}^{n} 1 = n$.
Problema 3.3 Dimostrare che in $\mathbb{N}$ vale la seguente equivalenza: $mn = 1 \quad \Leftrightarrow \quad m = n = 1$.
Problema 3.4 Sia $k \in \mathbb{N}$, $k \neq 0$. Dimostrare che per ogni $m,n \in \mathbb{N}$ si ha

$$mk = nk \quad \Leftrightarrow \quad m = n.$$

Problema 3.5 Sia $k \in \mathbb{N}$, $k \neq 0$. Dimostrare che per ogni $m,n \in \mathbb{N}$ si ha

$$mk \leq nk \quad \Rightarrow \quad m \leq n.$$

Problema 3.6 Definiamo per induzione la potenza di un numero naturale:

$$\textit{se } m \in \mathbb{N} \textit{ poniamo } m^0 = 1 \quad \wedge \quad m^{s(n)} = m m^n$$

Dimostrare che valgono le seguenti proprietà della potenza
1. $m^n m^k = m^{n+k}$
2. $m^n k^n = (mk)^n$

Problema 3.7 Usando il principio di induzione mostrare le seguenti asserzioni. In questo esercizio dovete utilizzare le proprietà dei numeri razionali e reali che conoscete dalle superiori.
1. $$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$
2. $$\sum_{i=1}^{n} (2i-1) = n^2$$
3. $$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$
4. $$\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$$
5. $$\sum_{i=1}^{n} i\, q^{i-1} = \frac{nq^{n+1} - (n+1)q^n + 1}{(1-q)^2}$$
   con $q \neq 1$ numero reale.
6. Se $x > -1$ allora
   $$(1+x)^n \geq 1 + nx$$
7. $$n! \geq 2^{n-1}$$

8.
$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

9.
$$\sum_{i=0}^{n} q^i = \frac{1-q^{n+1}}{1-q}$$

Problema 3.8 Come conseguenza delle proprietà della somma e del prodotto di numeri naturali si dimostrino (per induzione) le seguenti utili formule relative alle sommatorie dove $k, m, n \in \mathbb{N}$ mentre c, a_k, b_k sono per ora numeri naturali ma tenete presente che in seguito, quando saranno definiti, potranno essere numeri reali qualsiasi:

$$\begin{aligned}
&\text{(i)} && \sum_{k=1}^{n}(c \cdot a_k) = c \cdot \sum_{k=1}^{n} a_k \\
&\text{(ii)} && \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k = \sum_{k=1}^{n}(a_k + b_k) \\
&\text{(iii)} && \sum_{k=1}^{n} a_k + \sum_{k=n+1}^{n+m} a_k = \sum_{k=1}^{n+m} a_k \\
&\text{(iv)} && \sum_{k=1}^{n} a_k = \sum_{k=1+m}^{n+m} a_{k-m} \\
&\text{(v)} && \sum_{k=1}^{n} c = c \cdot n \\
&\text{(vi)} && \sum_{k=1}^{n} a_k = \sum_{k=1}^{n} a_{n-k+1} = \sum_{k=0}^{n-1} a_{n-k}\,.
\end{aligned} \tag{3.1}$$

Problema 3.9 Dimostrare, utilizzando le formule (3.1), che:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,.$$

Problema 3.10 Dire se sia possibile dimostrare per induzione che il numero $n^2 + n + 17$ è primo per ogni $n \in \mathbb{N}$.

4. Insiemi finiti e insiemi infiniti

4.1 Insiemi finiti

Sia $n \in \mathbb{N}$ un numero naturale e sia $\xi(n) = \{1,2,3,\ldots,n\}$ l'insieme dei numeri naturali da 1 sino ad n. Iniziamo il capitolo con la seguente proposizione.

Proposizione 4.1 — Principio di Dirichlet. Se $m \neq n$, allora non esiste una biezione tra $\xi(m)$ e $\xi(n)$.

Dimostrazione. Se $m \neq n$ possiamo assumere, senza ledere la generalità, che $n < m$. Dimostriamo che non esiste una funzione iniettiva da $\xi(m)$ in $\xi(n)$ da cui la tesi della proposizione. Prima di procedere osserviamo che è sufficiente mostrare che non esiste una funzione iniettiva da $\xi(n+1)$ in $\xi(n)$. Infatti, supponiamo che non esista una iniettiva da $\xi(n+1)$ in $\xi(n)$ e supponiamo, invece, che esista una iniettiva da $\xi(m)$ in $\xi(n)$. Essendo $n < m$, segue che $n+1 \leq m$ (si veda il Problema 3.1) da cui $\xi(n+1) \subseteq \xi(m)$, ed essendo la restrizione di una funzione iniettiva una funzione iniettiva si avrebbe una funzione iniettiva da $\xi(n+1)$ in $\xi(n)$ contro l'ipotesi.

Dimostriamo quindi che non esiste una funzione iniettiva da $\xi(n+1)$ in $\xi(n)$ per induzione su n. Se $n = 1$, $\xi(2) = \{1,2\}$, $\xi(1) = \{1\}$ e l'unica funzione da $\xi(2)$ in $\xi(1)$ è la funzione costante che non è iniettiva. Supponiamo adesso che non esista una funzione iniettiva da $\xi(n+1)$ in $\xi(n)$ e dimostriamo che non esiste una funzione iniettiva da $\xi(n+2)$ in $\xi(n+1)$. Supponiamo, per assurdo, che esista una funzione iniettiva $f : \xi(n+2) \to \xi(n+1)$ e sia $k \in \xi(n+1)$, tale che $f(n+2) = k$. Consideriamo la seguente funzione

$$
\begin{array}{rccc}
g: & \xi(n+1) & \to & \xi(n+1) \\
 & i & \longmapsto & g(i) = \begin{cases} i & \text{se } i \neq k, n+1 \\ n+1 & \text{se } i = k \\ k & \text{se } i = n+1 \end{cases}
\end{array}
$$

Chiaramente g è una funzione biettiva da cui la funzione $\bar{f} = g \circ f : \xi(n+2) \to \xi(n+1)$ è iniettiva. Inoltre $\bar{f}(n+2) = g \circ f(n+2) = g(f(n+2)) = g(k) = n+1$. Segue che la funzione $\bar{f}$ può essere ristretta a $\xi(n+1)$ per ottenere una funzione (restringendo anche il codominio a $\xi(n)$) iniettiva da $\xi(n+1)$ in $\xi(n)$ contro l'ipotesi induttiva.

■

Siamo nella giusta posizione per dare la definizione di insieme finito.

Definizione 4.1 Sia X un insieme. Diciamo che X è *finito* se:
$X = \varnothing$
oppure
$X \neq \varnothing$ ed esiste un numero naturale $n \in \mathbb{N}$ ed una biezione tra $\xi(n)$ e X.

Chiamiamo il numero n la *cardinalità* dell'insieme finito X e la indichiamo con $|X| = n$. Se $X = \varnothing$ poniamo $|X| = 0$.

Osservazione 4.1
1. Per il Principio di Dirichlet, il numero n nella definizione di insieme finito è unico.
2. Ovviamente se un insieme Y è in biezione con un altro insieme finito X allora anch'esso è finito con $|Y| = |X|$.

Proposizione 4.2 Sia X un insieme finito.
(a) Se $Y \subseteq X$, allora Y è finito e $|Y| \leq |X|$.
(b) Se $f : X \to Z$ è suriettiva, allora Z è finito e $|Z| \leq |X|$.

Dimostrazione.

(a) Per induzione su $n = |X|$. Se $n = 0$ allora $X = \varnothing$ e l'unico sottoinsieme di X è $Y = \varnothing$ da cui Y è finito e $|Y| = 0 = |X|$. Supponiamo adesso che la proposizione sia vera quando $|X| = n$ e dimostriamo che è vera quando $|X| = n+1$. Sia $x_0 \in X$ un suo elemento e poniamo $X = (X \setminus \{x_0\}) \cup \{x_0\}$. Sia adesso $Y \subseteq X$ e distinguiamo due casi.
Caso 1. $x_0 \notin Y$. Allora $Y \subseteq X \setminus \{x_0\}$ con $|X \setminus \{x_0\}| = n$. Dall'ipotesi induttiva Y è finito e $|Y| \leq n \leq n+1$.
Caso 2. $x_0 \in Y$. Allora $Y = Y' \cup \{x_0\}$ con $Y' \subseteq X \setminus \{x_0\}$. Sempre dall'ipotesi induttiva segue che Y' è finito e $|Y'| \leq n$. Esiste quindi una biezione $f : \xi(m) \to Y'$ con $m \leq n$. Si consideri la funzione

$$g: \begin{array}{ccc} \xi(m+1) & \to & Y \\ i & \mapsto & g(i) = \begin{cases} f(i) & \text{se } i \neq m+1 \\ x_0 & \text{se } i = m+1 \end{cases} \end{array}$$

La funzione g è chiaramente biettiva da cui segue che Y è finito, inoltre $|Y| = m+1 \leq n+1$.

(b) Sia $f : X \to Z$ suriettiva, allora, per la Proposizione 2.3, esiste una funzione iniettiva $g : Z \to X$. Consideriamo la funzione biettiva $\tilde{g} : Z \to g(Z)$ definita da $\tilde{g}(z) = g(z)\ \forall z \in Z$. Poiché $g(Z) \subseteq X$ e X è finito segue dal punto (a) che $g(Z)$ è finito e $|g(Z)| \leq |X|$. Infine, poiché $\tilde{g} : Z \to g(Z)$ è una biezione anche Z è finito e $|Z| = |g(Z)| \leq |X|$. ■

Proposizione 4.3 Siano X e Y due insiemi finiti. Allora
(a) $|X \cup Y| = |X| + |Y| - |X \cap Y|$;
(b) $|X \times Y| = |X||Y|$;
(c) $|\mathscr{P}(X)| = 2^{|X|}$.

Dimostrazione.

(a) Dato un insieme X per ogni $A \in \mathscr{P}(X)$ abbiamo definito la funzione caratteristica $\mathscr{X}_A : X \to \{0,1\}$ di A come

$$\mathscr{X}_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A\,. \end{cases}$$

Nel Problema 2.5 è stato richiesto di verificare, per $A, B \subseteq X$, la seguente identità:

$$\mathscr{X}_{A\cup B} = \mathscr{X}_A + \mathscr{X}_B - \mathscr{X}_{A\cap B}.$$

Inoltre, se A è finito, usando che $\sum_{i=1}^{n} 1 = n$, si perviene all'utile identità $|A| = \sum_{a\in A} \mathscr{X}_A(a)$. Segue che, se consideriamo X, Y come sottoinsiemi di $X \cup Y$,

$$\begin{aligned} |X \cup Y| &= \sum_{x\in X\cup Y} \mathscr{X}_{X\cup Y}(x) = \sum_{x\in X\cup Y} (\mathscr{X}_X(x) + \mathscr{X}_Y(x) - \mathscr{X}_{X\cap Y}(x)) \\ &= \sum_{x\in X\cup Y} \mathscr{X}_X(x) + \sum_{x\in X\cup Y} \mathscr{X}_Y(x) - \sum_{x\in X\cup Y} \mathscr{X}_{X\cap Y}(x) \\ &= \sum_{x\in X} \mathscr{X}_X(x) + \sum_{x\in Y} \mathscr{X}_Y(x) - \sum_{x\in X\cap Y} \mathscr{X}_{X\cap Y}(x) \\ &= |X| + |Y| - |X \cap Y|. \end{aligned}$$

(b) Sia $|X| = m$, $|Y| = n$ e dimostriamo la proposizione per induzione su m con n fissato. Se $m = 0$ allora $X = \varnothing \quad \wedge \quad X \times Y = \varnothing$ da cui $|X \times Y| = 0 \quad \wedge \quad |X||Y| = 0 \cdot n = 0$, quindi è vera. Se $m = 1$ si osservi che $\{x\} \times Y$ è in corrispondenza biunivoca con Y (si costruisca una biezione). Quindi $|\{x\} \times Y| = |Y| = n = 1 \cdot n$ da cui la proposizione è verificata anche per $m = 1$. Supponiamo adesso che, quando $|X| = m$, valga

$$|X \times Y| = |X||Y| = m \cdot n$$

e dimostriamo che la stessa vale quando $|X| = m + 1$. Sia $x_0 \in X$ e si scriva

$$X = (X \setminus \{x_0\}) \cup \{x_0\} = X' \cup \{x_0\}$$

dove $|X'| = m$. Tenendo in considerazione l'Esercizio 1.4, segue che

$$X \times Y = \big(X' \cup \{x_0\}\big) \times Y = (X' \times Y) \cup (\{x_0\} \times Y).$$

Inoltre,

$$(X' \times Y) \cap (\{x_0\} \times Y) = (X' \cap \{x_0\}) \times Y = \varnothing \times Y = \varnothing.$$

Applicando il punto (a) si trova

$$|X \times Y| = |(X' \times Y) \cup (\{x_0\} \times Y)| = |(X' \times Y)| + |(\{x_0\} \times Y)| = mn + n = (m+1)n.$$

(c) Sia $|X| = n$ e dimostriamo la proposizione per induzione su n. Se $n = 0$ allora $X = \varnothing$ e $\mathscr{P}(X) = \mathscr{P}(\varnothing) = \{\varnothing\}$. Segue che $|\mathscr{P}(X)| = 1 = 2^0$ quindi la proposizione è vera per $n = 0$. Supponiamo che se $|X| = n$ allora $|\mathscr{P}(X)| = 2^n$ e dimostriamo la proposizione quando $|X| = n + 1$. Sia $x_0 \in X$ e si scriva $X = (X \setminus \{x_0\}) \cup \{x_0\} = X' \cup \{x_0\}$ dove $|X'| = n$. Sia adesso $Y \subseteq X$. Ci sono due casi: $x_0 \notin Y$ e $Y \subseteq X'$ oppure $x_0 \in Y$ e $Y = Y' \cup \{x_0\}$ con $Y' \subseteq X'$. L'insieme delle parti di X si può quindi descrivere come

$$\mathscr{P}(X) = \{Y \subseteq X : Y \subseteq X'\} \cup \{Y = Y' \cup \{x_0\} : Y' \subseteq X'\}.$$

Ovviamente

$$\{Y \subseteq X : Y \subseteq X'\} \cap \{Y = Y' \cup \{x_0\} : Y' \subseteq X'\} = \varnothing.$$

Infatti, essendo un elemento del primo insieme un sottoinsieme di X che non contiene x_0 ed essendo un elemento del secondo insieme un sottoinsieme di X che contiene x_0, non possono esserci elementi in comune. Applicando (a) si trova

$$\begin{aligned} |\mathscr{P}(X)| &= |\{Y \subseteq X : Y \subseteq X'\}| + |\{Y = Y' \cup \{x_0\} : Y' \subseteq X'\}| \\ &= |\mathscr{P}(X')| + |\mathscr{P}(X')| = 2^n + 2^n = 2^{n+1}. \end{aligned}$$

■

Esercizio 4.1 Nella Proposizione 4.3 ci siamo posti il problema di calcolare le cardinalità dell'unione, del prodotto cartesiano e dell'insieme potenza di insiemi finiti senza porci la domanda se fossero realmente finiti. È un utile esercizio dimostrare, prioritariamente, che se X e Y sono due insiemi finiti allora sono finiti $X \cup Y$, $X \times Y$ e $\mathscr{P}(X)$.

Proposizione 4.4 Sia X un insieme finito. Allora una funzione $f : X \to X$ è iniettiva se e solo se è suriettiva.

Dimostrazione.
"$\Rightarrow$" Sia $f : X \to X$ iniettiva. Dimostriamo che $X \subseteq f(X)$. Siccome $f : X \to X$ è iniettiva esiste una biezione $X \leftrightarrow f(X)$ da cui $|f(X)| = |X|$. Inoltre $X = f(X) \cup (X \setminus f(X))$ e $f(X) \cap (X \setminus f(X)) = \varnothing$. Segue, dalla Proposizione 4.3, che $|X| = |f(X)| + |X \setminus f(X)| = |X| + |X \setminus f(X)| \quad \Rightarrow \quad |X \setminus f(X)| = 0 \quad \Rightarrow \quad X \setminus f(X) = \varnothing \quad \Rightarrow \quad X \subseteq f(X)$. Quindi $X = f(X)$ e f è suriettiva.

"$\Leftarrow$" Sia $f : X \to X$ suriettiva. Allora, dalla Proposizione 2.3, esiste una funzione $g : X \to X$ iniettiva tale che $f \circ g = \mathrm{Id}_X$. Dall'implicazione "$\Rightarrow$" la funzione g è biettiva e quindi esiste l'inversa g^{-1}. Componendo con g^{-1} a destra di $f \circ g = \mathrm{Id}_X$ si trova $f \circ g \circ g^{-1} = \mathrm{Id}_X \circ g^{-1} \quad \Rightarrow \quad f = g^{-1} \quad \Rightarrow \quad f$ è biettiva ed in particolare iniettiva. ■

4.2 Insiemi infiniti

Nel paragrafo precedente abbiamo definito la nozione di insieme finito non vuoto: *$X \neq \varnothing$ è finito se esiste un numero naturale $n \in \mathbb{N}$ ed una biezione tra $\xi(n)$ e X.*
È naturale chiedersi se esistono insiemi che non soddisfano la definizione di insieme finito, cioè se esiste un insieme X che soddisfa alla seguente condizione: $\forall n \in \mathbb{N}$ *non esiste una biezione tra $\xi(n)$ e X.*
Se un tale insieme X esiste allora non è finito e viene naturale appellarlo con l'aggettivo *infinito*. In altre parole diciamo che un insieme è infinito se non è finito.
Prima di procedere è bene osservare che la nozione di insieme infinito (nel senso non finito) è equivalente ad altre due come illustrato nella seguente proposizione.

Proposizione 4.5 Sia X un insieme. Allora le seguenti affermazioni sono equivalenti
(a) X non è finito;
(b) esiste una funzione iniettiva da $\mathbb{N}$ in X;
(c) esiste una funzione $f : X \to X$ iniettiva ma non suriettiva.

Dimostrazione. Per dimostrare che le tre affermazioni sono equivalenti mostreremo che (a)$\Rightarrow$(b), (b)$\Rightarrow$ (c) e (c)$\Rightarrow$ (a). Il lettore deve poi convincersi che una volta dimostrate le implicazioni in modo ciclico valgono anche tutte le altre implicazioni.

(a)$\Rightarrow$(b) Supponiamo che X non sia finito e costruiamo una funzione iniettiva da $\mathbb{N}$ in X. L'insieme X non è vuoto, altrimenti sarebbe finito, quindi esiste un elemento $x_0 \in X$. Definiamo, per induzione, la seguente funzione $f : \mathbb{N} \to X$: $f(0) = x_0$; supponiamo che $f(n)$ sia definita e che $f(0), \ldots, f(n)$ siano elementi distinti di X, allora definiamo $f(n+1) = x_{n+1}$ con $x_{n+1} \notin \{f(0), \ldots, f(n)\}$. L'elemento x_{n+1} deve esistere altrimenti $X = \{f(0), \ldots, f(n)\}$ ed $f : \{0, \ldots, n\} \to X$ sarebbe una biezione contro l'ipotesi che X non è finito.

(b)$\Rightarrow$ (c) Supponiamo esista una funzione iniettiva $g : \mathbb{N} \to X$. Si consideri la funzione biettiva $\tilde{g} : \mathbb{N} \to g(\mathbb{N})$ definita da $\tilde{g}(n) = g(n), n \in \mathbb{N}$. Utilizzando la funzione $\tilde{g}$ e la funzione successore si

può costruire la seguente funzione iniettiva non suriettiva

$$\begin{array}{ccccccc} h : g(\mathbb{N}) & \xrightarrow{\tilde{g}^{-1}} & \mathbb{N} & \xrightarrow{s} & \mathbb{N} & \xrightarrow{\tilde{g}} & g(\mathbb{N}) \\ x & \longmapsto & \tilde{g}^{-1}(x) & \mapsto & s(\tilde{g}^{-1}(x)) & \longmapsto & \tilde{g}(s(\tilde{g}^{-1}(x))) \end{array}$$

La funzione h è iniettiva poiché composizione di funzioni iniettive. Inoltre, l'elemento $g(0) \in g(\mathbb{N})$ non appartiene all'immagine di h. Se così fosse, cioè se esistesse $x_0 \in g(\mathbb{N})$ con $h(x_0) = g(0)$ si avrebbe $\tilde{g} \circ s \circ \tilde{g}^{-1}(x_0) = \tilde{g}(0)$ da cui, essendo $\tilde{g}$ iniettiva, $s \circ \tilde{g}^{-1}(x_0) = 0$ contro il fatto che $0 \notin s(\mathbb{N})$. Quindi h non è suriettiva. Estendiamo adesso h ad una funzione su tutto X nel modo seguente:

$$\begin{array}{rccl} f: & X & \to & X \\ & x & \mapsto & f(x) = \begin{cases} h(x) & \text{se } x \in g(\mathbb{N}) \\ x & \text{se } x \in X \setminus g(\mathbb{N}) \end{cases} \end{array}$$

La funzione f risulta iniettiva e non surittiva (il lettore deve fare tutto il ragionamento necessario per arrivare a questa conclusione).

(c)$\Rightarrow$ (a) Se esiste una funzione $f : X \to X$ iniettiva non surittva l'insieme X non è finito in virtù della Proposizione 4.4. ■

L'insieme dei numeri naturali è evidentemente infinito; basti considerare che la funzione successore $s : \mathbb{N} \to \mathbb{N}$ è iniettiva ma non suriettiva. Questo fatto giustifica il nome dato all'*assioma dell'infinito*, il quale permette proprio la costruzione dei numeri naturali che costituiscono, per l'appunto, un insieme infinito.
È interessante notare che delle tre definizioni equivalenti di insieme infinito la più interessante è quella che asserisce l'esistenza di una funzione $f : X \to X$ iniettiva ma non suriettiva. Questa definizione, infatti, prescinde dalla costruzione dei numeri naturali. Sorge spontanea la domanda se l'esistenza di un insieme X e di una funzione $f : X \to X$ iniettiva ma non suriettiva garantisca l'esistenza dei numeri naturali, ossia l'esistenza di un sistema di Peano. La risposta è affermativa come mostrato nella seguente proposizione.

Proposizione 4.6 Sia X un insieme e supponiamo esista una funzione $f : X \to X$ iniettiva non suriettiva. Allora esistono un sottoinsieme $C \subseteq X$, un elemento $a \in C$ e un'applicazione iniettiva $s : C \to C$ tale che la terna (C, s, a) sia un sistema di Peano.

Dimostrazione. Sia $f : X \to X$ iniettiva non suriettiva e sia $a \in X \setminus f(X)$. Si consideri la famiglia

$$\mathscr{A} = \{A \subseteq X : a \in A \quad \wedge \quad f(A) \subseteq A\}$$

La famiglia $\mathscr{A}$ non è vuota, $X \in \mathscr{A}$. Sia

$$C = \bigcap_{A \in \mathscr{A}} A$$

Si ha

$$f(C) = f(\bigcap_{A \in \mathscr{A}} A) \subseteq \bigcap_{A \in \mathscr{A}} f(A) \subseteq \bigcap_{A \in \mathscr{A}} A = C$$

quindi $C \in \mathscr{A}$. Sia adesso $s = f_{|C}$. Allora la terna (C, s, a) è un sistema di Peano. A tal scopo, si noti che P_1, P_2, P_3 e P_4 sono immediati mentre per P_5 sia $E \subseteq C$ con $a \in E$ e $s(E) \subseteq E$. Allora $E \in \mathscr{A}$ da cui $C = \bigcap_{A \in \mathscr{A}} A \subseteq E$. ■

4.3 Problemi proposti

Problema 4.1 Dati due insiemi X e Y denotiamo con

$$X+Y = \{(x,0)\colon x \in X\} \cup \{(y,1)\colon y \in Y\} \subset (X \cup Y) \times \{0,1\}$$

la *somma disgiunta* di X e Y. Dimostrare che se X e Y sono finiti

$$|X+Y| = |X| + |Y|$$

Problema 4.2 Siano A, B due insiemi finiti con $B \subset A$. Si provi che

$$|A \setminus B| = |A| - |B|$$

Problema 4.3 Siano X, Y, Z tre insiemi finiti. Dimostrare che

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

Problema 4.4 Sia X un insieme finito. Dimostrare che per ogni $x \in X$, non esiste una biezione tra X e $X \setminus \{x\}$.

Problema 4.5 Sia X un insieme tale che esiste una funzione $f : X \to X$ iniettiva ma non suriettiva. Dimostrare che per ogni $x \in X \setminus f(X)$ esiste una funzione iniettiva $\mathbb{N} \to X$ con $f(0) = x$.

Problema 4.6 Dimostrare che un insieme X è infinito se e solo se esiste un sottoinsieme $A \subseteq X$, $A \neq X$, e una corrispondenza biunivoca da X in A.

Problema 4.7 Sia X l'insieme dei numeri naturali pari. Determinare una funzione iniettiva da $\mathbb{N}$ in X. Concludere che X è infinito.

5. Relazioni di equivalenza

5.1 Definizione e proprietà

Definizione 5.1 Sia $X \neq \varnothing$ un insieme e sia $R \subseteq X \times X$ una relazione binaria su X. La relazione R è una *relazione di equivalenza* se soddisfa alle seguenti proprietà:

(a) $\forall x \in X \quad (x,x) \in R$ (riflessiva);
(b) Se $(x,y) \in R \quad \Rightarrow \quad (y,x) \in R$ (simmetrica);
(c) Se $(x,y) \in R \quad \wedge \quad (y,z) \in R \quad \Rightarrow \quad (x,z) \in R$ (transitiva).

Osservazione 5.1

(a) La propietà riflessiva è equivalente al fatto che la diagonale di X sia un sottoinsieme di R.
(b) Si suole indicare con xRy quando la coppia (x,y) appartiene a R e si legge *x è in relazione di equivalenza con y*. È comune trovare anche la notazione $x \sim y$ per indicare xRy.

■ **Esempio 5.1** Sia X l'insieme delle rette del piano e sia R la relazione

$rRs \quad \Leftrightarrow \quad r$ e s sono rette parallele, in formula $r||s$.

È immediato verificare che R definisce una relazione di equivalenza. Al contrario, la relazione

$rR's \quad \Leftrightarrow \quad r$ e s sono rette perpendicolari, in formula $r \perp s$,

non definisce una relazione di equivalenza. Infatti, non vale né la proprietà riflessiva né quella transitiva. ■

Osservazione 5.2 Ogni insieme non vuoto X ammette sempre almeno due relazioni di equivalenza:

(a) l'uguaglianza: $xRy \quad \Leftrightarrow \quad x = y$, che corrisponde all'insieme $R = \Delta_X = \{(x,y) : x,y \in X, x = y\}$;
(b) la relazione banale: $xRy \quad \forall x,y \in X$, corrispondente all'intero prodotto $X \times X$.

Tali relazioni di equivalenza sono distinte se e solo se $|X| \geq 2$. Inoltre, essendo $\Delta_X \subseteq R$ per una qualsiasi relazione di equivalenza, possiamo dire che l'uguaglianza e la relazione banale sono, rispettivamente, la "minima" e la "massima" tra le relazioni di equivalenza di X.

Esercizio 5.1 Determinare tutte le relazioni di equivalenza dell'insieme $\{1,2,3\}$.

Definizione 5.2 Sia X un insieme e sia R una relazione di equivalenza su X. Per un dato $x \in X$ l'insieme di tutti gli elementi di X che sono in relazione con x si chiama *classe di equivalenza* di

x e si denota con $[x]_R$; quindi:

$$[x]_R = \{y \in X : yRx\} \subseteq X.$$

Di solito, quando si indica con $[x]_R$ una classe di equivalenza, l'elemento x si chiama *rappresentante della classe*.
La proprietà riflessiva assicura che per ogni $x \in X$, xRx, quindi $x \in [x]_R$. In particolare $[x]_R \neq \varnothing \quad \forall x \in X$, ed inoltre (dimostrare l'uguaglianza per esercizio)

$$\bigcup_{x \in X} [x]_R = X\,.$$

■ **Esempio 5.2** Sia $X = \{a,b,c,d,e\}$ e sia R la relazione di equivalenza

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

Allora si trova

$$[a]_R = [b]_R = [d]_R = \{a,b,d\} \qquad [c]_R = [e]_R = \{c,e\}\,.$$

Si noti che la famiglia di insiemi $\{\{a,b,d\},\{c,e\}\}$ forma una partizione di X. Tale fatto non è una peculiarità di questo esempio ma vale sempre come mostrato dalla seguente proposizione. ■

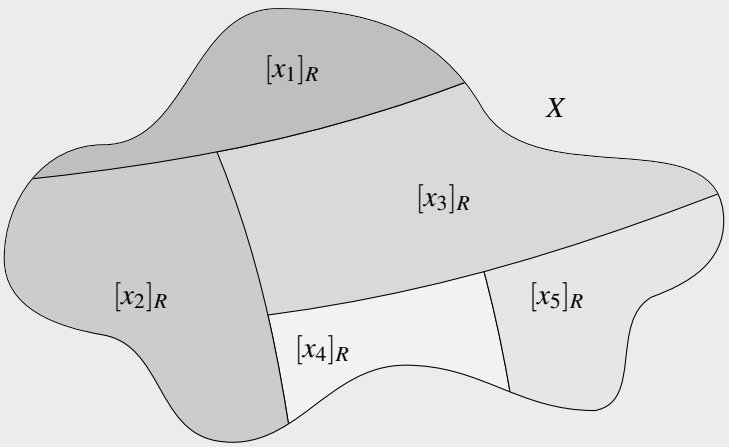
Proposizione 5.1 Sia X un insieme e sia R una relazione di equivalenza su X. Allora la famiglia di sottoinsiemi

$$L_R = \{[x]_R : x \in X\}$$

definisce una partizione di X.

Dimostrazione. Abbiamo già osservato che $[x]_R \neq \varnothing$ per ogni $x \in X$ e che $\bigcup_{x \in X}[x]_R = X$ rimane solo da mostrare che $\forall x,y \in X$ si ha $[x]_R \neq [y]_R \quad \Leftrightarrow \quad [x]_R \cap [y]_R = \varnothing$. "$\Rightarrow$" Se per assurdo esistesse $z \in [x]_R \cap [y]_R$ allora $zRx \quad \wedge \quad zRy$ da cui (per la proprietà simmetrica) $xRz \quad \wedge \quad zRy$ e (per la proprietà transitiva) xRy. Adesso, se xRy si verifica facilmente (esercizio) che $[x]_R = [y]_R$ che conduce ad un assurdo. "$\Leftarrow$" Se $[x]_R \cap [y]_R = \varnothing$ allora $[x]_R$ e $[y]_R$ non hanno elementi in comune ed essendo entrambi non vuoti sono necessariamente distinti. ■

Osservazione 5.3 Graficamente, se pensiamo ad un insieme X come la regione di un piano, le classi di equivalenza suddividono X in sottoinsiemi disgiunti, come mostra la figure seguente, nella quale l'insieme X è l'unione delle cinque classi di equivalenza $[x_1]_R, [x_2]_R, [x_3]_R, [x_4]_R, [x_5]_R$ con $x_i \in X$, $i = 1,2,3,4,5$.



Dato un insieme X consideriamo i seguenti insiemi

$$\mathscr{R} = \{R \subseteq X \times X : R \text{ è una relazione di equivalenza}\}$$
$$\mathscr{L} = \{L \subseteq \mathscr{P}(X) : L \text{ è una partizione di } X\}$$

Vale la seguente proposizione.

Proposizione 5.2 La funzione

$$\begin{array}{rccc} \varphi: & \mathscr{R} & \to & \mathscr{L} \\ & R & \longmapsto & \varphi(R) = L_R = \{[x]_R : x \in X\} \end{array}$$

è una biezione.

Dimostrazione.

Iniettività. Siano R, R' due relazioni di equivalenza su X e supponiamo che $\varphi(R) = \varphi(R')$. Dimostriamo che $R = R'$, ovvero che $R \subseteq R'$ e $R' \subseteq R$. Si osservi preliminarmente che $\varphi(R) = \varphi(R')$ implica $L_R = \{[x]_R : x \in X\} = L_{R'} = \{[x]_R : x \in X\}$ quindi per ogni classe $[x]_R$ esiste un elemento $x' \in X$ tale che $[x]_R = [x']_{R'}$. Sia adesso $(x,y) \in R$ allora $x, y \in [x]_R = [x']_{R'} \quad \Rightarrow \quad xR'x' \quad \wedge \quad yR'x' \overset{\text{simmetrica}}{\Rightarrow}$ $xR'x' \quad \wedge \quad x'R'y \overset{\text{transitiva}}{\Rightarrow} xR'y \quad \Rightarrow \quad (x,y) \in R'$. Allo stesso modo si dimostra che $R' \subseteq R$.

Suriettività. Sia $L \in \mathscr{L}$ una partizione di X. Definiamo la seguente relazione su X

$$\forall x, y \in X \quad xRy \quad \Leftrightarrow \quad \exists A \in L : x, y \in A$$

La relazione R è di equivalenza: è riflessiva poiché, dalla definizione di partizione, per ogni $x \in X$ esiste un $A \in L$ con $x \in A$; è simmetrica, infatti $x, y \in A \quad \Rightarrow \quad y, x \in A$; è transitiva: se $xRy \quad \wedge \quad yRz \quad \Rightarrow \quad \exists A \in L : x, y \in A \quad \wedge \quad \exists A' \in L : y, z \in A'$. Poiché $y \in A \cap A'$ segue che $A \cap A' \neq \varnothing$ e, dalla definizione di partizione, si ha che $A = A'$, così $x, y, z \in A$ e xRz.

Per terminare mostriamo che $\varphi(R) = L_R = L$. Sia $[x]_R \in L_R$, allora esiste $A \in L$ con $x \in A$. Mostriamo che $[x]_R = A$. Infatti, se $y \in [x]_R$ allora yRx ed esiste un elemento di L che li contiene entrambi il quale non può che essere A poiché x appartiene ad A, quindi $[x]_R \subseteq A$. Viceversa, se $y \in A$ allora $x, y \in A$ e, per definizione di R, xRy da cui $y \in [x]_R$. Abbiamo quindi dimostrato che $L_R \subseteq L$. Il lettore mostri, per esercizio, che $L \subseteq L_R$. ■

5.2 Insieme quoziente

Diamo la seguente importante definizione

Definizione 5.3 Sia R una relazione di equivalenza su un insieme $X \neq \varnothing$. L'insieme delle classi di equivalenza

$$\{[x]_R : x \in X\}$$

si chiama *insieme quoziente* di X modulo la relazione di equivalenza R e si indica con

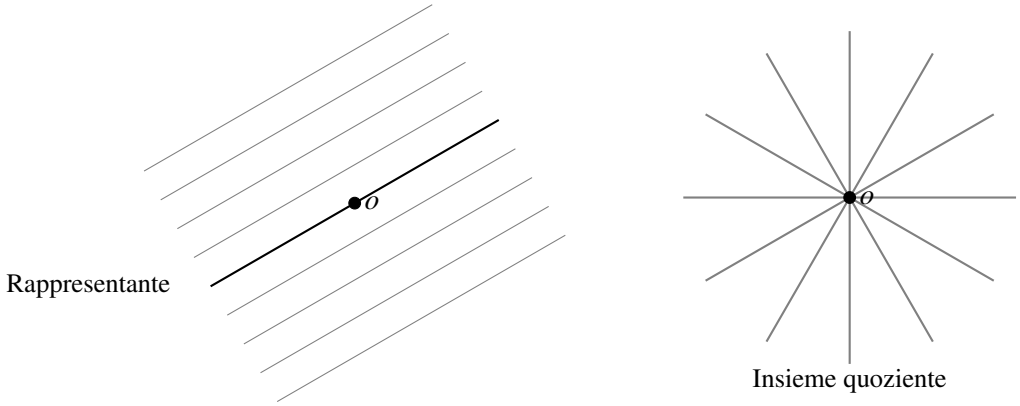
$$X/R$$

Vedremo nel seguito molti esempi di insieme quoziente, in verità non è azzardato dire che in matematica "quasi tutti" gli insiemi si costruiscono come insiemi quozienti di altri.
Si tenga presente che gli elementi di X/R sono classi di equivalenza, quindi sottoinsiemi di X. Ancora, si osservi che a partire da un insieme infinito l'insieme quoziente può essere finito. Anche per quest'ultima considerazione vedremo in seguito importanti costruzioni.

■ **Esempio 5.3** Il seguente esempio vuole solamente dare un'idea visiva di un certo insieme quoziente senza la pretesa di indicare tutti i dettagli necessari. Sia X l'insieme delle rette del piano e sia R la relazione di equivalenza (già definita precedentemente)

$$rRs \quad \Leftrightarrow \quad r \text{ e } s \text{ sono rette parallele, in formula } r||s.$$

Se fissiamo un punto del piano, chiamiamolo o, allora per ogni data classe di equivalenza di rette parallele vi è una ed una sola retta della classe che passa per o. Possiamo quindi rappresentare una classe di equivalenza con il particolare rappresentante dato dalla retta della classe passante per o. In questo modo l'insieme quoziente X/R si può pensare come l'insieme delle rette del piano passanti per o.



■

Definizione 5.4 Sia R una relazione di equivalenza su un insieme $X \neq \varnothing$. L'applicazione suriettiva

$$\begin{array}{rccc} \pi: & X & \to & X/R \\ & x & \longmapsto & [x]_R \end{array}$$

prende il nome di *proiezione canonica*.

■ **Esempio 5.4** Sia $f : X \to Y$ una funzione. Allora la relazione su X definita da

$$\forall x, y \in X \quad xR_f y \quad \Leftrightarrow \quad f(x) = f(y)$$

è di equivalenza (verificare per esercizio). ■

Proposizione 5.3 Sia $f : X \to Y$ una funzione. Allora f si può ottenere come composizione di una funzione suriettiva seguita da una funzione iniettiva.

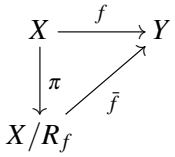
Dimostrazione. Data $f : X \to Y$ sia R_f la relazione di equivalenza definita nell'Esempio 5.4 e definiamo la funzione

$$\begin{array}{rccc} \bar{f}: & X/R_f & \to & Y \\ & [x]_{R_f} & \mapsto & f(x) \end{array}$$

La funzione $\bar{f}$ risulta ben definita poiché se $x' \in [x]_{R_f}$ allora $f(x') = f(x)$. Quindi la definizione di $\bar{f}$ non dipende dal rappresentante scelto. Inoltre $\bar{f}$ è iniettiva, infatti $\bar{f}([x]_{R_f}) = \bar{f}([x']_{R_f}) \quad \Rightarrow \quad f(x) = f(x') \quad \Rightarrow \quad xR_f x' \quad \Rightarrow \quad [x]_{R_f} = [x']_{R_f}$. Si consideri adesso la proiezione canonica $\pi : X \to X/R_f$ la quale è suriettiva. Infine, per ogni $x \in X$ si ha

$$\bar{f} \circ \pi(x) = \bar{f}(\pi(x)) = \bar{f}([x]_{R_f}) = f(x),$$

da cui segue che $f = \bar{f} \circ \pi$. Il fatto che $f = \bar{f} \circ \pi$ si esprime anche dicendo che il seguente diagramma è commutativo:



■

Osservazione 5.4 Si noti che se $f : X \to Y$ è una funzione suriettiva, allora la funzione

$$\begin{array}{rccc} \bar{f}: & X/R_f & \to & Y \\ & [x]_{R_f} & \mapsto & f(x) \end{array}$$

definisce una funzione biettiva.

5.3 Problemi proposti

Problema 5.1 Stabilire se le seguenti relazioni sono di equivalenza sull'insieme $A = \{a,b,c,d,e\}$. In caso affermativo, determinare l'insieme quoziente.

1. $R_1 = \{(a,a),(a,b),(a,c),(e,e),(b,a),(b,b),(c,a),(b,c),(c,b),(c,c),(d,d),(d,d)\}$
2. $R_2 = \{(a,a),(b,c),(b,b),(c,a),(c,c),(a,b),(a,c),(d,d)\}$
3. $R_3 = \{(a,a),(b,b),(c,c),(d,d),(e,e)\}$

Problema 5.2 Stabilire se i seguenti insiemi formano delle partizioni dell'insieme $X = \{1,2,3,4,5,6,7\}$

1. $\mathscr{L}_1 = \{\{1,2\},\{4,5,6\}\}$
2. $\mathscr{L}_2 = \{\{1,4,5,7\},\{2\},\{3,6\}\}$
3. $\mathscr{L}_3 = \{\{1,2,3\},\{4,3,5,6\},\{7\}\}$
4. $\mathscr{L}_4 = \{\{4,5\},\{1,3,7\},\{6,2\}\}$
5. $\mathscr{L}_5 = \{\{1,4,5,7,2\},\varnothing,\{3,6\}\}$
6. $\mathscr{L}_6 = \{\{1,4,5,7,2\},\{\varnothing\},\{3,6\}\}$

In caso affermativo trovare la relazione di equivalenza che le determinano.

Problema 5.3 Si ha α un piano e r una retta che giace su α. Nell'insieme A delle rette del piano α che non sono parallele a r, si consideri la relazione cosi definita: x è in relazione con y se e solo se le rette x e y si intersecano in un punto di r. Verificare che è una relazione di equivalenza è caratterizzare l'insieme quoziente.

Problema 5.4 Sia $X = \mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ e si consideri in X la relazione R definita ponendo, per ogni $a,b,c,d \in X$

$$(a,b)\,R\,(c,d) \quad \Leftrightarrow \quad ab = cd$$

Si dimostri che R è una relazione di equivalenza. Si determinino le classi di equivalenza degli elementi $(0,0)$ e $(1,60)$ di X.

Problema 5.5 Sia $X = \mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ e si consideri in X la relazione R definita ponendo, per ogni $a,b,c,d \in X$

$$(a,b)\,R\,(c,d) \quad \Leftrightarrow \quad a+d = b+c$$

Si dimostri che R è una relazione di equivalenza. Si determinino le classi di equivalenza degli elementi $(0,0)$ e $(1,9)$ di X.

Problema 5.6 Dato un insieme X diciamo che una relazione binaria R su X è *antisimmetrica* se: $\forall x,y \in X,\ (x,y) \in R \quad \wedge \quad (y,x) \in R \quad \Rightarrow \quad x = y$. Sia A un insieme non vuoto. Determinare quali fra le proprietà riflessiva, simmetrica, antisimmetrica e transitiva sono soddisfatte dalle seguenti relazioni definite su $\mathscr{P}(A)$:

1. Per ogni $X,Y \in \mathscr{P}(A), \quad X\,R\,Y \quad \Leftrightarrow \quad X \subseteq Y$.

2. Per ogni $X, Y \in \mathscr{P}(A)$, $\quad X R Y \quad \Leftrightarrow \quad X \cap Y = \varnothing$.
3. Per ogni $X, Y \in \mathscr{P}(A)$, $\quad X R Y \quad \Leftrightarrow \quad X \cap Y \neq \varnothing$.

Problema 5.7 Sia R la relazione su $\mathbb{N}$ definita da:

$$a R b \quad \Leftrightarrow \quad a+b \quad \text{è pari}$$

Dimostrare che R è d'equivalenza su $\mathbb{N}$ e determinare la classe d'equivalenza di 0 e di 1. Quante classi ha la relazione R?

Problema 5.8 Sia R la relazione su $\mathbb{N}$ definita da:

$$a R b \quad \Leftrightarrow \quad a+b \quad \text{è dispari}$$

La relazione R è d'equivalenza?

Problema 5.9 Denotato con $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, sia R la relazione su $\mathbb{N}^* \times \mathbb{N}^*$ definita da

$$(a,b) R (c,d) \quad \Leftrightarrow \quad ad = bc$$

Dimostra che R è d'equivalenza. Qual è la classe d'equivalenza di $(1,1)$? Qual è la classe d'equivalenza di $(1,2)$? Quante classi ha la relazione R?

Problema 5.10 Sia R la relazione binaria su $A = \mathscr{P}(\mathbb{N})$ definita da: $X R Y \quad \Leftrightarrow \quad X$ e Y sono finiti con $|X| = |Y|$ **oppure** X, Y sono entrambi infiniti.

1. Dimostrare che R è d'equivalenza.
2. Determinare la classe di equivalenza dell'elemento $\varnothing$ di A.
3. Dato un numero naturale n determinare la classe di equivalenza di $\{n\}$ in A.
4. Determinare la classe di equivalenza dell'insieme dei numeri pari.
5. Quante sono le classi d'equivalenza di R?

6. Numeri interi e numeri razionali

6.1 Costruzione degli interi

Se $n \leq m$ abbiamo definito $m-n=k$ dove $k \in \mathbb{N}$ è tale che $m=n+k$. Un'analisi attenta mostra che per un dato numero naturale k esistono infinite coppie di numeri naturali tali che $m-n=k$. Per esempio, le coppie $(5,2),(6,3),(7,4),\ldots$ realizzano il numero 3. Verrebbe quindi naturale definire la seguente relazione su $\mathbb{N}\times\mathbb{N}$:

$$(m,n)R(m',n') \quad \Leftrightarrow \quad m-n=m'-n'$$

Tale relazione si può, però, definire solo se $n \leq m$ e $n' \leq m'$. Per ovviare a questo fatto osserviamo che, quando $n \leq m$ e $n' \leq m'$, la relazione $m-n=m'-n' \quad \Rightarrow \quad m=n+k \quad \wedge \quad m'=n'+k \quad \Rightarrow \quad m+n'=n+k+n' \quad \wedge \quad m'+n=n'+k+n \quad \Rightarrow \quad m+n'=m'+n$. L'ultima relazione, $m+n'=m'+n$, ha piena validità per tutte le coppie $(m,n),(m',n') \in \mathbb{N}\times\mathbb{N}$. Possiamo quindi definire la relazione

$$(m,n)R(m',n') \quad \Leftrightarrow \quad m+n'=m'+n\,, \tag{6.1}$$

che è di equivalenza in virtù del Problema 5.5.

Definizione 6.1 I *numeri interi* sono l'insieme quoziente

$$\mathbb{Z}=(\mathbb{N}\times\mathbb{N})/R$$

dove R è la relazione (6.1).

Quindi un numero intero è una classe di equivalenza $[(m,n)]_R$ che indicheremo, per alleggerire le notazioni, con $[m,n]$.
Definiamo ora due operazioni binarie sui numeri interi.

Definizione 6.2 La somma su $\mathbb{Z}$ è l'operazione binaria $+_{\mathbb{Z}}:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ definita da, $\forall a,b,c,d \in \mathbb{N}$,

$$[a,b]+_{\mathbb{Z}}[c,d]=[a+_{\mathbb{N}}c,b+_{\mathbb{N}}d]\,.$$

Nel seguito, per non appesantire la notazione, ometteremo il pedice nel simbolo di somma $+_{\mathbb{N}}$ e $+_{\mathbb{Z}}$ confidando sul fatto che il lettore non dovrebbe avere dubbi su quale somma utilizzare a seconda del contesto.

Esercizio 6.1 Dimostrare che l'operazione di somma è ben definita, cioè che se $(a',b') \in [a,b]$ e $(c',d') \in [c,d]$ allora $(a'+c',b'+d') \in [a+c,b+d]$.

Proposizione 6.1 — Proprietà della somma. L'operazione di somma in $\mathbb{Z}$ gode delle seguenti proprietà, $\forall a,b,c,d,e,f \in \mathbb{N}$,

1. $[a,b]+[c,d]=[c,d]+[a,b]$ (commutativa)
2. $([a,b]+[c,d])+[e,f]=[a,b]+([c,d]+[e,f])$ (associativa)
3. $[a,b]+[0,0]=[a,b]$ (esistenza dello zero)
4. $[a,b]+[b,a]=[0,0]$ (esistenza dell'opposto)

Dimostrazione. Esercizio. ■

La Proposizione 6.1 mostra che i numeri interi assieme all'operazione di somma formano un *gruppo algebrico* la cui definizione è la seguente.

Definizione 6.3 Un insieme S assieme ad un'operazione binaria $* : S \times S \to S$ forma un *gruppo algebrico* se, $\forall a,b,c \in S$, valgono le seguenti proprietà:

1. $(a*b)*c = a*(b*c)$ (associativa)
2. esiste $e \in S$ con $a*e = e*a = a \quad \forall a \in S$ (esistenza dell'elemento neutro)
3. per ogni $a \in S$ esiste $a^{-1} \in S$ tale che $a*a^{-1} = a^{-1}*a = e$ (esistenza dell'inverso)

Inoltre se $a*b = b*a \quad \forall a,b \in S$ il gruppo $(S,*)$ si dice *abeliano*.

Quindi $(\mathbb{Z},+)$ è un gruppo algebrico abeliano. Siamo soliti chiamare l'elemento neutro $[0,0]$ lo *zero* di $\mathbb{Z}$ e l'inverso rispetto alla somma *opposto*.

■ **Esempio 6.1** A titolo di esempio si osservi che, dato un insieme X, l'insieme $B(X) = \{f : X \to X : f \text{ è biettiva}\}$ assieme all'operazione $* : B(X) \times B(X) \to B(X)$ definita da $f*g = f \circ g$, $\forall f,g \in B(X)$, forma un gruppo algebrico non abeliano. ■

Definizione 6.4 Il prodotto su $\mathbb{Z}$ è l'operazione binaria $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definita da, $\forall a,b,c,d \in \mathbb{N}$,

$$[a,b] \cdot [c,d] = [ac+bd, ad+bc]. \tag{6.2}$$

Esercizio 6.2 Dimostrare che l'operazione di prodotto è ben definita.

Proposizione 6.2 — Proprietà del prodotto. L'operazione di prodotto in $\mathbb{Z}$ gode delle seguenti proprietà, $\forall a,b,c,d,e,f \in \mathbb{N}$,

1. $[a,b] \cdot [c,d] = [c,d] \cdot [a,b]$ (commutativa)
2. $([a,b] \cdot [c,d]) \cdot [e,f] = [a,b] \cdot ([c,d] \cdot [e,f])$ (associativa)
3. $[a,b] \cdot [1,0] = [a,b]$ (esistenza dell'elemento neutro)
4. $[a,b]([c,d]+[e,f]) = [a,b] \cdot [c,d] + [a,b] \cdot [e,f]$ (distributiva)

Dimostrazione. Esercizio. ■

La Proposizione 6.2 mostra che i numeri interi assieme alle due operazioni di somma e prodotto formano un *anello* la cui definizione è la seguente.

Definizione 6.5 Un insieme A assieme a due operazioni binarie $+ : A \times A \to A$ e $\cdot : A \times A \to A$ forma un *anello* se valgono le seguenti proprietà:

1. $(A,+)$ è un gruppo abeliano;
2. l'operazione $\cdot$ è associativa;
3. vale la proprietà distributiva.

Inoltre: se l'operazione $\cdot$ è commutativa l'anello si chiama *commutativo*; se esiste l'elemento neutro e per l'operazione $\cdot$ l'anello si chiama *unitario*.

Quindi $(\mathbb{Z},+,\cdot)$ è un anello unitario commutativo.

In un anello unitario $(A,+,\cdot)$ gli elementi invertibili rispetto alla moltiplicazione, cioè gli elementi $a \in S$ tali che esiste $b \in S$ con $ab = ba = e$ si dicono *unità*.

6.2 Numeri naturali, numeri interi e ordine

Consideriamo la seguente funzione iniettiva dai numeri naturali nei numeri interi

$$\begin{array}{rccc} J: & \mathbb{N} & \to & \mathbb{Z} \\ & n & \mapsto & [n,0] \end{array}$$

Poichè J è iniettiva possiamo identificare $\mathbb{N}$ con la sua immagine $J(\mathbb{N}) \subseteq \mathbb{Z}$. Inoltre J conserva le operazioni di somma e prodotto. Infatti, $\forall m,n \in \mathbb{N}$,

$$J(m +_{\mathbb{N}} n) = [m +_{\mathbb{N}} n, 0] = [m,0] +_{\mathbb{Z}} [n,0] = J(m) +_{\mathbb{Z}} J(n)$$

$$J(m \cdot_{\mathbb{N}} n) = [m \cdot_{\mathbb{N}} n, 0] = [m,0] \cdot_{\mathbb{Z}} [n,0] = J(m) \cdot_{\mathbb{Z}} J(n)$$

Quindi le operazioni di $\mathbb{Z}$ ristrette a $J(\mathbb{N})$ coincidono con le operazioni definite sui numeri naturali. Identifichiamo n con $[n,0]$ e scriviamo $n \simeq [n,0]$. Vediamo adesso di comprendere la natura degli elementi in $\mathbb{Z}$ del tipo $[0,n]$, $n \in \mathbb{N}$. Dalla

$$[n,0] + [0,n] = [n,n] = [0,0] \simeq 0$$

si deduce che $[0,n]$ è l'opposto del numero $n \simeq [n,0]$. Poniamo, per convenzione, $-n \simeq [0,n]$. Si ha

$$n + (-n) = 0\,.$$

Introduciamo un ordine in $\mathbb{Z}$ che ristretto ad $\mathbb{N}$ coincida con l'ordine definito in $\mathbb{N}$.

Definizione 6.6 Siano $[a,b],[c,d] \in \mathbb{Z}$ due interi. Poniamo

$$[a,b] \leq_{\mathbb{Z}} [c,d] \quad \Leftrightarrow \quad a + d \leq_{\mathbb{N}} b + c\,.$$

Esercizio 6.3 Dimostrare che la Definizione 6.6 non dipende dal rappresentante scelto, cioè che se $(a',b') \in [a,b]$ e $(c',d') \in [c,d]$ allora

$$a + d \leq_{\mathbb{N}} b + c \quad \Leftrightarrow \quad a' + d' \leq_{\mathbb{N}} b' + c'$$

Soluzione: Sappiamo che (omettiamo di scrivere il pedice nella somma)

$$a' + b = a + b' \quad \wedge \quad c' + d = c + d'$$

Vogliamo dimostrare che

$$a + d \leq b + c \quad \Leftrightarrow \quad a' + d' \leq b' + c'$$

Dimostriamo "⇒".

$$a + d \leq b + c \quad \Rightarrow \quad a + d + a' + b \leq b + c + a' + b = b + c + a + b' \quad \Rightarrow \quad d + a' \leq c + b'$$

da cui

$$d + a' + d' \leq c + b' + d' = c + d' + b' = c' + d + b' \quad \Rightarrow \quad a' + d' \leq b' + c'\,.$$

Restringendo $\leq_{\mathbb{Z}}$ ai numeri naturali si trova

$$[m,0] \leq_{\mathbb{Z}} [n,0] \quad \Leftrightarrow \quad m \leq_{\mathbb{N}} n,$$

quindi l'ordine definito in $\mathbb{Z}$ estende l'ordine dei numeri naturali, in altri termini

$$J(m) \leq_{\mathbb{Z}} J(n) \quad \Leftrightarrow \quad m \leq_{\mathbb{N}} n\,.$$

Inoltre, $\forall n \in \mathbb{N}$,

$$[0,0] \leq_{\mathbb{Z}} [n,0] \quad \wedge \quad [0,n] \leq_{\mathbb{Z}} [0,0],$$

cioè

$$0 \leq_{\mathbb{Z}} n \quad \wedge \quad -n \leq_{\mathbb{Z}} 0\,.$$

Quindi i numeri naturali diversi da zero sono interi positivi (maggiori di zero) mentre i numeri della forma $-n, n \in \mathbb{N}$, sono interi negativi (minori di zero). Infine, si osservi che ogni numero intero diverso da zero si può scrivere nella forma n o $-n$ per qualche $n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Infatti, se $[a,b] \neq 0$ allora $a \neq b$ da cui, per la dicotomia dei numeri naturali,

$$[a,b] = \begin{cases} [a-b,0] & \text{se } b < a \\ \\ [0,b-a] & \text{se } a < b \end{cases}$$

Possiamo distinguere tre situazioni di prodotto tra due numeri interi:

1. $[a,b] > 0 \quad \wedge \quad [c,d] > 0$. In questo caso possiamo identificare $[a,b] = [n,0]$ e $[c,d] = [n',0]$ con $n, n' \in \mathbb{N}$. Segue dalla (6.2) che

$$[a,b][c,d] = [n,0][n',0] = [nn',0] > 0\,.$$

2. $[a,b] > 0 \quad \wedge \quad [c,d] < 0$. In questo caso possiamo identificare $[a,b] = [n,0]$ e $[c,d] = [0,n']$ con $n, n' \in \mathbb{N}$. Segue dalla (6.2) che

$$[a,b][c,d] = [n,0][0,n'] = [0,nn'] < 0\,.$$

3. $[a,b] < 0 \quad \wedge \quad [c,d] < 0$. In questo caso possiamo identificare $[a,b] = [0,n]$ e $[c,d] = [0,n']$ con $n, n' \in \mathbb{N}$. Segue dalla (6.2) che

$$[a,b][c,d] = [0,n][0,n'] = [nn',0] > 0\,.$$

Ritroviamo in questo modo l'usuale regola dei segni valida per la moltiplicazioni tra numeri interi.

Proposizione 6.3 La relazione d'ordine $\leq_{\mathbb{Z}}$ definita su $\mathbb{Z}$ soddisfa le seguenti proprietà, $\forall a,b,c,d,e,f \in \mathbb{N}$,

(a) $[a,b] \leq_{\mathbb{Z}} [a,b]$ (riflessiva);
(b) $[a,b] \leq_{\mathbb{Z}} [c,d] \quad \wedge \quad [c,d] \leq_{\mathbb{Z}} [a,b] \quad \Leftrightarrow \quad [a,b] = [c,d]$ (antisimmetrica);
(c) $[a,b] \leq_{\mathbb{Z}} [c,d] \quad \wedge \quad [c,d] \leq_{\mathbb{Z}} [e,f] \quad \Rightarrow \quad [a,b] \leq_{\mathbb{Z}} [e,f]$ (transitiva);
(d) $[a,b] \leq_{\mathbb{Z}} [c,d] \quad \vee \quad [c,d] \leq_{\mathbb{Z}} [a,b]$ (dicotomia);

Dimostrazione. Esercizio. ■

Da ora in poi indicheremo i numeri interi semplicemente con $x, y, z, etc.$ omettendo di indicare la classe di equivalenza.

Esercizio 6.4 Siano $x,y,z \in \mathbb{Z}$. Dimostrare le seguenti proprietà.
1. $x \leq y \quad \Rightarrow \quad x+z \leq y+z$.
2. Se $z > 0$ allora $x \leq y \quad \Rightarrow \quad xz \leq yz$.
3. Se $z < 0$ allora $x \leq y \quad \Rightarrow \quad yz \leq xz$.

Osservazione 6.1 Dall'Esercizio 6.4 se $0 \leq x \leq y$ allora, moltiplicando l'ultima per x, si ottiene $xx \leq yx$ mentre, moltiplicando per y, si trova $xy \leq yy$. Le ultime due condizioni, per la proprietà transitiva, implicano $x^2 \leq y^2$.
Inoltre, $\forall x \in \mathbb{Z}$, si ha $xx = x^2 \geq 0$.

Proposizione 6.4 — Proprietà archimedea. Per ogni $x,y \in \mathbb{Z}$, con $0 < x < y$, esiste un $n \in \mathbb{N}$ tale che $nx > y$.

Dimostrazione. Dimostriamo la proposizione per induzione su x. Se $x = 1$ si scelga $n = y+1$ da cui $nx = (y+1)1 = y+1 > y$. Supponiamo che la proposizione sia vera per $x \geq 1$ e per ogni $y > x$. Dimostriamo che la proposizione è vera per $x+1$ e per ogni $y > x+1$. Sia quindi $x+1 < y$, allora $x < y-1$ e, per ipotesi induttiva, esiste $n \in \mathbb{N}$ con $nx > y-1$. Segue che $(n+1)(x+1) > (n+1)x = nx+x > y-1+x \geq y$. ■

6.3 Problemi proposti

Problema 6.1 Dimostrare che le operazioni di somma e prodotto definite in $\mathbb{Z}$:
1. non dipendono dal rappresentante scelto;
2. sono commutative;
3. sono associative;
4. vale la proprietà distributiva.

Problema 6.2 Dimostrare la Proposizione 6.3.

Problema 6.3 Dimostrare che per ogni $x,y,z \in \mathbb{Z}$ valgono le seguenti proprietà.
1. $x \leq y \quad \Rightarrow \quad x+z \leq y+z$
2. se $z > 0$ allora $x \leq y \quad \Rightarrow \quad xz \leq yz$
3. se $z < 0$ allora $x \leq y \quad \Rightarrow \quad yz \leq xz$

Problema 6.4 Dimostrare che le seguenti proprietà sono equivalenti in $\mathbb{Z}$.
1. per ogni $z \in \mathbb{Z}$ esiste un $n \in \mathbb{N}$ con $n > z$;
2. per ogni $z,z' \in \mathbb{Z}$ con $0 < z < z'$ esiste un $n \in \mathbb{N}$ con $nz > z'$.

Problema 6.5 In un anello $(A,+,\cdot)$ le *unità* sono gli elementi invertibili rispetto a "$\cdot$". Dimostrare che nell'anello $(\mathbb{Z},+,\cdot)$ le uniche unità sono 1 e -1.

6.4 I numeri razionali

Poniamo $\mathbb{Z}^\star = \mathbb{Z} \setminus \{0\}$ e definiamo su $\mathbb{Z} \times \mathbb{Z}^\star$ la relazione

$$(a,b)R(a',b') \quad \Leftrightarrow \quad ab' = a'b\,.$$

Esercizio 6.5 Verificare che la relazione R è di equivalenza.

Definizione 6.7 Definiamo i *numeri razionali* come l'insieme quoziente

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^\star)/R\,.$$

Un numero razionale è quindi una classe di equivalenza $[a,b]$ che, di solito, denotiamo con

$$\frac{a}{b}$$

dove (a,b) è un rappresentante della classe.
Definiamo due operazioni su Q nel modo seguente.

Definizione 6.8 La somma su $\mathbb{Q}$ è l'operazione binaria $+ : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ definita da, $\forall a,b,c,d\in\mathbb{Z}$,

$$[a,b]+[c,d]=[ad+bc,bd]\,.$$

La moltiplicazione su $\mathbb{Q}$ è l'operazione binaria $\cdot : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ definita da, $\forall a,b,c,d\in\mathbb{Z}$,

$$[a,b]\cdot[c,d]=[ac,bd]\,.$$

Esercizio 6.6

1. Verificare che la somma ed il prodotto sono operazioni ben definite, cioè non dipendono dal rappresentante scelto.
2. Dimostrare che le due operazioni godono della proprietà associativa, commutativa e distributiva.
3. Dimostrare che $[0,1]$ è l'elemento neutro per la somma, lo zero di $\mathbb{Q}$.
4. Dimostrare che $[1,1]$ è l'elemento neutro per il prodotto, l'uno di $\mathbb{Q}$.
5. Dimostrare che $\forall\,[a,b]\in\mathbb{Q}$ esiste l'opposto, cioè $[c,d]\in\mathbb{Q}$ tale che $[a,b]+[c,d]=[0,1]$.
6. Dimostrare che se $a\neq 0$ allora $[a,b][b,a]=[1,1]$. Quindi ogni elemento diverso dallo zero ha un inverso moltiplicativo.

Definizione 6.9 Un insieme S dotato di due operazioni binarie, $(S,+,\cdot)$, è un *campo* se è un anello unitario commutativo nel quale ogni elemento diverso da zero ha un inverso moltiplicativo.

Dall'Esercizio 6.6 segue che $(\mathbb{Q},+,\cdot)$ è un campo.

Consideriamo adesso l'applicazione

$$\begin{array}{rccc} J: & \mathbb{Z} & \to & \mathbb{Q} \\ & z & \mapsto & [z,1] \end{array}$$

la quale è chiaramente iniettiva e soddisfa alle seguenti prorietà (da verificare per esercizio):

1. $J(z+_{\mathbb{Z}}w)=J(z)+_{\mathbb{Q}}J(w),\quad \forall z,w\in\mathbb{Z}$;
2. $J(z\cdot_{\mathbb{Z}}w)=J(z)\cdot_{\mathbb{Q}}J(w),\quad \forall z,w\in\mathbb{Z}$.

Segue che possiamo identificare i numeri interi $\mathbb{Z}$ con il sottoinsieme $J(\mathbb{Z})\subseteq\mathbb{Q}$. In analogia con quanto fatto in $\mathbb{Z}$ definiamo un ordine su $\mathbb{Q}$ che estenda l'ordine su $\mathbb{Z}$. Poniamo

$$[a,b]\leq[c,d]\quad\Leftrightarrow\quad\begin{cases} ad\leq bc & \text{quando } bd>0 \\ bc\leq ad & \text{quando } bd<0 \end{cases} \tag{6.3}$$

Esercizio 6.7 Dimostrare che la (6.3) non dipende dal rappresentante scelto.

Si vede immediatamente che restringendo l'ordine (6.3) ai numeri interi si ottiene, per ogni $z,z'\in\mathbb{Z}$,

$$[z,1]\leq[z',1]\quad\Leftrightarrow\quad z\leq z'$$

da cui l'ordine su $\mathbb{Q}$ estende quello già definito su $\mathbb{Z}$.

Osservazione 6.2 Denotato con $0 = [0,1]$ lo zero di $\mathbb{Q}$ segue immediatamente dalla (6.3) che, per ogni $a, b \in \mathbb{Z}$

$$\begin{cases} [a,b] \geq 0 & \Leftrightarrow \quad ab \geq 0 \\ [a,b] \leq 0 & \Leftrightarrow \quad ab \leq 0 \end{cases}$$

Si osservi inoltre che $(a,b)R(-a,-b)$. Quindi se $[a,b]$ è un numero razionale positivo possiamo sempre scegliere un rappresentante con $a, b > 0$.

Esercizio 6.8 Dimostrare che l'ordine $\leq$ definito su $\mathbb{Q}$ gode delle proprietà: riflessiva, transitiva e antisimmetrica. Dimostrare inoltre che per ogni coppia di numeri razionali $q, q' \in \mathbb{Q}$ si ha: $q \leq q' \quad \vee \quad q' \leq q$.

Esercizio 6.9 — Proprietà archimedea di $\mathbb{Q}$. Dimostrare che le seguenti proprietà sono equivalenti in $\mathbb{Q}$.

1. per ogni $q \in \mathbb{Q}$ esiste un $n \in \mathbb{N}$ con $n > q$;
2. per ogni $q, q' \in \mathbb{Q}$ con $0 < q < q'$ esiste un $n \in \mathbb{N}$ con $nq > q'$;
3. per ogni $q \in \mathbb{Q}$, $q > 0$, esiste un $n \in \mathbb{N}$ con $0 < 1/n < q$.

Dimostrare poi che una, quindi tutte, sono vere in $\mathbb{Q}$.

7. Calcolo combinatorio

7.1 Il coefficiente binomiale

Definizione 7.1 Sia $n \in \mathbb{N}$ definiamo il *fattoriale* di n, indicato con $n!$, per induzione nel modo seguente:

$0! = 1$

se $n!$ è definito allora $(n+1)! = (n+1)n!$

Segue che $1! = 1 \cdot 0! = 1 \cdot 1 = 1$, $2! = 2 \cdot 1! = 2 \cdot 1 = 2$, $3! = 3 \cdot 2! = 3 \cdot 2 = 6$ e così via si trova, per $n > 0$,

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

Definizione 7.2 Sia X un insieme finito, $|X| = n$. Il numero di sottoinsiemi $Y \subseteq X$ con cardinalità $k \leq n$ prende il nome di *coefficiente binomiale* e si indica con

$$\binom{n}{k} = |\{Y \subseteq X : |Y| = k\}|$$

Osservazione 7.1

1. Per ogni sottoinsieme $Y \subseteq X$ con k elementi il complementare $X \setminus Y$ è un sottoinsieme di X con $n-k$ elementi. Segue che
$$\binom{n}{k} = \binom{n}{n-k}$$
2. Se $k = 0$ si trova
$$\binom{n}{0} = \{\text{numero di sottoinsiemi con 0 elementi di un insieme con } n \text{ elementi}\} = 1$$
infatti vi è solo l'insieme vuoto.
3. Se $k = n$ si trova
$$\binom{n}{n} = \{\text{numero di sottoinsiemi con } n \text{ elementi di un insieme con } n \text{ elementi}\} = 1$$
infatti vi è solo X stesso.

Proposizione 7.1 Sia $n \in \mathbb{N}$ e sia $0 < k < n+1$. Allora

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Dimostrazione. Sia X un insieme con $|X| = n+1$ e sia $x_0 \in X$ un elemento. Allora $X = (X \setminus \{x_0\}) \cup \{x_0\}$. Sia $Y \subseteq X$ con $|Y| = k$. Ci sono due casi

$x_0 \notin Y$ In questo caso $Y \subseteq X \setminus \{x_0\}$ con $|X \setminus \{x_0\}| = n$;

$x_0 \in Y$ In questo caso si avrà $Y = Y' \cup \{x_0\}$ con $Y' \subseteq X \setminus \{x_0\}$ e $|Y'| = k-1$.

Segue che

$$\begin{aligned}\binom{n+1}{k} &= \left|\{Y : Y \subseteq X \setminus \{x_0\}, |Y| = k\} \cup \{Y = Y' \cup \{x_0\} : Y' \subseteq X \setminus \{x_0\}, |Y'| = k-1\}\right| \\ &= \left|\{Y : Y \subseteq X \setminus \{x_0\}, |Y| = k\}\right| + \left|\{Y = Y' \cup \{x_0\} : Y' \subseteq X \setminus \{x_0\}, |Y'| = k-1\}\right| \\ &= \binom{n}{k} + \binom{n}{k-1}.\end{aligned}$$

■

Proposizione 7.2 Sia $n \geq 1$. Allora, per ogni $0 \leq k \leq n$, vale la seguente formula

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{7.1}$$

Dimostrazione. Dimostriamo la proposizione per induzione su n. Per $n = 1$ si trova

$$\binom{1}{0} = 1 \quad \wedge \quad \frac{1!}{0!\,(1-0)!} = 1$$

$$\binom{1}{1} = 1 \quad \wedge \quad \frac{1!}{1!\,(1-1)!} = 1$$

quindi è verificata. Supponiamo che sia vera per n e per ogni $0 \leq k \leq n$. Dimostriamo che è vera per $n+1$ e per ogni $0 \leq k \leq n+1$. Verifichiamo inizialmente che vale per $k = 0$ e $k = n+1$. Infatti, come prima, si trova

$$\binom{n+1}{0} = 1 \quad \wedge \quad \frac{(n+1)!}{0!\,(n+1)!} = 1$$

$$\binom{n+1}{n+1} = 1 \quad \wedge \quad \frac{(n+1)!}{(n+1)!\,(n+1-(n+1))!} = 1$$

Sia adesso $0 < k < n+1$. Applicando la Proposizione 7.1 abbiamo

$$\begin{aligned}\binom{n+1}{k} &= \binom{n}{k} + \binom{n}{k-1} \overset{\text{ip.ind.}}{=} \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!} \\ &= \frac{n!}{k(k-1)!\,(n-k)!} + \frac{n!}{(k-1)!\,(n+1-k)(n-k)!} \\ &= \frac{(n+1-k)n! + kn!}{k!\,(n+1-k)!} = \frac{(n+1)!}{k!\,(n+1-k)!}.\end{aligned}$$

■

Proposizione 7.3 — Formula del binomio di Newton. Siano $a,b \in \mathbb{Q}$, $a,b \neq 0$, e sia $n \geq 1$. Allora

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

Dimostrazione. Per induzione su n. Per $n = 1$ è vera, infatti:

$$(a+b)^1 = a+b \quad \wedge \quad \sum_{i=0}^{1} \binom{1}{i} a^{1-i} b^i = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a+b .$$

Supponiamo che sia vera per n e dimostriamola per $n+1$.

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n \overset{\text{ip.ind.}}{=} (a+b)\left(\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i\right) \\ &= \sum_{i=0}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^{i+1} \end{aligned}$$

$$\begin{aligned} (k = i+1 \text{ nella } 2^o \text{ somma}) &= \sum_{i=0}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1} b^k \\ &= a^{n+1} + \sum_{i=1}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1} b^k + b^{n+1} \\ (i = k \text{ nella } 2^o \text{ somma}) &= a^{n+1} + \sum_{i=1}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=1}^{n} \binom{n}{i-1} a^{n+1-i} b^i + b^{n+1} \\ &= a^{n+1} + \sum_{i=1}^{n} \left[\binom{n}{i} + \binom{n}{i-1}\right] a^{n+1-i} b^i + b^{n+1} \\ (\text{per la Proposizione 7.1}) &= a^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} a^{n+1-i} b^i + b^{n+1} \\ &= \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i} b^i . \end{aligned}$$

■

Se elenchiamo per ogni valore di n, in riga, i coefficienti binomiali $\binom{n}{k}$ al variare di $0 \leq k \leq n$ si ottiene il seguente triangolo

$$\begin{array}{lccccccccccc} n=0 & & & & & \binom{0}{0} & & & & & & \\ n=1 & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\ n=2 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\ n=3 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\ n=4 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\ n=5 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} \end{array}$$

Dalla Proposizione 7.1 si deduce immediatamente che in ciascuna riga gli elementi di questa si ottengono come somma di due elementi adiacenti della riga precedente. Ossia, utilizzando questa proprietà, il triangolo di sopra diventa

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Tale costruzione, molto utile nella pratica per calcolare i coefficienti binomiali ed in particolare per calcolare la potenza di un binomio, prende il nome di *Triangolo di Pascal–Tartaglia*.

Esercizio 7.1 Utilizzando la formula del Binomio di Newton verificare le seguenti identità:

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}=0\,,\qquad \sum_{i=0}^{n}\binom{n}{i}=2^n$$

7.2 Sul numero delle funzioni tra due insiemi finiti

Siano X,Y due insiemi finiti con $|X|=m$ e $|Y|=n$. Ricordiamo che l'insieme Y^X è costituito da tutte le funzioni da X in Y, quindi con $|Y^X|$ indichiamo il numero di tutte le funzioni da un insieme con m elementi ad un insieme con n.
Definiamo inoltre i seguenti insiemi:

$I(X,Y)=\{f:X\to Y:\ f \text{ è iniettiva}\}$
$S(X,Y)=\{f:X\to Y:\ f \text{ è suriettiva}\}$
$B(X,Y)=\{f:X\to Y:\ f \text{ è biettiva}\}$

Scopo di questa sezione è calcolare la cardinalità di questi insiemi che denoteremo nel modo seguente

$I(m,n)=|\{f:X\to Y:\ f \text{ è iniettiva}\}|$
$S(m,n)=|\{f:X\to Y:\ f \text{ è suriettiva}\}|$
$B(m,n)=|\{f:X\to Y:\ f \text{ è biettiva}\}|$

Dimostriamo innanzitutto la seguente formula che fornisce la cardinalità dell'unione di un numero finito di insiemi finiti.

Proposizione 7.4 Siano $Y_1,\dots,Y_n\subseteq X$ n sottoinsiemi di un insieme finito X. Allora

$$|Y_1\cup Y_2\cup\cdots\cup Y_n|=\sum_{i=1}^{n}|Y_i|-\sum_{i<j}|Y_i\cap Y_j|+\sum_{i<j<k}|Y_i\cap Y_j\cap Y_k|+\cdots+(-1)^{n-1}|Y_1\cap\cdots\cap Y_n| \quad (7.2)$$

Dimostrazione. Verifichiamo che ogni elemento $x_0\in Y_1\cup Y_2\cup\cdots\cup Y_n$ sia contato una sola volta nell'espressione a destra della formula (7.2). Supponiamo che x_0 appartenga a $h\le n$ dei sottoinsiemi $Y_1,\dots,Y_n$. Senza ledere la generalità possiamo supporre che $x_0\in Y_1\cap Y_2\cap\cdots\cap Y_h$, cioè che x_0 appartenga proprio ai primi $Y_1,\dots,Y_h$. Segue che x_0 è contato, nell'espressione a destra della formula (7.2), un numero di volte pari a:

$$\delta(x_0)=\binom{h}{1}-\binom{h}{2}+\binom{h}{3}+\cdots+(-1)^{h-1}\binom{h}{h}$$

Calcoliamo $1-\delta(x_0)$. Si trova

$$1-\delta(x_0)=\binom{h}{0}-\binom{h}{1}+\binom{h}{2}-\binom{h}{3}+\cdots+(-1)^h\binom{h}{h}=\sum_{i=0}^{h}\binom{h}{i}(-1)^i\overset{\text{Esercizio 7.1}}{=}0$$

da cui la tesi. ■

Osservazione 7.2 Molto probabilmente nella dimostrazione precedente quello che ha suscitato perplessità è il calcolo di quante volte x_0 è contato nei termini del tipo $\sum_{i<j}|Y_i \cap Y_j|$. Si osservi che la somma va eseguita per tutte le possibili scelte degli indici $\{i,j\}$ con $i,j \leq h$ e $i<j$. Le possibili scelte degli indici $\{i,j\}$ corrispondono a tutti i possibili sottoinsiemi con due elementi dell'insieme $\{1,\ldots,h\}$ che ha h elementi. Tale numero è, per definizione, $\binom{h}{2}$.

Esercizio 7.2 Dimostrare la Proposizione 7.4 per induzione sul numero n di sottoinsiemi $Y_1,\ldots,Y_n \subseteq X$.

Iniziamo con il calcolo della cardinalità dell'insieme di tutte le funzioni. Prima di enunciare il risultato osserviamo che dato un insieme Y si può definire, per induzione, Y^n, $n \in \mathbb{N}^*$, nel modo seguente

$$Y^1 = Y \quad \wedge \quad Y^{n+1} = Y \times Y^n$$

Proposizione 7.5 Siano X,Y due insiemi finiti con $|X| = m$ e $|Y| = n$. Allora

$$\left|Y^X\right| = n^m$$

Dimostrazione. Sia $f : X \to Y$ una funzione e sia $X = \{x_1,\ldots,x_m\}$. La funzione f è univocamente determinata dalla m-pla delle immagini degli elementi di X, cioè da

$$\{f(x_1),\ldots,f(x_m)\} \in Y^m = \overbrace{Y \times Y \times \cdots \times Y}^{m-\text{volte}}.$$

Possiamo quindi definire la funzione biettiva (verificare per esercizio)

$$\begin{array}{rccc} \varphi: & Y^X & \to & Y^m \\ & f & \longmapsto & \{f(x_1),\ldots,f(x_m)\} \end{array}$$

Segue che

$$|Y^X| = |Y^m| = |Y|^m = n^m$$

dove è necessario dimostrare per induzione su m che $|Y^m| = |Y|^m$ (Esercizio per il lettore). ■

Consideriamo ora l'insieme delle funzioni biettive da X in Y. Essendo X e Y finiti possiamo identificarli con $\xi(m)$ e $\xi(n)$ rispettivamente. Dalla Proposizione 4.1 $B(m,n) = 0$ se $m \neq n$, quindi l'unico caso interessante è $m = n$. Le funzioni biettive da $\xi(m) = \{1,\ldots,m\}$ in se stesso prendono il nome di *permutazioni* di $\xi(m)$ e vale la seguente proposizione.

Proposizione 7.6 Sia $m \in \mathbb{N}^*$, allora

$$B(m,m) = m!$$

Dimostrazione. Dobbiamo dimostrare che la cardinalità dell'insieme delle permutazioni di m elementi è $m!$. Procediamo per induzione su m. Se $m = 1$ allora $\xi(1) = \{1\}$ e l'unica funzione biettiva da $\xi(1)$ in se stesso è l'identità. Segue che $B(1,1) = 1$ così come $1! = 1$. Supponiamo che $B(m,m) = m!$ e dimostriamo che $B(m+1,m+1) = (m+1)!$. Consideriamo i seguenti insiemi

$$\begin{aligned} F_1 &= \{f : \xi(m+1) \to \xi(m+1) :\ f \text{ è biettiva} \quad \wedge \quad f(1) = 1\} \\ F_2 &= \{f : \xi(m+1) \to \xi(m+1) :\ f \text{ è biettiva} \quad \wedge \quad f(1) = 2\} \\ &\vdots \\ F_{m+1} &= \{f : \xi(m+1) \to \xi(m+1) :\ f \text{ è biettiva} \quad \wedge \quad f(1) = m+1\} \end{aligned}$$

Per costruzione gli insiemi $F_1, \dots, F_{n+1}$ sono disgiunti e

$$B(\xi(m+1), \xi(m+1)) = \bigcup_{i=1}^{m+1} F_i$$

Inoltre $|F_i| = B(m,m)$, per ogni $i = 1, \dots, m+1$. Quindi, dall'ipotesi induttiva, $|F_i| = m!$, per ogni $i = 1, \dots, m+1$. Infine, dalla Proposizione 7.4, si trova

$$B(m+1, m+1) = \left| \bigcup_{i=1}^{m+1} F_i \right| = \sum_{i=1}^{m+1} |F_i| = \sum_{i=1}^{m+1} m! = (m+1)m! = (m+1)!$$

■

Per intuire il valore di $I(m,n)$ facciamo il seguente ragionamento. Se $n < m$, allora per il principio di Dirichlet $I(m,n) = 0$. Possiamo quindi supporre che $m \leq n$. Supponiamo che $f : X \to Y$ sia una funzione iniettiva, allora $f(x_1)$ può essere uno qualsiasi dei valori di Y. Abbiamo quindi n differenti scelte per l'immagine di x_1. Consideriamo adesso $f(x_2)$. Se abbiamo fissato $f(x_1)$, essendo f iniettiva, $f(x_2)$ può assumere tutti i valori di Y tranne il valore scelto per $f(x_1)$. Segue che $f(x_2)$ si può scegliere in $n-1$ modi differenti. Procedendo si avranno $n-2$ scelte per $f(x_3)$ sino ad arrivare a $f(x_m)$ che avrà $n-(m-1)$ possibili scelte. Il ragionamento visto sopra conduce ad enunciare la seguente proposizione.

Proposizione 7.7 Siano X, Y due insiemi finiti con $|X| = m \leq |Y| = n$. Allora

$$I(m,n) = n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}.$$

Dimostrazione. Senza ledere la generalità possiamo supporre che $X = \xi(m)$ e $Y = \xi(n)$. Se $f : \xi(m) \to \xi(n)$ è iniettiva allora $f(\xi(m)) \subseteq \xi(n)$ è in corrispondenza biunivoca con $\xi(m)$. Quindi $|f(\xi(m))| = |\xi(m)| = m$. Sia $Y \subseteq \xi(n)$, $|Y| = m$, e sia

$$F_Y = \{f : \xi(m) \to \xi(n) \colon f \text{ è iniettiva} \quad \wedge \quad f(\xi(m)) = Y\}$$

Chiaramente

$$|F_Y| = |\{f : \xi(m) \to Y \colon f \text{ è biettiva}\}|$$

Segue dalla Proposizione 7.6 che $|F_Y| = B(m,m) = m!$. Inoltre, se $Y, Y' \subseteq \xi(n)$ con $Y \neq Y'$ allora $F_Y \cap F_{Y'} = \varnothing$. Si può facilmente verificare (mostrando la doppia inclusione) che

$$I(\xi(m), \xi(n)) = \bigcup_{Y \subseteq \xi(n), |Y| = m} F_Y$$

da cui, per la Proposizione 7.4 e tenendo in considerazione la (7.1), si ha

$$I(m,n) = \left| \bigcup_{Y \subseteq \xi(n), |Y| = m} F_Y \right| = \sum_{Y \subseteq \xi(n), |Y| = m} |F_Y| = \binom{n}{m} m! = \frac{n!}{(n-m)!}$$

■

Enunciamo adesso la formula che restituisce il numero di funzioni suriettive. Essendo $S(m,n) = 0$ se $m < n$, supponiamo che $n \leq m$.

Proposizione 7.8 Siano X, Y due insiemi finiti con $|X| = m \geq |Y| = n$. Allora

$$S(m,n) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m .$$

Dimostrazione. Sia $Y = \{y_1, \ldots, y_n\}$. Descriviamo inizialmente l'insieme delle funzioni non suriettive da X in Y. A tal scopo definiamo gli insiemi

$$L_i = \{f : X \to Y : y_i \notin f(X)\}, \quad i \in \{1, \ldots, n\}.$$

Si può verificare immediatamente (mostrando la doppia inclusione) che

$$\bigcup_{i=1}^{n} L_i = \{f : X \to Y : f \text{ non è suriettiva}\}.$$

Le funzioni suriettive si possono ottenere come differenza tra l'insieme di tutte le funzioni e l'insieme delle funzioni non suriettive, cioè

$$S(X,Y) = Y^X \setminus \bigcup_{i=1}^{n} L_i$$

Poiché $\cup_{i=1}^{n} L_i \subseteq Y^X$, per il Problema 4.2 si trova

$$S(m,n) = \left| Y^X \setminus \bigcup_{i=1}^{n} L_i \right| = \left| Y^X \right| - \left| \bigcup_{i=1}^{n} L_i \right| .$$

Applicando la Proposizione 7.4 e la Proposizione 7.5 si trova

$$\begin{aligned}
S(m,n) &= n^m - \left| \bigcup_{i=1}^{n} L_i \right| \\
&= n^m - \left\{ \sum_{i=1}^{n} |L_i| - \sum_{i<j} |L_i \cap L_j| + \cdots + (-1)^{n-1} |L_1 \cap \cdots \cap L_n| \right\} \\
&= n^m - \sum_{i=1}^{n} (n-1)^m + \sum_{i<j} (n-2)^m + \cdots + (-1)(-1)^{n-1} (n-n)^m \\
&= \binom{n}{0} n^m - \binom{n}{1} (n-1)^m + \binom{n}{2} (n-2)^m + \cdots + \binom{n}{n} (-1)^n (n-n)^m \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m ,
\end{aligned}$$

concludendo la prova. ■

7.3 Numeri di Stirling e numeri di Bell

In questa sezione ci proponiamo di risolvere il seguente problema. Sia X un insieme con $|X| = m$:

quante sono le partizioni di X costituite da $n \leq m$ sottoinsiemi di X?

Supponiamo che $L = \{A_1, \ldots, A_n\}$ sia una partizione di X costituita da n sottoinsiemi $A_i \subseteq X, i = 1, \ldots, n$.

Dalla Proposizione 5.2 la partizione L corrisponde ad un'unica relazione di equivalenza R su X costituita da n classi di equivalenza. Segue che l'insieme quoziente X/R ha cardinalità n, ovvero $|X/R| = n$, ed inoltre la proiezione

$$\pi : X \to X/R$$

definisce una funzione suriettiva da un insieme con m elementi in un insieme con n elementi.

Viceversa, se $f : X \to Y$ è una funzione suriettiva da un insieme X, con $|X| = m$, in un insieme $Y = \{y_1, \ldots, y_n\}$, con $|Y| = n$, la famiglia di sottoinsiemi di X

$$\{f^{-1}(y_1), \ldots, f^{-1}(y_n)\}$$

costituisce una partizione di X (verificare per esercizio) costituita da n sottoinsiemi.
Si potrebbe pensare che vi è quindi una corrispondenza biunivoca tra le funzioni suriettive da un insieme con m elementi in un insieme con n elementi e le partizioni di un insieme con m elementi in n parti. Di fatto, la corrispondenza descritta sopra non è biunivoca, infatti esistono funzioni suriettive diverse che inducono la stessa partizione. Per capire quali, si consideri una funzione suriettiva $f : X \to Y$ e una qualsiasi funzione biettiva (permutazione) σ di Y in se stesso. La composizione $f_\sigma = \sigma \circ f : X \to Y$ definisce una funzione suriettiva che coincide con f se e solo se $\sigma = \mathrm{Id}_Y$. La partizione di X indotta da f_σ è $\{f_\sigma^{-1}(y_1), \ldots, f_\sigma^{-1}(y_n)\} = \{f^{-1}(\sigma^{-1}(y_1)), \ldots, f^{-1}(\sigma^{-1}(y_n))\}$ la quale coincide, a meno dell'ordine, con la partizione $\{f^{-1}(y_1), \ldots, f^{-1}(y_n)\}$. Quindi, per ogni permutazione di Y, f_σ determina una nuova funzione suriettiva che induce la stessa partizione di X in n parti. Segue che, se indichiamo con

$$P(m,n) = \{\text{numero di partizioni di un insieme con } m \text{ elementi in } n \text{ parti}\}$$

allora

$$P(m,n) = \frac{S(m,n)}{n!},$$

dove abbiamo tenuto conto della Proposizione 7.6.
I numeri $P(m,n)$ si chiamano *Numeri di Sterling*. Infine, il numero di tutte le partizioni di un insieme X, $|X| = m$, è dato da

$$\mathrm{Bell}(m) = P(m,1) + P(m,2) + \cdots + P(m,m) = \sum_{j=1}^{m} P(m,j) = \sum_{j=1}^{m} \frac{1}{j!} \sum_{i=0}^{j} (-1)^i \binom{j}{i} (j-i)^m.$$

Il numero $\mathrm{Bell}(m)$ prende il nome di *Numero di Bell*.

Osservazione 7.3 A titolo di esempio mostriamo i numeri di Bell per i primi 10 numeri naturali

m	1	2	3	4	5	6	7	8	9	10
$\mathrm{Bell}(m)$	1	2	5	15	52	203	877	4140	21147	115975

Quindi per un insieme con 6 elementi esistono ben 203 partizioni o, equivalentemente, 203 relazioni di equivalenza.

Osservazione 7.4 Un problema che suona simile a quello di ricercare tutte le partizioni di un insieme con m elementi è quello noto in letteratura come *partizioni di un intero positivo m* dove con tale termine si deve intendere una decomposizione additiva di m in numeri interi senza tener conto dell'ordine. Per esempio, le partizioni di 4 sono 5 come indicato di seguito:

1	4
2	$3+1$
3	$2+2$
4	$2+1+1$
5	$1+1+1+1$

Se indichiamo con $P(m)$ il numero delle partizioni di un intero positivo si trova, per i primi 10

interi positivi,

m	1	2	3	4	5	6	7	8	9	10
$P(m)$	1	2	3	5	7	11	15	22	30	42

Una domanda spontanea è la seguente. Per il numero di partizioni di un insieme con m elementi, cioè per $Be(m)$, abbiamo trovato una formula esplicita. Esiste una formula esplicita per $P(m)$?

La risposta è negativa se uno cerca una formula che restituisce il valore esatto di $P(m)$ ma esiste una formula asintotica che restituisce un valore che, diviso per il valore esatto di $P(m)$, tende a 1 man mano che m cresce. Tale formula, intuita dalla sorprendente mente di *Srinivasa Ramanujan* e dimostrata assieme a *Godfrey Harold Hardy*, è la seguente:

$$P(m) \sim \frac{1}{4m\sqrt{3}} \exp\left(\pi\sqrt{\frac{2m}{3}}\right) \text{ per } m \to \infty$$

L'articolo originale con la dimostrazione della formula asintotica è reperibile al link:
`http://ramanujan.sirinudi.org/Volumes/published/ram36.pdf`
Si osservi che se poniamo

$$P_{\text{asintotico}} = \frac{1}{4m\sqrt{3}} \exp\left(\pi\sqrt{\frac{2m}{3}}\right)$$

allora

m	1	2	3	4	5	6	7	8	9	10
$P_{\text{asintotico}}$	1.88	2.72	4.09	6.10	8.94	12.9	18.3	25.5	35.3	48.1

7.4 Problemi proposti

Problema 7.1 Siano X e Y due insiemi finiti. Dimostrare per induzione prima su $m = |X|$ e dopo su $n = |Y|$ che $|Y^X| = n^m$.

Problema 7.2 Sia $X = \{1,2,3,4,5\}$

1. Quanti sono i sottoinsiemi di X che contengono 1?
2. Quanti sono i sottoinsiemi A di X tali che $A \cap \{2,3\} \neq \varnothing$?
3. Quante sono le applicazioni suriettive di X in $\{1,2,3\}$ (senza usare la formula)?

Problema 7.3 Mostrare che per $j \leq k \leq n$, si ha

$$\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$$

Problema 7.4 Dire se la seguente affermazione è vera o falsa

$$\binom{n}{k} = \binom{n-2}{k} + \binom{n-2}{k-1} + \binom{n-2}{k-2}$$

dove $n > 2$ e $1 < k < n-1$.

Problema 7.5 Sia $c, c \leq n$, fissato e si assuma per convenzione che $\binom{k}{i} = 0$ se $k < i$. Mostrare che

$$\sum_{k=0}^{n} \binom{k}{c} = \binom{n+1}{c+1}$$

Problema 7.6 Mostrare che, per r fissato,

$$\sum_{k=0}^{n} \binom{r+k}{k} = \binom{r+n+1}{n}$$

Problema 7.7 Mostrare che

$$\sum_{k=0}^{n} \binom{n-k}{k} = f_{n+1}$$

dove f_n è la successione di Fibonacci: $f_1 = f_2 = 1$ e $f_n = f_{n-1} + f_{n-2}$.

Problema 7.8 Dimostrare per induzione che ogni numero intero positivo può essere scritto come somma di un numero finito di numeri di Fibonacci distinti.

Problema 7.9 Dimostrare la formula ricorsiva:

$$B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(k)\,,$$

dove $B(n)$ rappresenta il numero di Bell.

8. Relazioni d'ordine

8.1 Definizioni ed esempi

In questo capitolo, prendendo spunto dalla relazione d'ordine definita sui numeri naturali, sui numeri interi e sui numeri razionali, consideriamo il concetto di *relazione d'ordine* per un insieme qualsiasi X. Iniziamo con le seguenti definizioni.

Definizione 8.1 Sia X un insieme. Una relazione binaria R su X si dice di *pre-ordine* se, $\forall x, y, z \in X$,

1. xRx (riflessiva)
2. $xRy \quad \wedge \quad yRz \quad \Rightarrow \quad xRz$ (transitiva)

Definizione 8.2 Sia X un insieme. Una relazione binaria R su X si dice *d'ordine parziale* se, $\forall x, y, z \in X$,

1. xRx (riflessiva)
2. $xRy \quad \wedge \quad yRz \quad \Rightarrow \quad xRz$ (transitiva)
3. $xRy \quad \wedge \quad yRx \quad \Rightarrow \quad x = y$ (antisimmetrica)

Indichiamo, solitamente, con $\leq_R$ una relazione d'ordine parziale. Quando dal contesto è chiaro di quale relazione d'ordine parziale si parla, la indicheremo semplicemente con $\leq$.

Indicheremo con $(X, \leq_R)$ un insieme dotato di una relazione d'ordine parziale e chiameremo tale insieme *parzialmente ordinato*.

Definizione 8.3 Sia $(X, \leq_R)$ un insieme parzialmente ordinato. Due elementi $x, y \in X$ si dicono *confrontabili* se

$$x \leq_R y \quad \vee \quad y \leq_R x$$

Definizione 8.4 Sia $(X, \leq_R)$ un insieme parzialmente ordinato. L'ordine si dice *totale* o *lineare* se per ogni coppia di elementi $x, y \in X$ risulta che x, y sono confrontabili. Un insieme dotato di un ordine totale si dice *totalmente ordinato*.

■ **Esempio 8.1** La relazione binaria su $\mathbb{N}$ definita da

$$m \leq n \quad \Leftrightarrow \quad \exists k \in \mathbb{N} : n = m + k$$

definisce una relazione d'ordine parziale in virtù della Proposizione 3.6. In più, per la dicotomia, tale relazione d'ordine è totale. Quindi $(\mathbb{N}, \leq)$ è un insieme totalmente ordinato. Allo stesso modo si vede che $(\mathbb{Z}, \leq)$ e $(\mathbb{Q}, \leq)$ sono insiemi totalmente ordinati. ■

■ **Esempio 8.2** Sia X un insieme e sia $\mathscr{P}(X)$ l'insieme delle parti. Definiamo su $\mathscr{P}(X)$ la seguente relazione, $\forall A, B \in \mathscr{P}(X)$

$$A \leq_{\subseteq} B \quad \Leftrightarrow \quad A \subseteq B$$

Verificare per esercizio che $\leq_{\subseteq}$ definisce una relazione d'ordine parziale. Tale relazione d'ordine parziale non è però totale, non è infatti possibile confrontare due sottoinsiemi A e B nel caso in cui non siano uno contenuto nell'altro, cioè se $A \nsubseteq B \quad \wedge \quad B \nsubseteq A$. ■

■ **Esempio 8.3** Definiamo su $\mathbb{N}^\star = \mathbb{N} \setminus \{0\}$ la seguente relazione

$$m \leq_{|} n \quad \Leftrightarrow \quad \exists k \in \mathbb{N} : n = mk \quad \Leftrightarrow \quad m|n \qquad (m \text{ divide } n)$$

Verificare per esercizio che $\leq_{|}$ definisce una relazione d'ordine parziale (solo l'antissimetrica è meno ovvia e si suggerisce di utilizzare il risultato del Problema 3.3). Anche in questo caso l'ordine non è totale. Per esempio $2 \nleq_{|} 3$ e $3 \nleq_{|} 2$ quindi 2 e 3 non sono confrontabili. ■

■ **Esempio 8.4** Sia $X = \{a, b, c\}$ e definiamo su X la relazione di pre-ordine (verificare)

$$R = \{(a,a), (b,b), (c,c), (a,b), (b,c), (a,c), (b,a)\}.$$

Si ha aRb e bRa ma $a \neq b$, quindi la relazione R non è d'ordine parziale poiché non è antisimmetrica. ■

Definizione 8.5 Sia $(X, \leq)$ un insieme parzialmente ordinato e sia $Y \subseteq X$ un sottoinsieme di X.

1. $y \in Y$ è un *minimo* di Y se $\forall z \in Y$ si ha $y \leq z$;
2. $y \in Y$ è un *massimo* di Y se $\forall z \in Y$ si ha $z \leq y$;
3. $y \in Y$ è un *minimale* di Y se $\forall z \in Y$, $z \leq y \quad \Rightarrow \quad z = y$;
4. $y \in Y$ è un *massimale* di Y se $\forall z \in Y$, $y \leq z \quad \Rightarrow \quad z = y$.

■ **Esempio 8.5** Sia $(\mathbb{N}, \leq)$ e sia $Y = \{2,3,4,5\}$. Allora 2 è un minimo mentre 5 è un massimo. ■

■ **Esempio 8.6** Sia $(\mathbb{N}^\star, \leq_{|})$ e sia $Y = \{2,4,8,16\}$. Allora 2 è un minimo mentre 16 è un massimo. Se invece consideriamo il sottoinsieme $Y = \{2,4,8,15\}$, allora 2 non è un minimo poiché $2 \nleq_{|} 15$. In questo caso 2 è minimale, nel senso che $2 \leq_{|} a$ per ogni $a \in Y$ con cui è confrontabile. Possiamo anche dire che 2, essendo un minimale di Y, è un minimo rispetto al sottoinsieme $Y' = \{2,4,8\}$ degli elementi di Y con cui è confrontabile. Gli elementi massimali di Y sono 8 e 15. Inoltre si osservi che 15 è anche minimale. ■

Proposizione 8.1 Sia $Y \subset (X, \leq)$ un sottoinsieme di un insieme parzialmente ordinato. Se Y ammette massimo (minimo) allora è unico.

Dimostrazione. Siano $x, y \in Y$ due massimi. Poiché y è un massimo si ha che $x \leq y$ ed allo stesso modo, poiché x è un massimo, $y \leq x$. Si ha quindi

$$x \leq y \quad \wedge \quad y \leq x \quad \Rightarrow \quad x = y.$$

■

Proposizione 8.2 Sia $Y \subset (X, \leq)$ un sottoinsieme di un insieme parzialmente ordinato. Se Y ammette massimo (minimo) x allora x è l'unico elemento massimale (minimale).

Dimostrazione. Sia $y \in Y$ massimale. Allora, essendo x un massimo, si ha $y \leq x$ da cui, essendo y massimale, segue che $y = x$. ■

Definizione 8.6 Sia $(X,\leq)$ un insieme parzialmente ordinato e sia $Y \subseteq X$ un sottoinsieme di X.
1. $y \in X$ è un *minorante* di Y se $\forall z \in Y$ si ha $y \leq z$;
2. $y \in X$ è un *maggiorante* di Y se $\forall z \in Y$ si ha $z \leq y$;
3. $y \in X$ è un *estremo inferiore* (Inf) se è il massimo dei minoranti;
4. $y \in X$ è un *estremo superiore* (Sup) di Y se è il minimo dei maggioranti.

Diciamo che un sottoinsieme di un insieme parzialmente ordinato $(X,\leq)$ è *limitato superiormente* (*inferiormente*) se ammette maggioranti (minoranti).

■ **Esempio 8.7** Sia $(\mathbb{N},\leq)$ e sia $Y=\{4,5,6,7\}$. Allora i numeri $0,1,2,3,4$ sono minoranti di Y, mentre i numeri $7,8,9,10,\ldots$ sono maggioranti. Segue che $\text{Inf}(Y)=4$ e $\text{Sup}(Y)=7$. ■

■ **Esempio 8.8** Sia $(\mathbb{N}^\star,\leq_|)$ e sia $Y=\{2,4,10,20\}$. Allora 2 è un minimo per Y, infatti $2 \leq_| x$ per ogni $x \in Y$. Si osservi che Y non è totalmente ordinato. Quindi l'esistenza del minimo (massimo) non garantisce che l'insieme sia totalmente ordinato. ■

■ **Esempio 8.9** Sia $(\mathbb{N}^\star,\leq_|)$ e sia $Y=\{8,12,20\}$. Allora i minoranti sono $1,2,4$ mentre i maggioranti sono i numeri $120,240,360,\ldots$. Segue che $\text{Inf}(Y)=4$ e $\text{Sup}(Y)=120$. ■

■ **Esempio 8.10** Sia $(X=\{1,2,3,4,9,12,18,36\},\leq_|)$ e sia $Y=\{2,3\}$. Allora l'insieme dei maggioranti di Y, $\{12,18,36\}$, non ammette minimo, quindi non esiste l'estremo superiore. ■

L'ultimo esempio suggerisce la seguente definizione.

Definizione 8.7 Un insieme parzialmente ordinato $(X,\leq)$ si dice *completo* se ogni sottoinsieme non vuoto limitato superiormente (inferiormente) ammette Sup (Inf).

Definizione 8.8 Sia $(X,\leq)$ un insieme parzialmente ordinato. L'ordine si dice *denso* se

$$\forall x,y \in X \quad x \leq y \quad \wedge \quad x \neq y \quad \exists z \in X : z \neq x,y \quad \wedge \quad x \leq z \leq y.$$

Definizione 8.9 Un insieme parzialmente ordinato $(X,\leq)$ si dice *ben ordinato* se ogni sottoinsieme non vuoto ammette minimo.

Si osservi subito che un insieme $(X,\leq)$ ben ordinato è totalmente ordinato. Infatti dati $x,y \in X$, l'insieme $\{x,y\} \subseteq X$ ammette un minimo. Se il minimo è x allora $x \leq y$, mentre se il minimo e y allora $y \leq x$.

8.2 Problemi proposti

Problema 8.1 Sia $D=\{1,2,3,4,6,12,18,36\}$ con la relazione d'ordine data dalla divisibilità: aRb se $a \mid b$. Sia $S=\{4,6\} \subset D$.
1. Con quali elementi di D è in relazione 6?
2. Determinare tutti i maggioranti e tutti i minoranti di S in D.
3. Determinare, se esistono, $\inf(S),\ \sup(S), \max(S), \min(S)$.

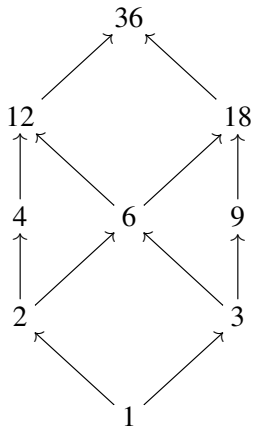
Problema 8.2 Sia X un insieme e siano R_1 e R_2 due relazioni di equivalenza su X.
1. Dimostrare che $R_1 \cap R_2$ è una relazione di equivalenza.
2. Descrivere la partizione di X associata alla relazione $R_1 \cap R_2$ in termini di quelle associate a R_1 e R_2.
3. Esibire un esempio di R_1 e R_2 tali che $R_1 \cup R_2$ non è una relazione di equivalenza.

Problema 8.3 Sia X un insieme e siano S_1 e S_2 due relazioni di ordine su X.
1. È vero che $S_1 \cap S_2$ è una relazione di ordine? Dimostrarlo o esibire un controesempio.
2. È vero che $S_1 \cup S_2$ è una relazione di ordine? Dimostrarlo o esibire un controesempio.

Problema 8.4 Sia R una relazione di ordine parziale su un insieme X. Per ogni $x \in X$ si definisca l'insieme $P_x=\{a \in X : (a,x) \in R\}$. Dimostrare che per ogni $x,y \in X$ si ha

$$(x,y) \in R \quad \Leftrightarrow \quad P_x \subseteq P_y$$

Problema 8.5 — Diagrammi di Hasse. Un insieme parzialmente ordinato *finito* può essere rappresentato graficamente mediante un *diagramma di Hasse* che si disegna nel modo seguente. Se aRb e $a \neq b$, si pone b al di sopra di a. Inoltre si collega a a b tramite un segmento orientato, omettendo i segmenti orientati che sono conseguenza della riflessività (in pratica, si omettono i circoletti intorno ai vari elementi), e anche quelli che sono conseguenza della transitività (se aRb e bRc, allora anche aRc ma non si disegna il corrispondente segmento orientato, visto che non aggiungerebbe nulla a quanto già sappiamo).
Il diagramma di Hasse di un insieme totalmente ordinato finito è "banale": non è altro che un insieme di punti uno sopra l'altro, dove un punto è collegato a quello che gli sta sopra da un segmento verticale orientato verso l'alto (provate, ad esempio, a disegnare il diagramma di Hasse dei numeri naturali da 1 a 5, ordinati tramite l'usuale relazione di minore o uguale). Quindi i diagrammi di Hasse interessanti sono quelli di insiemi ordinati parzialmente ma non totalmente, ossia in cui esistono coppie di elementi non confrontabili.
Ad esempio, sia $D = \{1,2,3,4,6,12,18,36\}$ con la relazione di ordine data dalla divisibilità: aRb se $a \mid b$. Il suo diagramma di Hasse è



Per ognuno dei seguenti insiemi ordinati, scrivere esplicitamente tutti i suoi elementi, e disegnare il suo diagramma di Hasse:

1. $\mathbf{D}_8$, $\mathbf{D}_{10}$, $\mathbf{D}_{12}$, $\mathbf{D}_{15}$, $\mathbf{D}_{24}$, ordinati tramite la divisibilità. Qui $\mathbf{D}_n$ indica l'insieme di tutti i divisori di n (incluso n).
2. $\mathscr{P}(\{a,b\})$, $\mathscr{P}(\{1,2,3\})$, ordinati tramite l'inclusione.

Problema 8.6 — Ordinamento del prodotto cartesiano. Siano (X,R) e (Y,S) due insiemi (parzialmente) ordinati. Allora si può ordinare il prodotto cartesiano $X \times Y$ in almeno due modi diversi:

(a) *Ordinamenti lessicografici.* L'*ordinamento lessicografico* consiste nella relazione d'ordine T su $X \times Y$ definita come segue: dati $(a,b),(c,d) \in X \times Y$, $(a,b)\,T\,(c,d)$ se $a \neq c$ e aRc oppure se $a = c$ e bSd.
Si ha che se R e S sono ordinamenti *totali*, allora anche T è un ordinamento *totale*. Infatti, siano (a,b) e (c,d) due elementi diversi del prodotto cartesiano $X \times Y$. Se $a = c$ allora necessariamente $b \neq d$. Poichè S è un ordinamento totale, bSd e quindi, per definizione $(a,b)\,T\,(c,d)$. Se $a \neq c$, allora, poichè R è un ordinamento totale, aRc e quindi, per definizione, $(a,b)\,T\,(c,d)$.

Si può analogamente definire l'ordinamento *lessicografico inverso* su $X \times Y$: esso consiste nella relazione d'ordine T' su $X \times Y$ definita come segue: dati $(a,b),(c,d) \in X \times Y$, $(a,b)\,T'\,(c,d)$ se

$b \neq d$ e bSd oppure se $b = d$ e aRc.

(b) *Ordinamento prodotto.* Esso consiste nella relazione d'ordine P su $X \times Y$ definita come segue: dati $(a,b), (c,d) \in X \times Y$, $(a,b)\,P\,(c,d)$ se aRc e bSd. Al contrario della definizione precedente, in generale P non è un ordinamento totale nemmeno se R e S sono ordinamenti totali. Ad esempio, in $\mathbb{N} \times \mathbb{N}$ ordinato tramite la relazione prodotto (in altre parole, $(x,y)\,P\,(z,t)$ se $x \leq z$ e $y \leq t$), gli elementi $(0,1)$ e $(1,0)$ non sono confrontabili.

Per ognuno dei seguenti insiemi ordinati, scrivere esplicitamente tutti i suoi elementi, e disegnare il suo diagramma di Hasse:

1. $\{1,2,3\} \times \mathbf{D}_6$ con l'ordinamento prodotto (dove $\{1,2,3\}$ è ordinato tramite l'usuale minore o uguale e $\mathbf{D}_6$ è ordinato tramite la divisibilità).
2. $\{1,2,3\} \times \mathbf{D}_6$ con l'ordinamento lessicografico (dove $\{1,2,3\}$ è ordinato tramite l'usuale minore o uguale e $\mathbf{D}_6$ è ordinato tramite la divisibilità).
3. $\mathbf{D}_6 \times \{1,2,3\}$ con l'ordinamento lessicografico (dove $\mathbf{D}_6$ è ordinato tramite la divisibilità e $\{1,2,3\}$ è ordinato tramite l'usuale minore o uguale).
4. $\mathscr{P}(\{a,b\}) \times \mathscr{P}(\{x\})$, ordinato:
   (i) tramite l'ordinamento prodotto;
   (ii) tramite l'ordinamento lessicografico;
   (iii) tramite l'ordinamento lessicografico inverso
   (dove i due insiemi delle parti sono ordinati dall'inclusione).

Problema 8.7 Sia $(X, \leq)$ un insieme pre ordinato (dove valgono solo le proprietà riflessiva e transitiva) e sia R la relazione su X definita da xRy se e solo se $x \leq y$. Dimostrare che R è equivalenza su X. Nell'insieme quoziente X/R definire la relazione

$$[x] \leq_R [y] \quad \Leftrightarrow \quad x \leq y.$$

Si verifichi che $\leq_R$ definisce una relazione d'ordine parziale su X/R.

Problema 8.8 Sia $(X, \leq)$ un insieme parzialmente ordinato. Sull'insieme X^X di tutte le funzioni di A in sè definiamo la relazione R ponendo, per ogni $f, g \in X^X$,

$$fRg \quad \Leftrightarrow \quad f(x) \leq g(x) \quad \forall x \in X.$$

Si dimostri che R è una relazione d'ordine parziale. Si provi che R è una relazione d'ordine totale se e solo se $|X| = 1$.

Problema 8.9 Mostrare che l'insieme dei numeri razionali $\mathbb{Q}$ con l'ordine definito in (6.3) è denso.

8.3 Il principio del buon ordinamento e l'induzione forte

Prima di enunciare il principio del buon ordinamento diamo la seguente caratterizzazione degli insiemi totalmente ordinati.

Proposizione 8.3 Un insieme parzialmente ordinato $(X, \leq)$ è totalmente ordinato se e solo se ogni sottoinsieme non vuoto finito Y di X ha massimo e minimo.

Dimostrazione.
"$\Rightarrow$" Per induzione su $n = |Y|$. Se $n = 1$ allora $Y = \{x\}$ e x rappresenta sia il massimo che il minimo. Supponiamo che la proposizione sia vera per n e dimostriamola vera quando $|Y| = n+1$. Sia quindi $Y = \{y_1, \ldots, y_{n+1}\} = \{y_1, \ldots, y_n\} \cup \{y_{n+1}\}$. Per ipotesi induttiva esiste $y_i = \min\{y_1, \ldots, y_n\}$ per qualche $i = 1, \ldots, n$. Siccome $(X, \leq)$ è totalmente ordinato si deve avere $y_i \leq y_{n+1} \quad \vee \quad y_{n+1} \leq y_i$. Nel primo caso y_i è un minimo per tutto Y mentre nel secondo caso il minimo è y_{n+1}. Allo stesso modo si dimostra che Y ha un massimo.

"$\Leftarrow$" Siano $x, y \in X$. Allora il sottoinsieme $\{x, y\}$ è finito e quindi ammette massimo è minimo, da cui $x \leq y \quad \vee \quad y \leq x$. In conclusione x e y sono confrontabili. ■

Teorema 8.1 — Principio del Buon Ordinamento. L'ordine definito sui numeri naturali è un buon ordinamento.

Dimostrazione. Sia $E \subseteq \mathbb{N}$ un sottoinsieme non vuoto. Si vuole dimostrare che E ammette un minimo. A tal fine, si consideri il seguente sottoinsieme dei numeri naturali che per costruzione contiene E:

$$E' = \{m \in \mathbb{N} : \exists n \in E \text{ con } n \leq m\}.$$

Si verifica immediatamente che:

(a) $E \subseteq E'$

(b) se $m \in E'$ e $m \leq m'$ allora $m' \in E'$

(c) se $m_o \in E'$ è un minimo di E' allora $m_o \in E$, cioè m_o è un minimo di E.

Per la (c): se $m_o \in E'$ è un minimo di E' allora $m_o \leq n$ per ogni $n \in E \subseteq E'$. Dalla definizione di E' esiste $n_o \in E$ con $n_o \leq m_o$. Segue che $m_o \leq n_o$ e $n_o \leq m_o$ da cui, per la proprietà antisimmetrica, $m_o = n_o \in E$.

Per concludere la dimostrazione basta verificare che E' ammette un minimo. Sia $n_1 \in E'$ (il quale esiste poiché $E \neq \varnothing$) e si consideri $\mathbb{N} \setminus E'$. Per la proprietà (b) se $n \in \mathbb{N} \setminus E'$ allora $n < n_1$. Si trova quindi che

$$\mathbb{N} \setminus E' \subseteq \{0, 1, \ldots, n_1 - 1\}.$$

Segue che $\mathbb{N} \setminus E'$ è finito e per la Proposizione 8.3, essendo $\mathbb{N}$ totalmente ordinato, $\mathbb{N} \setminus E'$ ha un massimo y_o. Mostriamo che $y_o + 1$ è un minimo di E'. Essendo $y_o < y_o + 1$ segue che $y_o + 1 \in E'$ (poiché y_o è il massimo di $\mathbb{N} \setminus E'$). Infine, per ogni $m \in E'$ si ha $y_o < m$ da cui, si veda il Problema 3.1, $y_o + 1 \leq m$. ■

Il Principio del Buon Ordinamento permette di dimostrare la seguente versione del principio di induzione.

Proposizione 8.4 — Induzione forte. Sia $P(n)$ una proposizione che soddisfa alle seguenti due condizioni:

(a) $P(0)$ è vera;

(b) $P(k)$ vera per ogni $k \in \mathbb{N}$ con $0 \leq k < n \quad \Rightarrow \quad P(n)$ vera.

Allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Dimostrazione. Sia $P(n)$ una proposizione che soddisfa (a) e (b) e si definisca

$$S = \{n \in \mathbb{N} : P(n) \text{ è falsa}\} \subseteq \mathbb{N}.$$

La tesi della proposizione è equivalente a dimostrare che $S = \varnothing$. Supponiamo per assurdo che $S \neq \varnothing$, allora, per il Principio del Buon Ordinamento, esiste un minimo $m \in S$. Per la (a), si ha $0 \notin S$ quindi $m > 0$. Inoltre, per ogni $k \in \mathbb{N}$ con $0 \leq k < m$ si ha che $k \notin S$ (poiché m è il minimo) cioè $P(k)$ è vera per ogni $0 \leq k < m$. Segue dalla (b) che $P(m)$ è vera contro l'ipotesi che $m \in S$. ■

Il principio di induzione forte appare, proprio come suggerisce il nome, una versione più forte del principio di induzione. Infatti afferma che per dimostrare che una proposizione è vera per ogni numero naturale basta verificare che è vera per 0 e che se è vera per tutti i numeri minori di un dato n allora è vera per n. Quindi l'induzione forte afferma che, nel passaggio induttivo, si può assumere che la proposizione sia vera per ogni numero minore di n al fine di dimostrare che è vera per n, differentemente dal principio di induzione debole il quale richiede di dimostrare che la proposizione è vera per n assumendo che sia vera solo per $n-1$. Ovviamente il Principio del Buon Ordinamento

è conseguenza della costruzione dei numeri naturali e quindi del principio di induzione debole. Segue che il principio di induzione forte è conseguenza del principio di induzione debole. Un buon esercizio è dimostrare che il principio di induzione forte implica il principio di induzione debole.

In analogia con quello che succede per il principio di induzione (si veda l'Osservazione 3.3) può accadere che una proposizione sia vera per tutti i numeri naturali maggiori o uguali di un dato numero naturale n_0. In tali condizioni il principio di induzione forte diventa:

Sia $n_0 \in \mathbb{N}$ e sia $P(n)$ una proposizione che soddisfa alle seguenti due condizioni:
(a) $P(n_0)$ è vera;
(b) $P(k)$ vera per ogni $k \in \mathbb{N}$ con $n_0 \leq k < n \quad \Rightarrow \quad P(n)$ vera.
Allora $P(n)$ è vera per ogni $n \geq n_0$.

■ **Esempio 8.11** Sia

$P(n) =$ il numero naturale n si può esprimere come somma di un certo numero di 3 e di un certo numero di 5.

Dimostrare che $P(n)$ è vera per ogni $n \geq 8$.

Usiamo il principio di induzione forte. Verifichiamo che $P(n)$ è vera per $n = 8$. Infatti, $8 = 3+5$ quindi $P(8)$ è vera. Supponiamo adesso che sia vera per tutti i k con $8 \leq k < n$ e dimostriamo che $P(n)$ è vera. A tal scopo si osservi che $n = 3+(n-3)$ ed essendo $n-3 < n$ la proposizione è vera per $n-3$ (per ipotesi induttiva), cioè $n-3$ può essere espresso come somma di un certo numero di 3 e di un certo numero di 5. Segue che anche n può essere espresso come somma di un certo numero di 3 e di un certo numero di 5, basta aggiungere 3 all'espressione che formava $n-3$.
La dimostrazione fatta presenta però un problema nella base induttiva. Infatti, nel passaggio induttivo dimostriamo che è vera per n assumendo che sia vera per $n-3$. Se $n = 9, 10$ non possiamo applicare quanto detto sopra poiché $10-3 = 7 < 8$ e $9-3 = 6 < 8$. Quindi bisogna verificare direttamente che sia vera anche per $n = 9, 10$. Ovviamente $9 = 3+3+3$ e $10 = 5+5$ quindi è vera anche per $n = 9, 10$. ■

Forti dell'osservazione fatta nell'esempio precedente il lettore dovrebbe risolvere il seguente esercizio.

Esercizio 8.1 Cercare l'errore nella seguente dimostrazione per induzione. Si consideri la proposizione:

$P(n) =$ *preso un insieme di n cavalli tutti i cavalli dell'insieme hanno lo stesso colore.*

Dimostriamo che $P(n)$ è vera per ogni $n \geq 1$.

$P(1)$ è vera. In un insieme con un solo cavallo è evidente che tutti i cavalli hanno lo stesso colore.

Si supponga che $P(n)$ sia vera. Sia A un insieme con $n+1$ cavalli. Se si toglie un cavallo a da A rimangono n cavalli che, per l'ipotesi induttiva, sono dello stesso colore (diciamo bianco per fissare le idee). Ora si rimetta il cavallo a dentro A e si tolga un altro cavallo diverso dal precedente; di nuovo si trova un insieme con n cavalli, quindi tutti dello stesso colore. Questo significa che anche il cavallo a è bianco concludendo la dimostrazione.

Esercizio 8.2 Dimostrare che il Principio del Buon Ordinamento implica il Principio di Induzione Debole.

Esercizio 8.3 Cercare l'errore nella seguente dimostrazione per induzione. Si consideri la proposizione:

$$P(n): \quad 2^n = 1$$

Dimostrare che $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Il caso base $P(0)$ è valido poiché $2^0 = 1$. Applichiamo il principio di induzione forte: supponiamo che $P(k)$ sia vera per tutti $0 \leq k \leq n$. Dimostriamo che $P(n+1)$ è vera:

$$2^{n+1} = \frac{2^n \cdot 2^n}{2^{n-1}} = \frac{1 \cdot 1}{1} = 1\,.$$

8.4 Il Lemma di Zorn

Definizione 8.10 Sia $(X, \leq)$ un insieme parzialmente ordinato. Un sottoinsieme $C \subseteq X$ si dice *catena* se $(C, \leq)$ è totalmente ordinato. Se C è finito chiamiamo $|C|$ la lunghezza della catena.

■ **Esempio 8.12** Si consideri $(\mathbb{N}^*, \leq_|)$ e sia

$$C = \{n \in \mathbb{N}^* : n = 2^k,\ k \in \mathbb{N}\}.$$

Si verifica facilmente che C è una catena. ■

■ **Esempio 8.13** Sia $\{A_i\}_{i=1}^n$ una famiglia di sottoinsiemi di un dato insieme X tali che

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n$$

Allora $C = \{A_1, A_2, \ldots, A_n\}$ è una catena dell'insieme parzialmente ordinato $(\mathscr{P}(X), \leq_\subseteq)$. ■

Definizione 8.11 Un insieme parzialmente ordinato $(X, \leq)$ si dice *induttivo* se ogni catena ammette maggioranti.

Proposizione 8.5 Se X è un insieme finito, allora un qualsiasi ordine parziale su X è induttivo.

Dimostrazione. Sia $(X, \leq)$ parzialmente ordinato e sia $C \subseteq X$ una catena. Allora $(C, \leq)$ è un insieme finito totalmente ordinato e, per la Proposizione 8.3, ammette un massimo y_o che è anche un maggiorante di C. ■

■ **Esempio 8.14** Sia

$$X = \{A \subseteq \mathbb{N} : A \text{ è finito}\} \subseteq \mathscr{P}(\mathbb{N})$$

con l'ordine parziale dato dall'inclusione. L'insieme $(X, \leq_\subseteq)$ non è induttivo. Infatti la catena

$$\{0\} \subseteq \{0,1\} \subseteq \{0,1,2\} \subseteq \cdots$$

non ha maggioranti poiché un sottoinsieme dei naturali che li contiene tutti è $\mathbb{N}$ stesso il quale non è finito e quindi non appartiene a X. Si osservi che X non ammette elementi massimali. Per verificarlo, si supponga che $A \in X$ sia massimale. Essendo A finito esiste un numero naturale $n_o \notin A$. Allora $B = A \cup \{n_o\} \in X$ e $A \subseteq B$ con $A \neq B$ contro l'ipotesi che A sia massimale. ■

Osservazione 8.1 L'insieme vuoto $\varnothing$ è una catena di un insieme parzialmente ordinato $(X,\leq)$. Infatti l'implicazione

$$\forall x,y\in\varnothing \quad\Rightarrow\quad x\leq y \quad\vee\quad y\leq x$$

è vera poiché la tesi è falsa (non esistono elementi dell'insieme vuoto). Con un ragionamento analogo si può dimostrare che l'insieme dei maggioranti dell'insieme vuoto è tutto X.

Il prossimo risultato mette in relazione l'essere induttivo con l'esistenza di elementi massimali.

Teorema 8.2 — Lemma di Zorn. Sia $(X,\leq)$ un insieme parzialmente ordinato induttivo. Allora X ammette un elemento massimale.

Dimostrazione. Supponiamo per assurdo che X non abbia elementi massimali. Sia C una catena di X e sia $c\in X$ un suo maggiorante. Siccome X non ammette elementi massimali, esiste un elemento $x\in X$ tale che $c<x$. Cioè per ogni catena esiste almeno un maggiorante che non appartiene alla catena. Segue che per ogni catena C possiamo definire il seguente insieme non vuoto costituito dai maggioranti non appartenenti alla catena:

$$M_C=\{x\in X:\forall c\in C, c<x\wedge x\notin C\}.$$

Sia $\mathscr{C}=\{C\subseteq X: C \text{ è una catena di } X\}$ e sia $\{M_C\}_{C\in\mathscr{C}}$ la famiglia di tutti gli insiemi M_C al variare di C, catena di X. Tale famiglia non è vuota in quanto X vi appartiene (dall'Osservazione 8.1 X è l'insieme dei maggioranti della catena $C=\varnothing$). Per l'assioma della scelta esiste una funzione di scelta

$$\begin{aligned}\varphi:\mathscr{C}&\to\bigcup_{C\in\mathscr{C}}M_C\\ C&\mapsto\varphi(C)=x_C,\end{aligned}$$

dove x_C è un maggiorante stretto (cioè $x_C\notin C$) per la catena C.
Prima di continuare con la dimostrazione introduciamo una classe particolare di sottoinsiemi di X.

Definizione 8.12 Un sottoinsieme $A\subseteq X$ è detto *conforming* se

(*i*) $(A,\leq)$ è ben ordinato (quindi totalmente ordinato per l'Osservazione 8.1);

(*ii*) per ogni $a\in A$ si ha

$$\varphi(P(A,a))=a$$

dove $P(A,a)=\{y\in A: y<a\}$ è il segmento iniziale di a in A.

Dimostriamo la seguente proprietà dei sottoinsiemi conforming di X che ci servirà nel proseguo della dimostrazione del Lemma di Zorn.

Proposizione 8.6 Siano A,B due sottoinsiemi conforming di X tali che $A\neq B$. Allora o $A=P(B,b)$ per un certo $b\in B$, oppure $B=P(A,a)$ per un certo $a\in A$.

Dimostrazione. Essendo $A\neq B$ possiamo supporre che $A\setminus B\neq\varnothing$. Essendo $A\setminus B\subseteq A$ ed essendo A ben ordinato esiste un minimo $a\in A\setminus B$. Allora

$$P(A,a)\subseteq B.$$

Infatti, se $x\in P(A,a)$ non appartenesse a B, allora $x\in A\setminus B$. Ma a è il minimo di $A\setminus B$ quindi $a\leq x$ contro l'ipotesi che $x\in P(A,a)$, cioè $x<a$.

Dimostriamo che $B = P(A,a)$. Supponiamo per assurdo che $B \setminus P(A,a) \neq \varnothing$ e chiamiamo con $b \in B \setminus P(A,a)$ il minimo. Sia ora $z \in A \setminus P(B,b)$ il minimo. Allora

$$P(A,z) = P(B,b).$$

Per dimostrare l'ultima uguaglianza si procede dimostrando la doppia inclusione.

$P(A,z) \subseteq P(B,b)$: se $x \in P(A,z)$ allora $x < z$, ma z è il minimo di $A \setminus P(B,b)$ quindi $x \in P(B,b)$;

$P(B,b) \subseteq P(A,z)$: consideriamo $y \in P(B,b)$ allora $y < b$. Dalla definizione di b si trova che y deve appartenere a $P(A,a)$ e quindi $y \in A$ con $y < b$. Se avessimo $z \leq y < b$ allora $z \in P(B,b)$ che contraddice la definizione di z. Quindi si deve avere che $y < z$ e quindi $y \in P(A,z)$.

Inoltre se $a < z$ allora $a \in P(A,z) = P(B,b)$ e quindi $a \in B$ contro l'ipotesi che $a \in A \setminus B$. Segue che $z \leq a$. Infine

$$z = \varphi(P(A,z)) = \varphi(P(B,b)) = b$$

da cui $z \neq a$, cioè $z < a$. Quindi

$$b = z \in P(A,a)$$

che contraddice la definizione di b. ■

La proposizione precedente mostra che la famiglia dei sottoinsiemi conforming di X forma una catena rispetto all'inclusione. Utilizzando questo fatto si vede che se A è un sottoinsieme conforming di X e $a \in A$, dato un elemento $x \in X$ per cui $x < a$, allora si ha una delle seguenti possibilità:

- $x \in A$;
- x non appartiene a nessun sottoinsieme conforming di X.

Infatti, se $x \notin A$ e $x \in B$ con B conforming si hanno due possibilità:

- $B = P(A,y) = \{z \in A : z < y\}$ per un certo $y \in A$, da cui, per definizione x apparterebbe ad A;
- $A = P(B,b) = \{z \in B : z < b\}$ per un certo $b \in B$. Se $b \leq x$, cioè se $x \notin A$, allora $a < b \leq x$ che contraddice l'ipotesi su x ($x < a$). Se invece $x < b$ allora $x \in P(B,b) = A$ e x apparterrebbe ad A.

Osserviamo adesso che un insieme conforming esiste. Infatti l'insieme vuoto $\varnothing$ è una catena di X, quindi possiamo applicare la funzione φ all'insieme vuoto e ottenere un certo elemento $\varphi(\varnothing) = x_0 \in X$. Sia $A = \{x_0\}$, allora A è ben ordinato ed inoltre $\varphi(P(\{x_0\},x_0)) = \varphi(\varnothing) = x_0$, quindi A è conforming.

Sia adesso

$$U = \bigcup_{A \text{ conforming}} A$$

l'unione di tutti i sottoinsiemi conforming di X. Verifichiamo che U è un sottoinsieme conforming di X:

(i) Mostriamo che $(U, \leq)$ è ben ordinato. Sia $Y \subseteq U$ un sottoinsieme di U. Se Y è contenuto in un sottoinsieme conforming A, allora Y ammette minimo poiché A è ben ordinato. Se Y non è completamente contenuto in un solo sottoinsieme conforming di X, allora $Y = U$. Ma in questo caso x_0 è un minimo di U (il singoletto $\{x_0\}$ è contenuto in tutti i sottoinsiemi conforming) e quindi di Y;

(ii) Prendiamo un elemento $u \in U$, allora esiste un sottoinsieme conforming A tale che $u \in A$. Sia $P(U,u)$ il segmento iniziale di u in U. Un qualunque elemento $y \in P(U,u)$ deve appartenere ad A, altrimenti non apparterrebbe a nessun sottoinsieme conforming di X, il che è assurdo poiché U è l'unione di tutti i sottoinsiemi conforming di X. Quindi

$$P(U,u) = P(A,u) \Rightarrow \varphi(P(U,u)) = \varphi(P(A,u)) = u.$$

Poiché U è una catena possiamo considerare la sua immagine attraverso la funzione φ:

$$\varphi(U) = z.$$

Consideriamo ora il sottoinsieme $U \cup \{z\}$ di X e dimostriamo che è un sottoinsieme conforming di X.

(i) Mostriamo che è ben ordinato. Sia $Y \subseteq U \cup \{z\}$, ci sono due casi. Se $Y \subseteq U$ allora Y ha un minimo poiché U è conforming. Se $z \in Y$ allora $Y = Y' \cup \{z\}$ con $Y' \subseteq U$. Sia $y_o \in Y'$ il minimo. Essendo z un maggiorante per U segue che $y_o < z$ da cui y_o è un minimo per tutto $Y = Y' \cup \{z\}$.

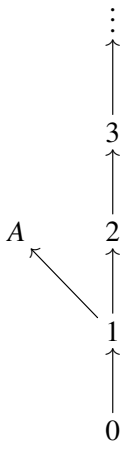
(ii) Sia adesso $x \in U \cup \{z\}$. Se $x \in U$, allora siccome $x < z$ si ha che $P(U \cup \{z\}, x) = P(U, x)$ da cui, siccome U è un sottoinsieme conforming, $\varphi(P(U \cup \{z\}, x)) = \varphi(P(U, x)) = x$. Se invece $x = z$ allora $P(U \cup \{z\}, z) = U$ e quindi $\varphi(P(U \cup \{z\}, z)) = \varphi(U) = z$.

Quindi $U \cup \{z\}$ è un sottoinsieme conforming che contiene U. Ma siccome U è l'unione di tutti i sottoinsiemi conforming di X si perviene ad una contraddizione che produce l'assurdo cercato alla non esistenza di un elemento massimale. ■

■ **Esempio 8.15** Mostriamo con un esempio che il viceversa del Lemma di Zorn non vale. Cioè esistono insiemi parzialmente ordinati che ammettono almeno un elemento massimale ma non sono induttivi. Sia $\mathbb{N}$ ordinato con l'ordine naturale $\leq$ e sia A un insieme qualunque. Nell'insieme $\mathbb{N} \cup \{A\}$ introduciamo la seguente relazione

$$a \leq_A b \quad \Leftrightarrow \quad \begin{cases} a, b \in \mathbb{N} \quad \wedge \quad a \leq b \\ a = 1 \quad \wedge \quad b = A \\ a = b = A \end{cases}$$

La relazione $\leq_A$ definisce una relazione d'ordine parziale su $\mathbb{N} \cup \{A\}$ (verificare) il cui diagramma di Hasse è riportato sotto:



L'elemento A è un massimale poiché l'unico elemento confrontabile con A, cioè 1, è minore di A. Ciò nonostante l'insieme $\mathbb{N}$ è una catena di $\mathbb{N} \cup \{A\}$ che non ammette maggioranti.

■

9. Cardinalità di insiemi infiniti

9.1 Confronto tra le cardinalità degli insiemi

Quando abbiamo trattato gli insiemi finiti abbiamo definito la cardinalità di un insieme finito come l'unico numero naturale $n \in \mathbb{N}$ per il quale esiste una biezione tra l'insieme $\{1,2,\ldots,n\}$ e X. Se l'insieme X non è finito, cioè se è infinito tale biezione non esiste per tutti i numeri naturali e sembra perciò difficile immaginare come definire la cardinalità di un insieme infinito. La risposta ovvia sarebbe: *la cardinalità di un insieme infinito è infinita*. Tale risposta ha ovviamente un suo significato e non è sbagliata in principio. Però la domanda corretta da porsi è la seguente: *dati due insiemi infiniti X e Y, questi hanno la stessa "infinità" di elementi?* Questa domanda è molto più complessa di quanto possa apparire a prima vista e l'argomento di questo capitolo è incentrato proprio su un tentativo di dare un senso a tale domanda.

Non daremo una definizione di cardinalità per un insieme qualunque ma, invece, forniremo un metodo per confrontare le cardinalità di due insiemi. Iniziamo con la seguente definizione.

Definizione 9.1 Siano X e Y due insiemi. Diciamo che X e Y sono *equipotenti*, scriviamo $|X| = |Y|$ se esiste una biezione tra X e Y.

Nel caso di insiemi finiti, l'ultima definizione non è necessaria poiché insiemi finiti con la stessa cardinalità sono per costruzione in corrispondenza biunivoca. Inoltre, sempre quando X e Y sono due insiemi finiti, vale la seguente affermazione:

$$|X| \leq |Y| \quad \Leftrightarrow \quad \textit{esiste una funzione iniettiva } f : X \to Y$$

Forti di questo fatto possiamo introdurre, per insiemi qualunque, la seguente relazione tra le rispettive cardinalità.

Definizione 9.2 Siano X e Y due insiemi. Diciamo che $|X| \leq |Y|$ se e solo se esiste una funzione iniettiva $f : X \to Y$.

L'aver utilizzato il simbolo $\leq$ suggerisce che la relazione sia una relazione d'ordine parziale. Per dimostrarlo osserviamo che l'applicazione $Id_X : X \to X$ è iniettiva quindi la relazione è riflessiva, cioè $|X| \leq |X|$. Inoltre se $|X| \leq |Y|$ e $|Y| \leq |Z|$ allora esistono due funzioni iniettive $f : X \to Y$ e $g : Y \to Z$. Segue che la composizione $g \circ f : X \to Z$ definisce una funzione iniettiva da X in Z e quindi $|X| \leq |Z|$. Abbiamo quindi dimostrato la proprietà transitiva. Per concludere bisogna dimostrare la proprietà antisimmetrica, cioè che se esiste una funzione iniettiva da X in Y e una funzione iniettiva da Y in X allora esiste una funzione biettiva da X in Y. Quest'ultima affermazione,

ancorché vera, non è di immediata dimostrazione e rappresenta l'enunciato di un famoso teorema.

Teorema 9.1 — Teorema di Cantor-Bernstein. Siano S e T due insiemi non vuoti. Se esistono $r : S \to T$ iniettiva e $q : T \to S$ iniettiva allora esiste una biezione tra T e S.

Prima di dimostrare il teorema enunciamo il seguente lemma.

Lemma 9.1 Sia $f : X \to X$ una funzione iniettiva e sia $Y \subseteq X$ tale che $f(X) \subseteq Y \subseteq X$. Allora esiste una biezione tra Y e X.

Dimostrazione. La dimostrazione è piuttosto tecnica ed è facoltativa. Chi desidera studiarla la trova nel libro di testo. ■

Dimostriamo adesso il Teorema di Cantor-Bernstein

Dimostrazione del Teorema 9.1. Si consideri la composizione $f = q \circ r : S \to S$ la quale è iniettiva poiché composizione di funzioni iniettive. Per costruzione si ha $f(S) \subseteq q(T) \subseteq S$. Quindi, per il Lemma 9.1, esiste una biezione tra $q(T)$ e S. Essendo $q : T \to S$ iniettiva l'insieme $q(T)$ è in corrispondenza biunivoca con T. Componendo le ultime due biezioni si perviene alla biezione desiderata tra T e S. ■

A questo punto sappiamo che la relazione introdotta tra le cardinalità di insiemi qualunque è una relazione d'ordine parziale. Di fatto tale relazione definisce un ordine totale, nel senso che dati due insiemi X e Y le corrispondenti cardinalità sono confrontabili. Quest'ultimo risultato, noto come Teorema di Hartgos è una bella applicazione del Lemma di Zorn. Il suo enunciato formale è il seguente.

Teorema 9.2 Siano S e T due insiemi non vuoti. Allora o esiste una funzione iniettiva da S in T o esiste una funzione iniettiva da T in S.

Dimostrazione. Sia

$$\mathscr{F} = \{J_A : A \to T : A \subseteq S,\ J_A \text{ iniettiva}\}.$$

Definiamo la seguente relazione binaria su $\mathscr{F}$:

$$J_A \leq J_B \quad \Leftrightarrow \quad A \subseteq B \quad \wedge \quad J_B|_A = J_A\,.$$

Si dimostra facilmente (Esercizio) che la relazione sopra definisce un ordine parziale su $\mathscr{F}$. Dimostriamo che $(\mathscr{F}, \leq)$ è induttivo. Data una catena $C = \{J_{B_i}\}_{i \in I}$ di $\mathscr{F}$ poniamo $B = \cup_{i \in I} B_i$ e definiamo $J_B : B \to T$ come $J_B(b) = J_{B_i}(b)$ dove B_i è uno qualsiasi degli insiemi della catena C che contiene b. A questo punto il lettore deve convincersi che la definizione di J_B non dipende dal particolare insieme B_i scelto, cioè che se $b \in B_j$ con $i \neq j$ allora $J_{B_i}(b) = J_{B_j}(b)$. Per come è costruita J_B segue che

$$J_{B_i} \leq J_B \quad \forall J_{B_i} \in C$$

quindi J_B è un maggiorante per C. Essendo C una generica catena, segue che $\mathscr{F}$ è induttivo. Dal Lemma di Zorn esiste un elemento massimale di $\mathscr{F}$:

$$J_0 : B_0 \to T\,.$$

Si presentano due casi

1. $B_0 = S$. In questo caso la funzione $J_0 : S \to T$ definisce una funzione iniettiva da S in T.

2. $S \setminus B_0 \neq \varnothing$. In questo caso esiste $x_0 \in S \setminus B_0$. Mostriamo che $J_0(B_0) = T$, cioè che J_0 è suriettiva. Se per assurdo non fosse suriettiva allora esisterebbe $y_0 \in T \setminus J_0(B_0)$. Definiamo in $B_0 \cup \{x_0\}$ la seguente funzione

$$\begin{array}{rccl} \xi: & B_0 \cup \{x_0\} & \to & T \\ & x & \mapsto & \xi(x) = \begin{cases} J_0(x) & \text{se } x \in B_0 \\ y_0 & \text{se } x = x_0 \end{cases} \end{array}$$

La funzione ξ è iniettiva (verificare) e $J_0 \leq \xi$ con $J_0 \neq \xi$ contraddicendo il fatto che J_0 è massimale. Quindi $J_0 : B_0 \to T$ è suriettiva da cui segue, dalla Proposizione 2.3, che esiste una funzione iniettiva da T in $B_0 \subseteq S$.

■

9.2 Insiemi numerabili

Iniziamo con la seguente definizione

Definizione 9.3 (a) Un insieme X è *numerabile* se $|X| = |\mathbb{N}|$, ovvero se esiste una funzione biettiva tra X e $\mathbb{N}$. Indichiamo la cardinalità dei numeri naturali con $\aleph_o$ (Aleph con zero, dove Aleph è la prima lettera dell'alfabetto ebraico). Quindi un insieme è numerabile se $|X| = \aleph_o$.

(b) Un insieme X infinito si dice *non numerabile* se non esiste una funzione biettiva tra X e $\mathbb{N}$.

Osservazione 9.1 Se un insieme infinito X non è numerabile, dalla Proposizione 4.5 segue che $|\mathbb{N}| < |X|$.

Vediamo adesso alcuni esempi di insiemi numerabili.

Proposizione 9.1 L'insieme dei numeri interi è numerabile.

Dimostrazione. Si consideri la funzione

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{Z} \\ & n & \mapsto & f(n) = \begin{cases} 0 & \text{se } n = 0 \\ \frac{n}{2} & \text{se } n \text{ è pari} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari} \end{cases} \end{array}$$

La funzione f è biettiva. Infatti siano $n, n' \in \mathbb{N}$ con $f(n) = f(n')$. Si hanno i seguenti casi:

1. se n, n' sono pari, allora $n/2 = n'/2$ da cui $n = n'$;
2. se n, n' sono dispari, allora $-(n+1)/2 = -(n'+1)/2$ da cui $n = n'$;
3. se n è pari e n' è dispari, allora $f(n) = f(n')$ non può avversi poiché implicherebbe l'uguaglianza assurda $n/2 = -(n'+1)/2$.

Abbiamo quindi dimostrato che f è iniettiva. Per la suriettività, sia $z \in \mathbb{Z}$ un numero intero. Se z è zero allora è immagine di zero. Se z è positivo allora è immagine di $2z$ mentre se z è negativo sarà immagine di $-2z-1$. ■

Proposizione 9.2 Il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ è numerabile.

Dimostrazione. Si consideri la funzione

$$\begin{array}{rccl} f: & \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ & (m,n) & \mapsto & f(m,n) = 2^m(2n+1) - 1 \end{array}$$

Dimostriamo che f è biettiva. Per la iniettività, siano $(m,n),(r,s) \in \mathbb{N}\times\mathbb{N}$ tali che $f(m,n) = f(r,s)$. Allora si deve avere $2^m(2n+1) = 2^r(2s+1)$. Se $m \neq r$ possiamo supporre che $m > r$ da cui, applicando la legge di cancellazione, si perviene all'identità $2^{m-r}(2n+1) = (2s+1)$ la quale è assurda poiché a sinistra vi è un numero pari mentre a destra uno dispari. Quindi $m = r$ e sostituendo in $2^m(2n+1) = 2^r(2s+1)$ si conclude che $n = s$. Dimostriamo che f è suriettiva. Ovviamente $f(0,0) = 0$. Sia $k \in \mathbb{N}$ un numero naturale. Se k è pari allora $k+1$ è dispari, cioè esiste un $n \in \mathbb{N}$ tale che $k+1 = 2n+1$. Segue che $f(0,n) = 2^0(2n+1)-1 = (k+1)-1 = k$. Se k è dispari allora $k+1$ è pari. Quindi $k+1 = 2\ell$. Se ℓ non è dispari allora $\ell = 2\ell'$ ed iterando tale processo si perviene a

$$k+1 = \underbrace{2\cdots 2}_{m \text{ volte}}\cdot\bar{\ell}$$

con $\bar{\ell}$ dispari o, eventualmente, $\bar{\ell} = 1$. Quindi esiste un $n \in \mathbb{N}$ con $\bar{\ell} = 2n+1$ e $f(m,n) = 2^m(2n+1)-1 = (k+1)-1 = k$. ■

Osservazione 9.2 — Facoltativa. Si consideri una funzione non costante $L : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ polinomiale di primo grado: $L(m,n) = am+bn+c$. Si osservi che $c = L(0,0)$ è necessariamente un numero naturale. Lo stesso vale per $a = L(1,0)-c$ e $b = L(0,1)-c$. Quindi a e b devono essere numeri naturali, non entrambi zero. Ma allora $L(m,n) = L(m-b,n+a)$, per ogni $m \geq b$. Quindi L non può essere iniettiva. Segue che non esiste una biezione lineare da $\mathbb{N}\times\mathbb{N}$ su $\mathbb{N}$.

Esiste invece una biezione quadratica. Si consideri la *funzione di accoppiamento di Cantor* $C : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ definita da

$$C(m,n) = \sum_{j=0}^{m+n} j + m = \frac{1}{2}(m+n)(m+n+1)+m\,.$$

Per verificare che C sia una biezione, abbiamo bisogno della proprietà seguente:

$$\textit{Se } m+n < m'+n', \textit{ allora } C(m,n) < C(m',n')$$

Per dimostrare la proprietà sopra, si osservi che, soggetto al vincolo $m+n = k$, il valore massimo di $C(m,n)$ è $C(k,0) = \frac{1}{2}k(k+1)+k$ e il valore minimo di $C(m,n)$ è $C(0,k) = \frac{1}{2}k(k+1)$. Se $k' \geq k+1$, allora per $m+n < m'+n' = k'$ si trova

$$C\left(m',n'\right) \geq C\left(0,k'\right) = \frac{1}{2}k'(k'+1) \geq \frac{1}{2}(k+1)(k+2) = \frac{1}{2}k(k+1)+k+1 > C(k,0) \geq C(m,n).$$

Dimostriamo adesso che C è iniettiva. Se $C(m,n) = C(m',n')$ allora $m+n = m'+n'$ da cui, per la definizione di C, segue immediatamente che $m = m'$ che assieme a $m+n = m'+n'$ implicano $n = n'$.
Dimostriamo adesso che C è suriettiva. Sia $z \in \mathbb{N}$ e sia $t_k = \frac{1}{2}k(k+1)$ il più grande numero triangolare non superiore a z. Sia $m = z-t_k$ e $n = k-m$. Allora $C(m,n) = z$.

Nessuna altra biezione polinomiale da $\mathbb{N}\times\mathbb{N}$ su $\mathbb{N}$, a parte $C(m,n)$ e la sua riflessione $C(n,m)$, è nota in letteratura. *Rudolf Fueter* e *George Pólya*, nel 1923, hanno dimostrato che non esistono altre funzioni quadratiche biunivoche e nel 1978 *John S. Lew* e *Arnold L. Rosenberg* hanno dimostrato che non esistono biezioni che siano date da un polinomio di grado 3. È ancora un problema aperto dimostrare che l'accoppiamento di Cantor sia l'unica funzione polinomiale biettiva da $\mathbb{N}\times\mathbb{N}$ su $\mathbb{N}$.

Sia $\{A_i\}_{i\in I}$ una famiglia di insiemi. Supponiamo che I sia numerabile, quindi identificabile con $\mathbb{N}$, e che per ogni $i \in I$ l'insieme A_i sia numerabile. Allora per ogni $i \in I$ esiste una funzione biettiva $f_i : \mathbb{N} \to A_i$. Utilizzando la Proposizione 9.2 si dimostra la numerabilità dell'unione degli A_i.

Proposizione 9.3 Sia $\{A_i\}_{i\in\mathbb{N}}$ una famiglia numerabile di insiemi numerabili. Allora $\bigcup_{i\in\mathbb{N}} A_i$ è numerabile.

Dimostrazione. Si consideri la funzione

$$\begin{array}{rccc} \varphi: & \mathbb{N}\times\mathbb{N} & \to & \bigcup_{i\in\mathbb{N}} A_i \\ & (m,n) & \mapsto & f_m(n) \end{array}$$

dove $f_m : \mathbb{N} \to A_m$, $m \in \mathbb{N}$, è biettiva. Dimostriamo che φ è suriettiva. Sia $x \in \cup_{i\in\mathbb{N}} A_i$, allora esiste $m \in \mathbb{N}$ tale che $x \in A_m$. Poiché $f_m : \mathbb{N} \to A_m$ è suriettiva esiste $n \in \mathbb{N}$ con $f_m(n) = x$, cioè $\varphi(m,n) = x$. Poiché $\varphi : \mathbb{N}\times\mathbb{N} \to \cup_{i\in\mathbb{N}} A_i$ è suriettiva, dalla Proposizione 2.3, esiste una funzione iniettiva da $\cup_{i\in\mathbb{N}} A_i$ in $\mathbb{N}\times\mathbb{N}$. Quindi $|\cup_{i\in\mathbb{N}} A_i| \leq |\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$. Adesso, essendo la funzione inclusione $A_1 \to \cup_{i\in\mathbb{N}} A_i$ iniettiva segue che $|\mathbb{N}| \leq |\cup_{i\in\mathbb{N}} A_i|$ che, assieme all'antissimetria, implicano che $|\mathbb{N}| = |\cup_{i\in\mathbb{N}} A_i|$. ■

Osservazione 9.3 In generale, valgono le seguenti affermazioni che utilizzeremo senza dimostrazione.

1. Dati due insiemi infiniti X e Y
$$|X\times Y| = \max\{|X|,|Y|\}$$
2. Dati due insiemi infiniti X e Y
$$|X\cup Y| = \max\{|X|,|Y|\}$$
3. Se X non è numerabile e Y è numerabile, allora
$$|X\setminus Y| = |X|.$$

■ **Esempio 9.1** Utilizzando la Proposizione 9.3 possiamo verificare che l'insieme dei numeri razionali è numerabile. A tal scopo basta scrivere

$$\mathbb{Q} = \frac{\mathbb{Z}\times\mathbb{Z}^*}{R} = \{[a,b] : a \in \mathbb{Z}, b \in \mathbb{Z}^*\} = \bigcup_{a\in\mathbb{Z}} \{[a,b] : b \in \mathbb{Z}^*\}$$

come unione numerabile di insiemi numerabili. ■

Non tutti gli insiemi sono numerabili. Qui non svolgiamo una trattazione formale sugli insiemi non numerabili ma ci limitiamo a fornire un primo esempio.

■ **Esempio 9.2** L'insieme $\mathscr{P}(\mathbb{N})$ non è numerabile. Infatti, dal Teorema di Cantor, non esiste alcuna funzione suriettiva da $\mathbb{N}$ in $\mathscr{P}(\mathbb{N})$ e quindi non può esistere una funzione biettiva. Mentre la funzione

$$\begin{array}{rccc} \varphi: & \mathbb{N} & \to & \mathscr{P}(\mathbb{N}) \\ & n & \mapsto & \{n\} \end{array}$$

è iniettiva. Quindi $|\mathbb{N}| < |\mathscr{P}(\mathbb{N})|$. ■

Indichiamo la cardinalità dell'insieme $\mathscr{P}(\mathbb{N})$ con $2^{\aleph_o}$ (tale notazione emula il fatto che per un insieme finito X si ha $|\mathscr{P}(X)| = 2^{|X|}$).

Osservazione 9.4 Una domanda spontanea che ci si può porre è se esistono insiemi la cui cardinalità sia strettamente compresa tra $\aleph_o$ e $2^{\aleph_o}$. La risposta non è affatto banale e rappresenta uno dei grandi problemi della matematica del ventesimo secolo noto come *Ipotesi del Continuo* il cui enunciato è il seguente: *non esiste un insieme X tale che* $\aleph_o < |X| < 2^{\aleph_o}$. Nel 1940, *Kurt Gödel* dimostrò che l'ipotesi del continuo non può essere dimostrata falsa usando il sistema di assiomi di Zermelo-Fraenkel, neppure con l'aggiunta dell'assioma della scelta. Mentre, nel 1963, *Paul Cohen* dimostrò che l'ipotesi del continuo non può essere neppure dimostrata vera a partire da quegli assiomi. Il risultato complessivo è che l'ipotesi del continuo è indipendente dal sistema di assiomi di Zermelo-Fraenkel e dall'assioma della scelta.

9.3 Problemi proposti

Problema 9.1 Sia X un insieme infinito. Dimostrare che per ogni $x \in X$, esiste una biezione tra X e $X \setminus \{x\}$.

Problema 9.2 Dimostrare che un insieme infinito X è numerabile se e solo se esiste una funzione suriettiva da $\mathbb{N}$ in X.

10. I numeri reali

10.1 Premessa

Nell'insieme dei numeri razionali abbiamo definito un ordine totale. Tale ordine però non è completo. Per mostrare questo esibiamo un esempio di un sottoinsieme di $\mathbb{Q}$ limitato inferiormente che non ammette estremo inferiore. Sia

$$A = \{q \in \mathbb{Q} \colon q > 0 \quad \wedge \quad q^2 > 2\}.$$

L'insieme dei minoranti di A è

$$B = \{q \in \mathbb{Q} \colon q < 0\} \cup \{q \in \mathbb{Q} \colon q \geq 0 \quad \wedge \quad q^2 < 2\}.$$

Si osservi che non esiste un numero razionale q tale che $q^2 = 2$[1]. Mostriamo che B non ha massimo, cioè per ogni $q \in B$ esiste $p \in B$ con $q < p$. Infatti, sia $q \in B$. Se $q \leq 0$ allora $q < 1$ e $1 \in B$. Se $q > 0$ allora si ha

$$\begin{cases} q > 0 \\ q^2 < 2 \end{cases} \quad \Rightarrow \quad \begin{cases} 2q+1 > 0 \\ 2-q^2 > 0 \end{cases} \quad \Rightarrow \quad \frac{2q+1}{2-q^2} > 0$$

Dalla Proprietà Archimedea (si veda l'Esercizio 6.9) esiste $n \in \mathbb{N}$ tale che

$$n > \frac{2q+1}{2-q^2} \quad \Rightarrow \quad 2-q^2 > \frac{2}{n}q + \frac{1}{n} \quad \Rightarrow \quad q^2 + \frac{2}{n}q + \frac{1}{n} < 2.$$

Segue che

$$\left(q + \frac{1}{n}\right)^2 = q^2 + \frac{2}{n}q + \frac{1}{n^2} \leq q^2 + \frac{2}{n}q + \frac{1}{n} < 2.$$

Quindi $p = q + 1/n \in B$ ed è strettamente maggiore di q.

Ci chiediamo se esiste un insieme X tale che:

(i) sia possibile definire due operazioni binarie $+$ e $\cdot$ tali che $(X, +, \cdot)$ sia un campo;
(ii) sia possibile definire un ordine totale $\leq$;
(iii) sia possibile definire un'applicazione iniettiva $J : (\mathbb{Q}, \leq) \to (X, \leq)$ tale che le operazioni e l'ordine ristrette a $J(\mathbb{Q})$ coincidano con le operazioni è l'ordine definiti su $\mathbb{Q}$ tramite J;
(iv) $(X, \leq)$ sia completo e $\mathbb{Q}$ sia denso in X.

Tale insieme esiste e sarà argomento della prossima sezione.

[1] Supponiamo esista $q = m/n$ con $q^2 = 2$ e m, n privi di fattori comuni. Allora $m^2 = 2n^2$ da cui si deduce che m^2 è pari e quindi m è pari. Segue che $m = 2k$ e, sostituendo in $m^2 = 2n^2$, si ottiene $4k^2 = 2n^2$ la quale implica che n^2 è pari e quindi anche n è pari. Si perviene alla contraddizione che m e n sono entrambi divisibili per 2 contro l'ipotesi che m e n non hanno fattori in comune.

10.2 Costruzione del campo ordinato dei numeri reali

Definizione 10.1 Una *sezione di Dedekind* è un sottoinsieme non vuoto $x \subseteq \mathbb{Q}$ tale che
(a) $x \neq \mathbb{Q}$, cioè x è un sottoinsieme proprio di $\mathbb{Q}$;
(b) x non ammette un massimo;
(c) se $p \in x$ e $q < p$ allora $q \in x$.

■ **Esempio 10.1** L'insieme

$$B = \{q \in \mathbb{Q} \colon q < 0\} \cup \{q \in \mathbb{Q} \colon q \geq 0 \quad \wedge \quad q^2 < 2\}$$

è una sezione di Dedekind. Infatti, non coincide con $\mathbb{Q}$ poiché non contiene alcun numero razionale maggiore di 2. Non ha massimo come dimostrato all'inizio del capitolo e chiaramente gode della proprietà (c) (il lettore deve però fare tutti i passaggi per convincersi). ■

Definizione 10.2 L'insieme dei *numeri reali*, denotato con il simbolo $\mathbb{R}$, è l'insieme di tutte le sezioni di Dedekind.

Adesso che abbiamo definito l'insieme dei numeri reali possiamo procedere con la definizione di somma e prodotto.

Definizione 10.3 Siano $x, y \in \mathbb{R}$ due numeri reali, definiamo la loro somma come

$$x +_{\mathbb{R}} y = \{p + q \colon p \in x \quad \wedge \quad q \in y\}.$$

Affinché la definizione sopra abbia senso è necessario verificare che $x +_{\mathbb{R}} y$ sia un numero reale. Verifichiamo quindi le tre proprietà che definiscono una sezione di Dedekind.

(a) Essendo x reale esite $a \in \mathbb{Q}$ con $a \notin x$. Allo stesso modo esiste $b \in \mathbb{Q}$ con $b \notin y$. Segue che $a > p$ per ogni $p \in x$ e $b > q$ per ogni $q \in y$. Concludiamo che $a + b > p + q$ per ogni $p \in x \quad \wedge \quad q \in y$ da cui $a + b \notin x +_{\mathbb{R}} y$.
(b) Sia $r = p + q \in x +_{\mathbb{R}} y$. Siccome $p \in x$ e $q \in y$ esistono $p' \in x$ con $p < p'$ e $q' \in y$ con $q < q'$. Segue che $r = p + q < p' + q' \in x +_{\mathbb{R}} y$. Quindi $x +_{\mathbb{R}} y$ non ha massimo.
(c) Sia $p + q \in x +_{\mathbb{R}} y$ e sia $r < p + q$. Allora $r - p < q \in y$ da cui $r - p \in y$. Segue che $r = p + (r - p) \in x +_{\mathbb{R}} y$.

Valgono le seguenti proprietà per ogni $x, y, z \in \mathbb{R}$ (verifica lasciata per esercizio):

$$x +_{\mathbb{R}} y = y +_{\mathbb{R}} x \qquad (x +_{\mathbb{R}} y) +_{\mathbb{R}} z = x +_{\mathbb{R}} (y +_{\mathbb{R}} z)$$

Definiamo adesso la funzione

$$\begin{array}{rccl} J \colon & \mathbb{Q} & \to & \mathbb{R} \\ & q & \mapsto & J(q) = \{p \in \mathbb{Q} \colon p < q\} \end{array}$$

Si verifica immediatamente (farlo per esercizio) che $J(q)$ è un numero reale e che J è iniettiva. Possiamo quindi identificare $\mathbb{Q}$ con $J(\mathbb{Q}) \subseteq \mathbb{R}$. Verifichiamo adesso che J conserva l'operazione di somma, cioè che

$$J(p) +_{\mathbb{R}} J(q) = J(p + q) \qquad \forall p, q \in \mathbb{Q}.$$

Procediamo mostrando la doppia inclusione.

$\boxed{J(p) +_{\mathbb{R}} J(q) \subseteq J(p + q)}$ Sia $r \in J(p) +_{\mathbb{R}} J(q)$, allora $r = p' + q'$ con $p' < p$ e $q' < q$. Segue che $r = p' + q' < p + q$ e quindi $r \in J(p + q)$.

$\boxed{J(p + q) \subseteq J(p) +_{\mathbb{R}} J(q)}$ Sia $r \in J(p + q)$, quindi $r < p + q$. Poiché $\mathbb{Q}$ è denso (si veda il Problema 8.9) esiste $r' \in \mathbb{Q}$ con $r < r' < p + q$. Allora $r' - p < q$ da cui $r' - p \in J(q)$, cioè

$r' - p = q' < q$. Quindi $r < r' = p + q'$. Ripetendo il ragionamento, da $r < p + q'$ si trova $r - q' < p$ e quindi $r - q' \in J(p)$, cioè $r - q' = p' < p$. Si conclude che $r = p' + q'$ con $p' < p$ e $q' < q$.

Utilizzando J possiamo definire

$$0_{\mathbb{R}} = J(0) = \{p \in \mathbb{Q} \colon p < 0\}.$$

Al fine di attribuire a $0_{\mathbb{R}}$ il ruolo di elemento neutro rispetto alla somma $+_{\mathbb{R}}$ bisogna verificare che

$$x +_{\mathbb{R}} 0_{\mathbb{R}} = x \qquad \forall x \in \mathbb{R}$$

Procediamo anche in questo caso mostrando la doppia inclusione.

$\boxed{x +_{\mathbb{R}} 0_{\mathbb{R}} \subseteq x}$ Sia $r \in x +_{\mathbb{R}} 0_{\mathbb{R}}$. Allora $r = p + q$ con $p \in x \quad \wedge \quad q \in 0_{\mathbb{R}}$. Poiché $q < 0$ segue che $p + q < p \in x$, da cui $r = p + q \in x$.

$\boxed{x \subseteq x +_{\mathbb{R}} 0_{\mathbb{R}}}$ Sia $p \in x$. Allora esiste $q \in x$ con $p < q$. Segue che $p - q < 0$ e quindi $p = q + (p - q) \in x +_{\mathbb{R}} 0_{\mathbb{R}}$.

Per concludere che $(\mathbb{R}, +_{\mathbb{R}})$ è un gruppo bisogna dimostrare l'esistenza dell'opposto. Definiamo

$$-x = \{p \in \mathbb{Q} \colon \exists s > p \text{ con } -s \notin x\}$$

La definizione appare piuttosto artificiosa ma è necessaria affinché $-x$ sia realmente un numero reale (provare per esercizio). Per dimostrare che $-x$ definisce l'opposto di x bisogna verificare che $x +_{\mathbb{R}} (-x) = 0_{\mathbb{R}}$ per ogni $x \in \mathbb{R}$. L'ultima uguaglianza deve essere dimostrata mostrando la doppia inclusione. Iniziamo

$\boxed{x +_{\mathbb{R}} (-x) \subseteq 0_{\mathbb{R}}}$ Sia $q + q' \in x +_{\mathbb{R}} (-x)$. Allora esiste $s \in \mathbb{Q}$ con $q' < s$ e $-s \notin x$, cioè $-s > p$ per ogni $p \in x$. In particolare $-s > q$. Adesso $q' < s$ e $-s > q$ (ovvero $s < -q$) implicano che $q' < s < -q$ da cui $q + q' < 0$, cioè $q + q' \in 0_{\mathbb{R}}$.

$\boxed{0_{\mathbb{R}} \subseteq x +_{\mathbb{R}} (-x)}$ Questa inclusione è più delicata. Utilizziamo, senza dimostrazione, il seguente

Lemma 10.1 Sia $0 < p \in \mathbb{Q}$ e sia $x \in \mathbb{R}$. Allora esiste $q \in x$ con $p + q \notin x$.

Sia $r \in 0_{\mathbb{R}}$, allora $r < 0$ e $-r/2 > 0$. Dal Lemma (con $p = -r/2$), per ogni $x \in \mathbb{R}$ esiste $q \in x$ con $(-r/2) + q \notin x$. Adesso $r = q + (r - q)$ con $q \in x$. Per concludere mostriamo che $r - q \in -x$. Poiché $r - q < r/2 - q$ se poniamo $s = r/2 - q$ si ha $-s = -r/2 + q \notin x$, da cui $r - q \in -x$.

Possiamo quindi concludere che $(\mathbb{R}, +_{\mathbb{R}})$ è un gruppo abeliano.
Prima di procedere con la definizione di prodotto di numeri reali introduciamo la relazione d'ordine su $\mathbb{R}$.

Definizione 10.4 Dati due numeri reali $x, y \in \mathbb{R}$ definiamo la seguente relazione

$$x \leq_{\mathbb{R}} y \quad \Leftrightarrow \quad x \subseteq y \quad \text{come sottoinsiemi di } \mathbb{Q}.$$

La relazione $\leq_{\mathbb{R}}$ definisce un ordine parziale su $\mathbb{R}$ come illustrato nell'Esempio 8.2.
Vale inoltre il seguente fatto.

Proposizione 10.1 La relazione d'ordine $\leq_{\mathbb{R}}$ definisce un ordine totale su $\mathbb{R}$.

Dimostrazione. Siano $x, y \in \mathbb{R}$ e supponiamo che $x \not\leq_{\mathbb{R}} y$, cioè $x \not\subseteq y$. Mostriamo che $y \subseteq x$. Siccome $x \not\subseteq y$ esiste $p \in x \setminus y$. Sia $q \in y$. Se $p < q$ allora (poiché y è un numero reale) $p \in y$ il ché è assurdo ($p \in x \setminus y$). Quindi $q < p \in x$ da cui (poiché x è un numero reale) $q \in x$. ■

Esercizio 10.1 Siano $p, q \in \mathbb{Q}$. Dimostrare che

$$J(p) \leq_{\mathbb{R}} J(q) \quad \Leftrightarrow \quad p \leq_{\mathbb{Q}} q\,.$$

L'esercizio precedente mostra che l'ordine definito sui numeri reali quando ristretto ai razionali coincide con l'ordine dei numeri razionali.

Siamo nella giusta posizione per mostrare che l'insieme dei numeri reali con l'odine sopra definito è completo.

Teorema 10.1 L'insieme ordinato $(\mathbb{R}, \leq_{\mathbb{R}})$ è completo.

Dimostrazione. Mostriamo che ogni sottoinsieme non vuoto limitato superiormente ammette estremo superiore. Sia $X \subseteq \mathbb{R}$ un sottoinsieme non vuoto limitato superiormente e sia $b \in \mathbb{R}$ un maggiorante di X, cioè per ogni $x \in X$, $x \leq_{\mathbb{R}} b$, ovvero, $x \subseteq b$. Sia

$$U = \bigcup_{x \in X} x \subseteq \mathbb{Q}\,.$$

Se mostriamo che U è un numero reale allora U è per costruzione il minimo dei maggioranti. Infatti ogni maggiorante contiene tutti gli elementi di X e quindi anche la loro unione. Procediamo

(a) $U \neq \varnothing$ poiché $X \neq \varnothing$. Inoltre $\bigcup_{x \in X} x \subseteq b \subsetneq \mathbb{Q}$. Quindi U è un sottoinsieme proprio di $\mathbb{Q}$.

(b) Se $p \in U$, allora esiste $x \in X$ con $p \in x$. Essendo x un numero reale segue che esiste $q \in x \subseteq U$ con $p < q$. Quindi U non ha massimo.

(c) Se $p \in U$ e $q < p$, allora $p \in x$ per qualche $x \in X$ e, essendo x reale, segue che $q \in x \subseteq U$.

Il lettore dovrebbe adesso mostrare per esercizio che ogni sottoinsieme non vuoto limitato inferiormente ammette estremo inferiore. ■

Esercizio 10.2 Dati $x, y, z \in \mathbb{R}$ dimostrare che

1. $x = y \quad \Leftrightarrow \quad x + z = y + z$
2. $x \leq_{\mathbb{R}} y \quad \Leftrightarrow \quad x +_{\mathbb{R}} z \leq_{\mathbb{R}} y +_{\mathbb{R}} z$

Definizione 10.5 Sia $x \in \mathbb{R}$ definiamo il *valore assoluto* di x come

$$|x| = x \cup (-x)$$

Esercizio 10.3 Verificare che per un dato $x \in \mathbb{R}$ il valore assoluto $|x|$ è un numero reale.

Osservazione 10.1 Il valore assoluto di un numero reale è sempre non negativo, nel senso che $0_{\mathbb{R}} \leq_{\mathbb{R}} |x|$ per ogni $x \in \mathbb{R}$. Per verificarlo, sia $q \in 0_{\mathbb{R}}$. Allora $q < 0$. Se $q \in x$ allora $q \in x \cup (-x) = |x|$ ed abbiamo finito. Se $q \notin x$, allora $p < q$ per ogni $p \in x$, quindi tutti i razionali di x sono negativi. Adesso, essendo $q \in 0_{\mathbb{R}}$ ed essendo $0_{\mathbb{R}}$ un numero reale esiste $q' \in 0_{\mathbb{R}}$ con $q < q' < 0$. Inoltre $-q' > 0$ quindi $-q' \notin x$. Segue che, ponendo $s = q'$, $q < s$ con $-s \notin x$, cioè $q \in -x$.

Definizione 10.6 — Prodotto di numeri reali. Siano $x, y \in \mathbb{R}$

1. Se $x, y > 0$ allora definiamo

$$x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}} \cup \{p\,q \colon 0 \leq p \in x \quad \wedge \quad 0 \leq q \in y\}$$

2. Se $x, y < 0$ allora definiamo
$$x \cdot_{\mathbb{R}} y = |x| \cdot_{\mathbb{R}} |y|$$
3. Se $x > 0$ e $y < 0$ allora definiamo
$$x \cdot_{\mathbb{R}} y = -(|x| \cdot_{\mathbb{R}} |y|)$$
4. Se $x = 0 \quad \vee \quad y = 0$ allora definiamo
$$x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}}$$

Proposizione 10.2 — Senza dimostrazione.

1. Per ogni $x, y \in \mathbb{R}$, $x \cdot_{\mathbb{R}} y$ è un numero reale;
2. Per ogni $x, y \in \mathbb{R}$
$$x \cdot_{\mathbb{R}} y = y \cdot_{\mathbb{R}} x$$
3. Per ogni $x, y, z \in \mathbb{R}$
$$x \cdot_{\mathbb{R}} (y \cdot_{\mathbb{R}} z) = (x \cdot_{\mathbb{R}} y) \cdot_{\mathbb{R}} z$$
4. Per ogni $x, y, z \in \mathbb{R}$
$$x \cdot_{\mathbb{R}} (y +_{\mathbb{R}} z) = x \cdot_{\mathbb{R}} y +_{\mathbb{R}} x \cdot_{\mathbb{R}} z$$
5. Se $1 = \{q \in \mathbb{Q} \colon q < 1\}$ allora per ogni $x \in \mathbb{R}$
$$x \cdot_{\mathbb{R}} 1 = 1 \cdot_{\mathbb{R}} x = x$$
6. Per ogni $x \in \mathbb{R}, x \neq 0$, denotato con
$$x^{-1} = \begin{cases} \{q \in \mathbb{Q} \colon \exists s \notin x \text{ con } q < 1/s\} & \text{se } x > 0 \\ -(|x|)^{-1} & \text{se } x < 0 \end{cases}$$
si ha
$$x \cdot_{\mathbb{R}} x^{-1} = x^{-1} \cdot_{\mathbb{R}} x = 1$$

In conclusione $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ è un campo. Da ora in poi tralasceremo l'utilizzo del pedice per indicare quali operazioni sono definite sui numeri reali confidando sul fatto che il contesto permetterà al lettore di individuare qual'è la giusta operazione da eseguire.

Osservazione 10.2 La dimostrazione della Proposizione 10.2, anche se concettualmente non difficile, prevede un utilizzo di certe disuguaglianza tra i numeri razionali che non sempre risultano immediate. Per tale motivo si è deciso di omettere la prova. È utile però osservare come mai non è possibile definire l'inverso x^{-1} del numero reale $0 \in \mathbb{R}$. Infatti, dalla definizione si avrebbe

$$0^{-1} = \{q \in \mathbb{Q} \colon \exists s \notin 0 \text{ con } q < 1/s\} = \{q \in \mathbb{Q} \colon \exists s > 0 \text{ con } q < 1/s\}.$$

Mostriamo che $0^{-1} = \mathbb{Q}$. Per definizione $0^{-1} \subseteq \mathbb{Q}$. Sia invece $q \in \mathbb{Q}$. Se $q \leq 0$ allora $q < 2 = 1/(1/2)$ quindi appartiene a 0^{-1} scegliendo $s = 1/2$. Se $q > 0$, per la proprietà Archimedea, esiste un $n \in \mathbb{N}$ con $n > q$. Ponendo $s = 1/n$ si trova $q < 1/s$ con $s > 0$, da cui $q \in 0^{-1}$. In conclusione, essendo $0^{-1} = \mathbb{Q}$ per la Definizione 10.1 l'insieme 0^{-1} non definisce un numero reale.

Esercizio 10.4 Dati $x, y, z \in \mathbb{R}$ dimostrare che

1. Se $z > 0$
$$x \leq y \quad \Leftrightarrow \quad xz \leq yz$$
2. Se $z < 0$
$$x \leq y \quad \Leftrightarrow \quad xz \geq yz$$

Proposizione 10.3 Le tre proprietà seguenti sono equivalenti.
(a) Per ogni $x \in \mathbb{R}$, esiste $N \in \mathbb{N}$ con $N > x$.
(b) Per ogni $x \in \mathbb{R}$, $x > 0$, esiste $N \in \mathbb{N}$ con $0 < 1/N < x$.
(c) Per ogni $x, y \in \mathbb{R}$, $0 < x < y$, esiste $N \in \mathbb{N}$ con $Nx > y$.

Dimostrazione.
(a) $\Rightarrow$ (b) Sia $x > 0$, allora, per la (a), esiste $N > x^{-1}$. Segue che $Nx > x^{-1}x = 1$ da cui $x > 1/N$.

(b) $\Rightarrow$ (c) Siano $0 < x < y$. Consideriamo $xy^{-1} > 0$. Allora, per la (b), esiste N con $1/N < xy^{-1}$ da cui $1 < Nxy^{-1}$, cioè $y < Nxy^{-1}y = Nx$.

(c) $\Rightarrow$ (a) Sia $x \in \mathbb{R}$. Se $x \leq 1$ allora $2 > x$. Se $x > 1$, allora $0 < 1 < x$ e, applicando la (c), esiste $N \in \mathbb{N}$ con $N \cdot 1 > x$. ■

Verifichiamo nella prossima proposizione che la (a), e quindi tutte e tre, sono vere in $\mathbb{R}$.

Proposizione 10.4 — Proprietà Archimedea dei numeri reali. Per ogni $x \in \mathbb{R}$, esiste $N \in \mathbb{N}$ con $N > x$.

Dimostrazione. Se per assurdo esistesse un $x \in \mathbb{R}$ con $n \leq x$ per ogni $n \in \mathbb{N}$ allora $\mathbb{N}$, come sottoinsieme dei numeri reali, sarebbe limitato in $\mathbb{R}$ da x. Usando la completezza di $\mathbb{R}$ esisterebbe il sup di $\mathbb{N}$ in $\mathbb{R}$, cioè esisterebbe $\bar{x} \in \mathbb{R}$ con $\bar{x} =$ min dei maggioranti. Quindi $\bar{x} - 1$ non sarebbe un maggiorante, implicando che esisterebbe $n \in \mathbb{N}$ con $n > \bar{x} - 1$. In conclusione si perviene all'assurdo che $n + 1 > \bar{x}$ mentre $\bar{x}$ è un maggiorante di $\mathbb{N}$. ■

Proposizione 10.5 L'insieme dei numeri razionali è denso nell'insieme dei numeri reali. Cioè per ogni $x, y \in \mathbb{R}$, $x < y$, esiste $q \in \mathbb{Q}$ con $x < q < y$.

Dimostrazione. Supponiamo inizialmente che $x > 0$ e sia $y \in \mathbb{R}$ tale che $0 < x < y$. Poiché $x < y$ si ha che $(y-x)^{-1} > 0$ e, per la proprietà Archimedea, esiste $n_o \in \mathbb{N}$ con $n_o > (y-x)^{-1}$. Segue che $n_o(y-x) > 1$ da cui $n_o y > n_o x + 1$. Consideriamo adesso l'insieme

$$A = \{m \in \mathbb{N} \colon n_o x < m\} \subseteq \mathbb{N}\,.$$

L'insieme A non è vuoto (per la proprietà Archimedea). Segue, dal Principio del Buon Ordinamento (Teorema 8.1), che esiste $\bar{m} = \min A > 0$ (poiché $n_o x > 0$). Quindi $\bar{m} - 1 \leq n_o x < \bar{m}$. Inoltre, $n_o y > n_o x + 1 \geq (\bar{m} - 1) + 1 = \bar{m}$. Otteniamo quindi che $n_o x < \bar{m} < n_o y$ la quale, essendo $n_o > 0$, si può riscrivere come

$$x < \frac{\bar{m}}{n_o} < y$$

L'ultima serie di disuguaglianze mostra che $\bar{m}/n_o$ è il numero razionale cercato.

Se $x \leq 0$, allora esiste $k \in \mathbb{N}$ con $k > -x$, cioè $0 < k+x$. Sia adesso $y \in \mathbb{R}$ con $x < y$. Allora $0 < x+k < y+k$ e, dal caso precedente, esiste $q \in \mathbb{Q}$ con $x+k < q < y+k$. Si ottiene infine $x < q-k < y$ da cui la tesi. ■

10.3 Cardinalità di $\mathbb{R}$

In questo paragrafo dimostriamo che l'insieme dei numeri reali non è numerabile. Per arrivare a tale risultato abbiamo bisogno di ricordare alcune formule notevoli sulla serie geometrica.

Sia $q \in \mathbb{Q}$ e sia $m \in \mathbb{N}$. Allora si dimostra per induzione su m che

$$\sum_{k=0}^{m} q^k = \frac{1-q^{m+1}}{1-q} \tag{10.1}$$

In particolare, se $q = 1/2$ si ottiene

$$\sum_{k=0}^{m} \left(\frac{1}{2}\right)^k = 2 - \left(\frac{1}{2}\right)^m \tag{10.2}$$

che, partendo da $k = 1$, diventa

$$\sum_{k=1}^{m} \left(\frac{1}{2}\right)^k = 1 - \left(\frac{1}{2}\right)^m < 1\,. \tag{10.3}$$

Adesso, per $n > m$, si trova

$$\sum_{k=m+1}^{n} \left(\frac{1}{2}\right)^k = \sum_{k=1}^{n} \left(\frac{1}{2}\right)^k - \sum_{k=1}^{m} \left(\frac{1}{2}\right)^k = 1 - \left(\frac{1}{2}\right)^n - 1 + \left(\frac{1}{2}\right)^m < \left(\frac{1}{2}\right)^m. \tag{10.4}$$

Siamo pronti per enunciare e dimostrare il seguente importante risultato

Teorema 10.2 La cardinalità dei numeri reali è pari alla cardinalità dell'insieme delle parti dei numeri naturali. Ovvero:

$$|\mathbb{R}| = |\mathscr{P}(\mathbb{N})| = 2^{\aleph_o}\,.$$

Dimostrazione. Premettiamo che $|\mathbb{N}| = |\mathbb{N}^*|$ dove $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Possiamo quindi dimostrare che $|\mathbb{R}| = |\mathscr{P}(\mathbb{N}^*)|$. Procediamo dimostrando che $|\mathbb{R}| \leq |\mathscr{P}(\mathbb{N}^*)|$ e $|\mathscr{P}(\mathbb{N}^*)| \leq |\mathbb{R}|$. La prima è ovvia poiché $\mathbb{R} \subseteq \mathscr{P}(\mathbb{Q})$ da cui $|\mathbb{R}| \leq |\mathscr{P}(\mathbb{Q})| = |\mathscr{P}(\mathbb{N}^*)|$ (per l'ultima uguaglianza il lettore è invitato a pensare alla costruzione di una biezione tra $\mathscr{P}(\mathbb{N}^*)$ e $\mathscr{P}(\mathbb{Q})$). Mostriamo che $|\mathscr{P}(\mathbb{N}^*)| \leq |\mathbb{R}|$. A tal scopo è sufficiente esibire una funzione iniettiva $\varphi : \mathscr{P}(\mathbb{N}^*) \setminus A \to \mathbb{R}$ dove $A \subseteq \mathscr{P}(\mathbb{N}^*)$ è un sottoinsieme numerabile. Infatti se esistesse tale φ si avrebbe $|\mathscr{P}(\mathbb{N}^*)| = |\mathscr{P}(\mathbb{N}^*) \setminus A| \leq |\mathbb{R}|$, dove nella prima uguaglianza abbiamo utilizzato l'Osservazione 9.3–(c). Sappiamo che

$$\mathscr{P}(\mathbb{N}^*) = 2^{\mathbb{N}^*} = \{f : \mathbb{N}^* \to \{0,1\}\}\,,$$

cioè $\mathscr{P}(\mathbb{N}^*)$ è l'insieme di tutte le funzioni a valori in $\{0,1\}$. Un elemento di $\mathscr{P}(\mathbb{N}^*)$ si può quindi pensare come una sequenza (successione) infinita formata da 0 e 1. Definiamo

$$F_0 = \{f : \mathbb{N}^* \to \{0,1\} \colon \exists k \in \mathbb{N}^* \text{ con } f(n) = 0\ \forall n > k\}$$

e

$$F_1 = \{f : \mathbb{N}^* \to \{0,1\} \colon \exists k \in \mathbb{N}^* \text{ con } f(n) = 1\ \forall n > k\}\,.$$

Intuitivamente F_0 è l'insieme di tutte le successioni che da un certo punto in poi sono sempre uguali a 0, mentre F_1 è l'insieme di tutte le successioni che da un certo punto in poi sono sempre uguali a

1. Gli insiemi F_0 e F_1 si possono vedere come unione numerabile di insiemi finiti risultando quindi numerabili. Segue che $A = F_0 \cup F_1$ è numerabile. Sia $X = 2^{\mathbb{N}^*} \setminus A$, per concludere la dimostrazione costruiamo una funzione iniettiva $\varphi : X \to \mathbb{R}$. Definiamo φ nel modo seguente:

$$\begin{array}{rccl} \varphi: & X & \to & \mathbb{R} \\ & f & \mapsto & \varphi(f) = \left\{ q \in \mathbb{Q} \colon \exists m \in \mathbb{N}^* \text{ con } q < \sum_{k=1}^{m} \frac{f(k)}{2^k} \right\} \end{array}$$

Prima di procedere nella dimostrazione dell'iniettività di φ bisogna assicurarsi che φ sia ben definita, cioè che $\varphi(f)$ sia un numero reale. Procediamo alla verifica delle condizioni della Definizione 10.1.

1. Tenendo in considerazione la (10.3), si ha, per ogni $m \in \mathbb{N}$,

$$0 < \sum_{k=1}^{m} \frac{f(k)}{2^k} < 1$$

   da cui $\varphi(f) \neq \varnothing$ e $\varphi(f) \neq \mathbb{Q}$.
2. Sia $q \in \varphi(f)$, allora esiste $m \in \mathbb{N}^*$ tale che $q < \sum_{k=1}^{m} \frac{f(k)}{2^k}$. Poiché $f \notin F_0$ esiste $m' > m$ con $f(m') = 1$. Si trova quindi

$$q < \sum_{k=1}^{m} \frac{f(k)}{2^k} < \sum_{k=1}^{m'} \frac{f(k)}{2^k}.$$

   Ponendo $q' = \sum_{k=1}^{m} \frac{f(k)}{2^k}$ per la relazione sopra si ha $q' \in \varphi(f)$ e $q < q'$. Così che $\varphi(f)$ non ha massimo.
3. Se $q \in \varphi(f)$ allora esiste $m \in \mathbb{N}^*$ tale che $q < \sum_{k=1}^{m} \frac{f(k)}{2^k}$. Se $p < q$ si ha che $p < \sum_{k=1}^{m} \frac{f(k)}{2^k}$ per lo stesso m e quindi $p \in \varphi(f)$.

Dimostriamo adesso che φ è iniettiva, cioè che per $f, g \in X$, $f \neq g$, si ha $\varphi(f) \neq \varphi(g)$. Sia $L = \{s \in \mathbb{N}^* \colon f(s) \neq g(s)\}$. Poiché $f \neq g$ l'insieme L è diverso dal vuoto da cui, per il Principio del Buon Ordinamento, esiste $m = \min(L)$. Supponiamo, senza ledere la generalità, che $f(m) = 0$ e $g(m) = 1$. Allora, per ogni $n < m$, si ha (poiché $g(m) = 1$)

$$\sum_{k=1}^{n} \frac{f(k)}{2^k} = \sum_{k=1}^{n} \frac{g(k)}{2^k} < \sum_{k=1}^{m} \frac{g(k)}{2^k}.$$

Se $n = m$ ugualmente

$$\begin{aligned} \sum_{k=1}^{m} \frac{f(k)}{2^k} &= \sum_{k=1}^{m-1} \frac{f(k)}{2^k} + \frac{f(m)}{2^k} = \sum_{k=1}^{m-1} \frac{f(k)}{2^k} + \frac{0}{2^k} \\ &< \sum_{k=1}^{m-1} \frac{g(k)}{2^k} + \frac{1}{2^k} = \sum_{k=1}^{m-1} \frac{g(k)}{2^k} + \frac{g(m)}{2^k} \\ &= \sum_{k=1}^{m} \frac{g(k)}{2^k}. \end{aligned}$$

Infine, per ogni $n > m$, si trova

$$\begin{aligned}
\sum_{k=1}^{n} \frac{f(k)}{2^k} &= \sum_{k=1}^{m-1} \frac{f(k)}{2^k} + \frac{f(m)}{2^m} + \sum_{k=m+1}^{n} \frac{f(k)}{2^k} \\
&= \sum_{k=1}^{m-1} \frac{g(k)}{2^k} + \frac{0}{2^m} + \sum_{k=m+1}^{n} \frac{f(k)}{2^k} \\
&\leq \sum_{k=1}^{m-1} \frac{g(k)}{2^k} + \sum_{k=m+1}^{n} \frac{1}{2^k} \\
\text{(per la (10.4))} \quad &< \sum_{k=1}^{m-1} \frac{g(k)}{2^k} + \frac{1}{2^m} \\
&= \sum_{k=1}^{m-1} \frac{g(k)}{2^k} + \frac{g(m)}{2^m} \\
&= \sum_{k=1}^{m} \frac{g(k)}{2^k}.
\end{aligned}$$

In conclusione, per ogni $n \in \mathbb{N}^*$,

$$\sum_{k=1}^{n} \frac{f(k)}{2^k} < \sum_{k=1}^{m} \frac{g(k)}{2^k}.$$

Segue che $q = \sum_{k=1}^{m} \frac{g(k)}{2^k} \notin \varphi(f)$ mentre, poiché $g \notin F_0$, esiste $m' > m$ tale che

$$q = \sum_{k=1}^{m} \frac{g(k)}{2^k} < \sum_{k=1}^{m'} \frac{g(k)}{2^k}$$

da cui

$$q = \sum_{k=1}^{m} \frac{g(k)}{2^k} \in \varphi(g).$$

In conclusione $\varphi(f) \neq \varphi(g)$ poiché esiste un elemento $q \in \varphi(g) \setminus \varphi(f)$. ■

La cardinalità dei numeri reali coincide quindi con la cardinalità del continuo, cioè la cardinalità dell'insieme delle parti dei numeri naturali.
I numeri reali che non sono razionali sono detti *irrazionali*. Ad esempio l'insieme

$$\alpha = 0_{\mathbb{R}} \cup \{q \in \mathbb{Q} \colon q \geq 0 \text{ e } q^2 < 2\}$$

definisce un numero reale che non si può identificare con alcun numero razionale della forma $J(p), p \in \mathbb{Q}$. Infatti, come dimostreremo subito dopo, $\alpha \cdot_{\mathbb{R}} \alpha = 2$ la quale implica, per le argomentazioni riportare all'inizio del capitolo, che α non è razionale. Comunemente un numero reale con la proprietà che il suo quadrato sia pari a 2 si denota con $\sqrt{2}$. Quindi $\sqrt{2}$ è un numero irrazionale.

Proposizione 10.6 Sia

$$\alpha = 0_{\mathbb{R}} \cup \{q \in \mathbb{Q} \colon q \geq 0 \text{ e } q^2 < 2\} \in \mathbb{R}$$

Allora $\alpha^2 = \alpha\,\alpha = 2$.

Dimostrazione. Mostriamo la doppia inclusione.
$\boxed{\alpha\,\alpha \subseteq 2}$ Se $r \in \alpha\,\alpha$ allora

$$r \in 0_{\mathbb{R}} \quad \vee \quad r = pq \text{ con } p, q \geq 0,\ p^2 < 2,\ q^2 < 2$$

Se $r \in 0_{\mathbb{R}}$ allora $r < 0 < 2$. Se $r = pq$ allora $r^2 = p^2q^2 < 4$ da cui $r < 2$ poiché se $r \geq 2$ allora $r^2 \geq 4$.

$\boxed{2 \subseteq \alpha\,\alpha}$ Sia $r \in 2 = \{q \in \mathbb{Q}\colon q < 2\}$. Se $r \leq 0$ allora $r < 1 \in \alpha\,\alpha$, possiamo quindi supporre che $r > 0$. È sufficiente dimostrare che esiste $q \in \mathbb{Q}$ con $r < q^2 < 2$. Infatti, se esistesse tale q, allora $q \in \alpha$ e $q\,q \in \alpha\,\alpha$ da cui, essendo $\alpha\,\alpha \in \mathbb{R}$, $r < q\,q \in \alpha\,\alpha$ implicherebbe che $r \in \alpha\,\alpha$. Dimostriamo che esiste $q \in \mathbb{Q}$ con $r < q^2 < 2$. Sia n_o un numero naturale fissato e si consideri l'insieme

$$S = \left\{ m \in \mathbb{N}\colon r < \frac{m^2}{n_o^2} \right\}$$

Poiché $S \neq \varnothing$, dal Principio del Buon Ordinamento esiste $m_o = \min(S) \geq 2$. Si trova quindi

$$\frac{(m_o-1)^2}{n_o^2} \leq r < \frac{m_o^2}{n_o^2}$$

Se esistesse un n_o tale che $m_o^2/n_o^2 < 2$ avremmo finito. Cerchiamo quindi per quale valore di n_o si ha $m_o^2/n_o^2 \geq 2$. Se $m_o^2/n_o^2 \geq 2$ si avrebbe

$$\frac{m_o^2}{n_o^2} \geq 2 > r \geq \frac{(m_o-1)^2}{n_o^2}$$

da cui

$$\frac{m_o^2}{n_o^2} - \frac{(m_o-1)^2}{n_o^2} \geq 2 - r$$

cioè

$$\frac{2m_o-1}{n_o^2} \geq 2 - r \tag{10.5}$$

Inoltre

$$(m_o-1)^2 \leq n_o^2 r \quad \wedge \quad \forall m_o \geq 2 \quad (2m_o-1)^2 \leq (3m_0-3)^2$$

da cui

$$(2m_o-1)^2 \leq (3m_0-3)^2 = 9(m_o-1)^2 \leq 9n_o^2 r$$

Combinando l'ultima diseguaglianza con la (10.5) si trova

$$(2-r)^2 \leq \frac{(2m_o-1)^2}{n_o^4} \leq \frac{9n_o^2 r}{n_o^4} = \frac{9r}{n_o^2} \quad \Rightarrow \quad n_o^2 \leq \frac{9r}{(2-r)^2}$$

Quindi se $n_o^2 > 9r/(2-r)^2$ si ha che $m_o^2/n_o^2 < 2$. ■

10.4 Problemi proposti

Problema 10.1 Sia

$$J : \mathbb{Q} \to \mathbb{R}$$

definita da $J(q) = \{p \in \mathbb{Q}\colon p < q\}$. Dimostrare che

1. Per ogni $q \in \mathbb{Q}$, $J(q)$ definisce un numero reale
2. Per ogni $p, q \in \mathbb{Q}$, $\quad p \leq_{\mathbb{Q}} q \quad \Leftrightarrow \quad J(p) \leq_{\mathbb{R}} J(q)$
3. Per ogni numero reale $x \in \mathbb{R}$ si ha che $J(1) \cdot_{\mathbb{R}} x = x$.

Problema 10.2 Dimostrare che per ogni $q, q' \in \mathbb{Q}$ con $q < q'$ esiste un $x \in \mathbb{R} \setminus \mathbb{Q}$ tale che $q < x < q'$.

Problema 10.3 Adatare la dimostrazione della Proposizione 10.6 per dimostrare che dato

$$\beta = 0_{\mathbb{R}} \cup \{q \in \mathbb{Q}\colon q \geq 0 \text{ e } q^2 < 3\}$$

allora $\beta^2 = \beta\,\beta = 3$, cioè $\beta = \sqrt{3}$.

11. I numeri complessi

11.1 Costruzione dei numeri complessi

Si consideri l'insieme $\mathbb{R}\times\mathbb{R}$ nel quale siano definite le seguenti operazioni

$$\begin{array}{rccc} +_{\mathbb{C}}: & (\mathbb{R}\times\mathbb{R})\times(\mathbb{R}\times\mathbb{R}) & \to & \mathbb{R}\times\mathbb{R} \\ & ((a,b),(c,d)) & \mapsto & (a+c,b+d) \end{array} \tag{11.1}$$

$$\begin{array}{rccc} \cdot_{\mathbb{C}}: & (\mathbb{R}\times\mathbb{R})\times(\mathbb{R}\times\mathbb{R}) & \to & \mathbb{R}\times\mathbb{R} \\ & ((a,b),(c,d)) & \mapsto & (ac-bd,ad+bc) \end{array} \tag{11.2}$$

Definizione 11.1 L'insieme $\mathbb{R}\times\mathbb{R}$ dotato delle operazioni di somma (11.1) e prodotto (11.2) prende il nume di *insieme dei numeri complessi* e sarà denotato con $\mathbb{C}$.

Osserviamo da subito che i numeri reali si possono immergere nei numeri complessi tramite la funzione iniettiva

$$\begin{array}{rccc} J: & \mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & a & \mapsto & (a,0) \end{array}$$

la quale rispetta le operazioni di somma e prodotto, nel senso che $\forall a,b\in\mathbb{R}$ (verifica lasciata per esercizio):

$$J(a)+_{\mathbb{C}}J(b)=J(a+_{\mathbb{R}}b)\,,\quad J(a)\cdot_{\mathbb{C}}J(b)=J(a\cdot_{\mathbb{R}}b)\,.$$

Osservazione 11.1 È bene rilevare che non è possibile estendere l'ordine di $\mathbb{R}$ ai numeri complessi. Nel senso che non è possibile definire un ordine su $\mathbb{C}$ che ristretto ad $\mathbb{R}$ coincida con l'ordine dei reali e tale che valgano le analoghe delle proprietà descritte nell'Esercizio 10.2 e nell'Esercizio 10.4. Infatti, se un tale ordine esistesse allora per ogni $z\in\mathbb{C}$ si avrebbe $z\cdot_{\mathbb{C}}z=z^2\geq 0$ contro il fatto che $(0,1)\cdot_{\mathbb{C}}(0,1)=(-1,0)\simeq -1\in\mathbb{R}$.

Denotiamo l'elemento $(0,1)\in\mathbb{C}$ con la lettera i, quindi $i^2=-1$. L'elemento i prende il nome di *unità immaginaria*.

Sia adesso $(a,b)\in\mathbb{C}$. Usando le operazioni su $\mathbb{C}$ si ottiene

$$(a,b)=(a,0)+(0,b)=(a,0)+(0,1)(b,0)\simeq a+ib$$

Segue che i numeri complessi si possono identificare come combinazioni lineari a coefficienti reali di 1 e i ed eseguire le operazioni di somma e prodotto considerando tale combinazione come un

binomio e ricordando che $i^2 = -1$. Cioè

$$(a+ib)+(c+id) = a+c+i(b+d), \quad (a+ib)(c+id) = ac-bd+i(ad+bc)$$

ritrovando le operazioni definite in $\mathbb{C}$.

Definizione 11.2 Dato un numero complesso $z = a+ib$ chiamiamo $a = \mathrm{Re}(z)$ la *parte reale* e $b = \mathrm{Im}(z)$ la *parte immaginaria*. Chiamiamo *reali* i numeri complessi la cui parte immaginaria è zero e *immaginari* quelli la cui parte reale è zero.

Esercizio 11.1 Mostrare che $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ è un campo.

Soluzione. L'elemento neutro rispetto alla somma è $0 = (0,0)$ mentre quello rispetto al prodotto è $1 = (1,0)$. Inoltre l'opposto di un numero complesso (a,b) è $(-a,-b)$. Chiaramente le due operazioni sono associative e commutative e vale la proprietà distributiva. Per terminare basta verificare l'esistenza dell'inverso moltiplicativo per ogni numero complesso $(a,b) \neq (0,0)$. Per questo basta osservare che $(a,b) \cdot_{\mathbb{C}} (a,-b)/(a^2+b^2) = (1,0) = 1$.

Da ora in poi quando è chiaro dal contesto omettiamo l'utilizzo del pedice per indicare che la somma e il prodotto sono quelle definite su $\mathbb{C}$.

Dato un numero complesso $z = a+ib$ chiamiamo $\bar{z} = a-ib$ il *coniugato* del numero complesso. Se definiamo il modulo di un numero complesso $z = a+ib$ come $|z| = \sqrt{a^2+b^2}$ si trova che $z \cdot_{\mathbb{C}} \bar{z} = a^2+b^2 = |z|^2$. Quindi dato un numero complesso $z = a+ib \neq 0$, ovvero con $a^2+b^2 \neq 0$, si ha che l'inverso moltiplicativo è dato da $z^{-1} = \bar{z}/|z|^2$.

■ **Esempio 11.1** Se $z = 2-i$ allora

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{2+i}{5} = \frac{2}{5} + i\frac{1}{5}.$$

■

Formalmente si scrive $z^{-1} = \bar{z}/|z|^2 = \bar{z}/(z\bar{z}) = 1/z$. Quindi useremo la notazione $1/z$ per indicare l'inverso di un numero complesso. Il lettore deve però riflettere che tale notazione non ha niente a che vedere con l'utilizzo delle normali frazioni definite sui numeri razionali.

Osservazione 11.2 Dato un numero complesso $z = a+ib$ si ha

$$\mathrm{Re}(z) = \frac{1}{2}(z+\bar{z}), \quad \mathrm{Im}(z) = \frac{1}{i}(z-\bar{z})$$

Inoltre valgono i seguenti criteri:

1. Un numero complesso z è reale se e solo se $z = \bar{z}$.
2. Un numero complesso z è immaginario se e solo se $z = -\bar{z}$.

11.2 Problemi proposti

Problema 11.1 Dimostrare che le operazione di somma è prodotto definite in $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ da

$$(a,b)+(a',b') = (a+a',b+b') \qquad (a,b)(a',b') = (aa'-bb',ab'+a'b)$$

soddisfano alle seguenti proprietà:

1. commutativa;
2. associativa.

Problema 11.2 Dimostrare che la funzione coniugio da $\mathbb{C}$ in $\mathbb{C}$ definita da $z = a+ib \mapsto \bar{z} = a-ib$ soddisfa le seguenti proprietà

1. $\overline{\overline{z}} = z$
2. $\overline{zw} = \overline{z}\,\overline{w}$
3. $\overline{z+w} = \overline{z} + \overline{w}$
4. $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$

Problema 11.3 Dimostrare che la funzione $|\cdot| : \mathbb{C} \to \mathbb{R}$ definita da $z = a + ib \mapsto |z| = \sqrt{z\,\overline{z}} = \sqrt{a^2+b^2}$ soddisfa le seguenti proprietà

1. $|zw| = |z|\,|w|$
2. $|z| - |w| \leq |z+w| \leq |z| + |w|$
3. $|z^{-1}| = |z|^{-1}$
4. $|z| - |w| \leq |z-w| \leq |z| + |w|$

Problema 11.4 Scrivere nella forma $a+ib$ i seguenti numeri complessi:

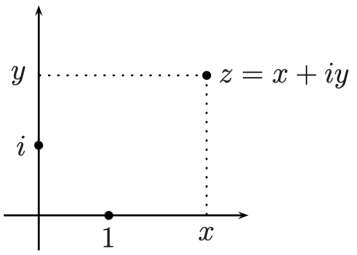
$$(4+2i)(1-i), \quad i^{-1}, \quad \frac{7-6i}{2+3i}, \quad (2+3i)^3, \quad \frac{2i}{(2+i)^2}$$

Problema 11.5 Determinare per quali $x \in \mathbb{R}$ il seguente numero è reale

$$\frac{x-2+ix}{x-3-5i}$$

11.3 Forma esponenziale dei numeri complessi

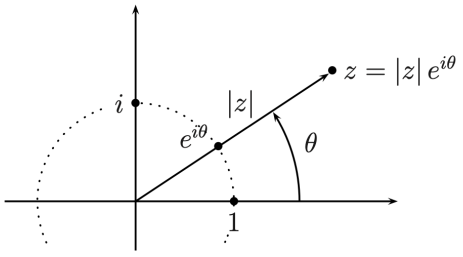
I numeri complessi scritti nella forma $z = x+iy$ prendono anche il nome di *forma cartesiana* dei numeri complessi poiché il numero viene individuato dalle sue coordinate (reali) x e y e si può scrivere $z = (x,y) = x(1,0) + y(0,1) = x + iy$ dove i particolari numeri complessi $(1,0)$ e $(0,1)$ sono stati identificati rispettivamente con l'unità reale 1 e l'unità immaginaria i. Si veda il disegno sotto che comunemente prende anche il nome di *Piano di Gauss*



La coordinata x è la parte reale di z mentre coordinata y è la parte immaginaria di z:

$$x = \mathrm{Re}(z), \quad y = \mathrm{Im}(z).$$

Esiste anche un'altra importante forma di rappresentare i numeri complessi, nota col nome di *forma esponenziale*. In questo caso, con riferimento alla figura sotto,

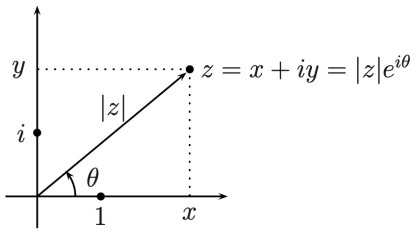


il numero complesso z viene invece individuato dal modulo $|z|$, ossia la distanza del punto z dall'origine, e dall'argomento, ossia l'angolo θ compreso tra la direzione positiva dell'asse delle x

e la semiretta uscente dall'origine e passante per z. Tale angolo viene espresso in radianti e non è definito quando $z = 0$, mentre per $z \neq 0$ è determinato, a meno di multipli di 2π (che corrisponde ad un angolo giro). In questo modo possiamo scrivere

$$z = |z|e^{i\theta}$$

dove il simbolo $e^{i\theta}$ è definito come il numero complesso di modulo unitario $\cos\theta + i\sin\theta$.
Con riferimento alla figura seguente



possiamo dare la procedura per passare dalla forma cartesiana a quella esponenziale e viceversa. Se $z = x + iy$ allora la sua forma esponenziale si ottiene tramite:

$$|z| = \sqrt{x^2+y^2}, \quad \theta = \begin{cases} \arccos(x/|z|) & \text{se } y \geq 0 \\ -\arccos(x/|z|) & \text{se } y < 0 \end{cases}$$

In questo modo viene calcolato solo uno degli infiniti argomenti associati a z e precisamente quello compreso nell'intervallo $(-\pi, \pi]$. L'insieme completo dei possibili argomenti è dato da $\theta + 2k\pi$, $k \in \mathbb{Z}$.

Il passaggio inverso è più semplice. Se $z = |z|e^{i\theta} = |z|(\cos\theta + i\sin\theta)$ allora $z = x + iy$ con

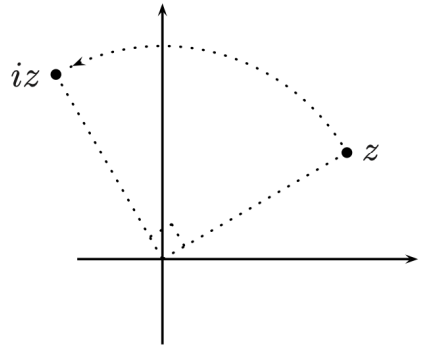
$$x = \mathrm{Re}(z) = |z|\cos\theta\,, \quad y = \mathrm{Im}(z) = |z|\sin\theta$$

■ **Esempio 11.2** Sia $z = \sqrt{3} + i$. Allora $|z| = \sqrt{3+1} = 2$ e, essendo $y = 1 > 0$, una determinazione dell'argomento è $\theta = \arccos(\sqrt{3}/2) = \pi/6$. Quindi $z = 2(\cos(\pi/6) + i\sin(\pi/6)) = 2e^{i\pi/6}$. ■

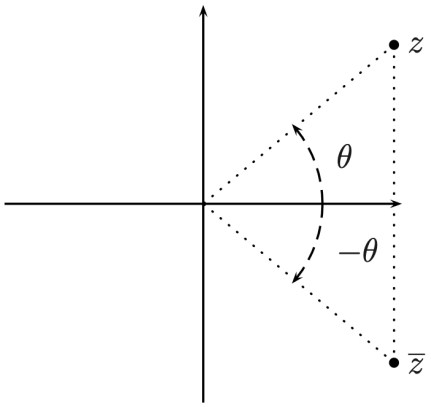
Con la notazione esponenziale la moltiplicazione dei numeri complessi diviene molto naturale. Infatti, se $z = |z|e^{i\theta}$ e $w = |w|e^{i\varphi}$ allora

$$\begin{aligned} z \cdot w = |z|e^{i\theta}|w|e^{i\varphi} &= |z||w|e^{i\theta}e^{i\varphi} = |z||w|(\cos\theta + i\sin\theta)(\cos\varphi + i\sin\varphi) \\ &= |z||w|(\cos\theta\cos\varphi - \sin\theta\sin\varphi + i(\sin\theta\cos\varphi + \sin\varphi\cos\theta)) \\ &= |z||w|(\cos(\theta+\varphi) + i\sin(\theta+\varphi)) \\ &= |z||w|e^{i(\theta+\varphi)}\,. \end{aligned}$$

Dunque nel prodotto di due numeri complessi i moduli si moltiplicano mentre gli argomenti si sommano. Un caso particolare molto interessante è il prodotto di un numero complesso z per i. Infatti, per quanto visto sopra la moltiplicazione per $i = e^{i\pi/2}$ corrisponde a una rotazione di 90 gradi in senso antiorario come mostrato nella figura sotto.



Il coniugato z di un numero complesso $z = x + iy$, definito come $\bar{z} = x - iy$ corrisponde al punto simmetrico di z rispetto all'asse reale. Quindi in forma esponenziale: se $z = |z|e^{i\theta}$ allora $\bar{z} = |z|e^{-i\theta}$, si veda la figura seguente



11.4 Potenza di un numero complesso

Come abbiamo visto, la forma esponenziale risulta particolarmente comoda quando si devono effettuare prodotti. Per esempio il calcolo del quadrato di un numero complesso $z = |z|e^{i\theta}$ si svolge nel seguente modo

$$z^2 = |z|e^{i\theta}|z|e^{i\theta} = |z|^2 e^{i2\theta}$$

Più in generale il calcolo della potenza n-esima, $n \in \mathbb{N}$, del numero complesso $z = |z|e^{i\theta}$ diventa la nota Formula di De Moivre

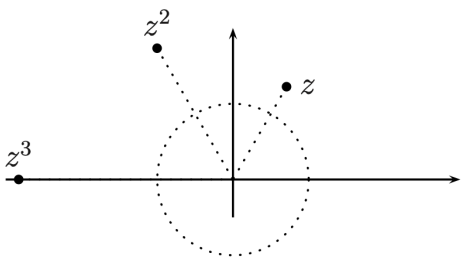
$$z^n = |z|^n e^{in\theta},$$

la cui dimostrazione si ottiene facilmente per induzione su n.

■ **Esempio 11.3** Calcoliamo le potenze di $z = \sqrt{2}e^{i\pi/3}$ per $n = 1, 2, 3$. Si trova:

$$z = \sqrt{2}e^{i\pi/3}, \quad z^2 = 2e^{i2\pi/3}, \quad z^3 = 2\sqrt{2}e^{i\pi} = -2\sqrt{2}$$

la cui rappresentazione nel Piano di Gauss è



Calcoliamo adesso le potenze di $z = 1/2 - i/2$ per $n = 1,2,3$. Possiamo eseguire direttamente il prodotto

$$z^2 = (1/2 - i/2)(1/2 - i/2) = 1/4 - 1/4 - i/2 = -i/2$$

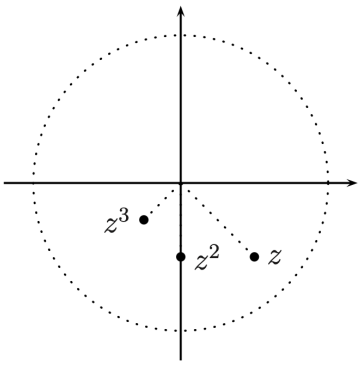
moltiplicando nuovamente

$$z^3 = zz^2 = (1/2 - i/2)(-i/2) = -1/4 - i/4\,.$$

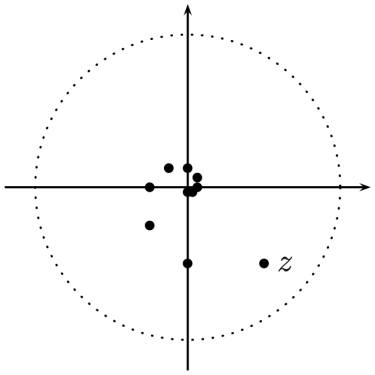
In alternativa possiamo scrivere z nella forma esponenziale e poi usare la Formula di De Moivre. Si trova $|z| = \sqrt{2}/2$ e $\theta = -\arccos(\sqrt{2}/2) = -\pi/4$. Quindi $z = \sqrt{2}/2e^{-i\pi/4}$ da cui

$$\begin{aligned} z^3 &= (\sqrt{2}/2)^3 e^{-i3\pi/4} = \sqrt{2}/4(\cos(3\pi/4) - i\sin(3\pi/4)) \\ &= \sqrt{2}/4(-\sqrt{2}/2 - i\sqrt{2}/2) = -1/4 - i/4\,. \end{aligned}$$

In questo caso la rappresentazione delle potenze di z è



Da questi esempi si può osservare che, facendo le successive potenze di un numero complesso z, i punti corrispondenti "girano" attorno all'origine. Se inoltre $|z| > 1$ allora i punti si allontanano indefinitamente, se $|z| = 1$ i punti rimangono sulla circonferenza unitaria e infine se $|z| < 1$ i punti si avvicinano all'origine. Ad esempio, le prime 10 potenze di $z = 1/2 - i/2$ sono:



■

11.5 Radici di un numero complesso

Per comprendere al meglio i risultati di questo paragrafo iniziamo con un'analisi delle equazioni in una variabile nei numeri reali. Più precisamente, dato un numero reale a ci si chiede quante e quali siano le soluzioni $x \in \mathbb{R}$ dell'equazione

$$x^n = a\,, \quad n \in \mathbb{N} \tag{11.3}$$

Come già osservato $x^2 \geq 0$ per ogni $x \in \mathbb{R}$ e di conseguenza se n è pari $x^n \geq 0$ per ogni $x \in \mathbb{R}$ e $x^n = (-x)^n$. Diversamente, se n è dispari il segno di x^n è lo stesso di x. Segue che, con riferimento all'equazione (11.3),

1. se n è pari e $a > 0$ esistono due soluzioni distinte: $\pm\sqrt[n]{a}$;
2. se n è pari e $a < 0$ non esistono soluzioni;
3. se n è dispari esiste sempre un'unica soluzione: $\sqrt[n]{a}$;
4. se $a = 0$ esiste solo la soluzione $x = 0$.

Consideriamo adesso, per un dato numero complesso w, l'equazione in $\mathbb{C}$

$$z^n = w\,, \quad n \in \mathbb{N} \tag{11.4}$$

Se $w = 0$ l'unica soluzione possibile è proprio $z = 0$. Supponiamo quindi che $w \neq 0$. In questo caso abbiamo il seguente risultato

Proposizione 11.1 Sia $w \in \mathbb{C}$, $w \neq 0$ e sia $n \in \mathbb{N}$, $n > 0$. Allora l'equazione (11.4) ha esattamente n soluzioni in $\mathbb{C}$.

Dimostrazione. Sia $w = |w|e^{i\theta}$. Allora un numero complesso $z = |z|e^{i\varphi}$ è soluzione della (11.4) se e solo se

$$z^n = |z|^n e^{in\varphi} = |w|e^{i\theta}$$

cioè se

$$\begin{cases} |z|^n = |w| \\ n\varphi = \theta + 2k\pi\,, \quad k \in \mathbb{Z} \end{cases} \tag{11.5}$$

La prima equazione della (11.5) ha un'unica soluzione positiva per $|z|$ che comunemente indichiamo con $|z| = \sqrt[n]{|w|}$. La seconda si riscrive come

$$\varphi = \frac{\theta + 2k\pi}{n}\,, \quad k \in \mathbb{Z}$$

la quale sembra produrre infinite soluzioni (una per ogni intero) ma, ricordando che nella forma esponenziali l'argomento è definito a meno di multipli interi di 2π, si ottiene

$$\begin{aligned} k = 0 \quad &\Rightarrow \quad \varphi = \frac{\theta}{n} \\ k = 1 \quad &\Rightarrow \quad \varphi = \frac{\theta}{n} + \frac{2\pi}{n} \\ \vdots \quad &\vdots \quad \vdots \\ k = n-1 \quad &\Rightarrow \quad \varphi = \frac{\theta}{n} + \frac{(n-1)2\pi}{n} \\ k = n \quad &\Rightarrow \quad \varphi = \frac{\theta}{n} + 2\pi \simeq \frac{\theta}{n} \end{aligned}$$

Segue che da $k = 0$ sino a $k = n-1$ si ottengono n soluzioni distinte mentre per $k \geq n$ le soluzioni si ripetono. In conclusione l'equazione (11.4) ammette per ogni $w = |w|e^{i\theta} \in \mathbb{C}$, $w \neq 0$, il seguente insieme di soluzioni

$$\left\{ z = |z|e^{i\varphi} \colon |z|^n = |w| \quad \wedge \quad \varphi = \frac{\theta + 2k\pi}{n}\,, \quad k = 0, 1, \ldots, n-1 \right\}.$$

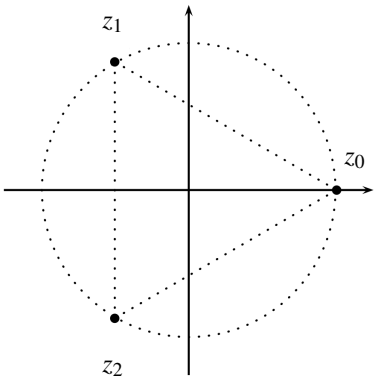
■

Convenzionalmente le soluzioni dell'equazione (11.4) prendono il nome di *radici n-esime di un numero complesso*.

■ **Esempio 11.4** Troviamo le soluzioni in $\mathbb{C}$ dell'equazione $z^3 = 1$. Siccome $1 = 1\,e^{i0}$ si ottengono le tre soluzioni

$$\left\{ z = |z|e^{i\varphi} \colon |z|^3 = 1 \quad \wedge \quad \varphi = \frac{0+2k\pi}{3}, \quad k = 0,1,3 \right\}$$
$$= \left\{ z_0 = e^{i0} = 1, \quad z_1 = e^{i(2\pi/3)}, \quad z_2 = e^{i(4\pi/3)} \right\}.$$

la cui rappresentazione grafica è la seguente

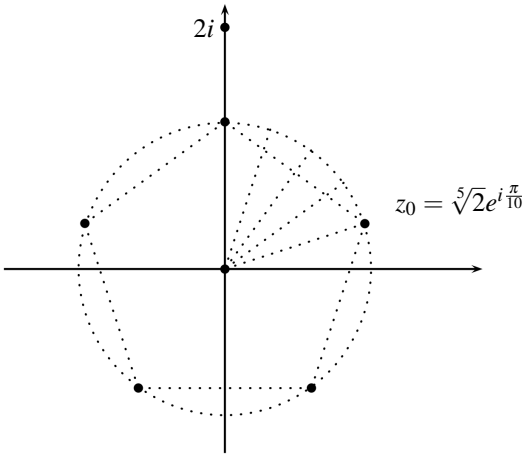


Dovrebbe essere chiaro a questo punto che le radici n-esime di 1 costituiscono i vertici di un n-agono regolare con un vertice nel punto $(1,0)$. ■

■ **Esempio 11.5** Le radici quinte del numero complesso $2i = 2e^{i\pi/2}$ sono:

$$\left\{ \sqrt[5]{2}e^{i\left(\frac{\pi}{10}+\frac{2k\pi}{5}\right)} \colon k = 0,1,2,3,4 \right\},$$

la cui rappresentazione grafica forma un pentagono sulla circonferenza di raggio $\sqrt[5]{2}$ con un vertice in $\sqrt[5]{2}e^{i\frac{\pi}{10}}$



In generale le radici n-esime di un numero complesso $w = |w|e^{i\theta}$ formano un n-agono regolare sulla circonferenza di raggio $\sqrt[n]{|w|}$ centrata nell'origine con un vertice in $z_0 = \sqrt[n]{|w|}e^{i\theta/n}$. ■

11.6 Problemi proposti

Problema 11.6 Calcolare il modulo dei seguenti numeri complessi:

$$1+i-\frac{i}{1-2i}; \quad (1+i)(1-i)(1+\sqrt{3}i); \quad \left(\frac{1+i}{1-i}-1\right)^2$$

Problema 11.7 Dato il numero complesso $z = e^{i\pi/6} + e^{i\pi/2}$
(a) esprimere z in forma cartesiana e in forma esponenziale;
(b) calcolare le radici cubiche di z.

Problema 11.8 Dimostrare che dato un numero complesso $w \neq 0$ le radici complesse ennesime di w, $\{z_0, z_1, \ldots, z_{n-1}\}$, soddisfano la condizione

$$z_0 + z_1 + \cdots + z_{n-1} = 0.$$

(Aiuto: utilizzare la formula $\sum_{i=0}^{n} q^i = \frac{1-q^{n+1}}{1-q}$)

Problema 11.9 Determinare la forma esponenziale dei seguenti numeri complessi

$$-1-i, \quad 2+2i, \quad -1+i\sqrt{3}, \quad 1-i3$$

Problema 11.10 Per quali $x, y \in \mathbb{R}$ risulta

$$(x+iy)^2 = -5+12i$$

Problema 11.11 Si determinino le radici seste di $1+i$ e le si rappresentino nel piano di Gauss.

Problema 11.12 Calcolare

$$\left(\frac{1+i}{1-i}\right)^{16} + \left(\frac{1-i}{1+i}\right)^{8},$$

Problema 11.13 Risolvere in $\mathbb{C}$ le seguenti equazioni

$$z^2 = i, \quad z^2 = -i, \quad z^2 = 1-i2$$

Problema 11.14 Mostrare che

$$(2+i\sqrt{5})^7 + (2-i\sqrt{5})^7 \in \mathbb{R}$$

Problema 11.15 Determinare tutti i numeri complessi z di modulo 1 tali che

$$\left|\frac{z}{\overline{z}} + \frac{\overline{z}}{z}\right| = 1$$

Problema 11.16 Calcolare la parte reale e immaginaria del numero complesso

$$\frac{(1+i)^{10}}{(1-i)^8}$$

Problema 11.17 Sia $z = 1/2 - i\sqrt{3}/2$. Calcolare

$$z^{8!-1}$$

Problema 11.18 Determinare l'insieme dei numeri complessi z tali che

$$|\bar{z}-2| = |\mathrm{Re}(z+2)|\,.$$

12. Aritmetica in $\mathbb{Z}$ - parte I

Questo capitolo è dedicato allo studio dei numeri interi. Ricordiamo che $(\mathbb{Z},+,\cdot)$ è un anello unitario commutativo il quale rappresenta, in un certo senso, il prototipo di anello unitario commutativo. Per tale ragione alcune delle considerazioni in questo capitolo avranno come protagonista un qualunque anello unitario commutativo $(A,+,\cdot)$. Tale impostazione permetterà di inquadrare l'algebra dei numeri interi in un contesto più generale ed, a volte, più naturale.

12.1 Divisione in un anello

Ricordiamo la definizione di anello.

Definizione 12.1 Un insieme A assieme a due operazionie binaria $+ : A \times A \to A$ e $\cdot : A \times A \to A$ forma un *anello* se, $\forall a,b,c \in A$, valgono le seguenti proprietà:

1. $(A,+)$ è un gruppo abeliano;
2. l'operazione $\cdot$ è associativa;
3. vale la proprietà distributiva.

Inoltre: se l'operazione $\cdot$ è commutativa l'anello si chiama *commutativo*; se esiste l'elemento neutro e per l'operazione $\cdot$ l'anello si chiama *unitario*.

Ricordiamo che in un anello unitario le *unità* sono gli elementi invertibili rispetto alla moltiplicazione $\cdot$.

Sia $(A,+,\cdot)$ un anello unitario commutativo. Un elemento $a \in A$, $a \neq 0$, si dice *divisore dello zero* se esiste $b \in A$, $b \neq 0$, tale che $a \cdot b = 0$. Un anello unitario commutativo privo di divisori dello zero prende il nome di *dominio di integrità* (o semplicemente dominio).

Esercizio 12.1 Dimostrare che l'anello dei numeri interi è un dominio di integrità.

Sia $(A,+,\cdot)$ un dominio di integrità. Diciamo che $a \in A$ *divide* $b \in A$, scriviamo $a|b$, se esiste $c \in A$ con $b = a \cdot c$. Se $b = a \cdot c$ diciamo altresì che b è un *multiplo* di a.

Definizione 12.2 Sia $(A,+,\cdot)$ un dominio di integrità. Un elemento $p \in A$ si dice *irriducibile* se $p \neq 0$, p non è un'unità e se $p = a \cdot b$, $a,b \in A$, implica che a o b sono una unità.

Osservazione 12.1 Ricordando che le unità di $\mathbb{Z}$ sono ± 1, si ottiene che un numero intero p è irriducibile se $p \neq 0,1,-1$ e se $p = a \cdot b$, $a,b \in \mathbb{Z}$, implica che a o b sono uguali a ± 1. In altri termini, un numero intero $p \neq 0,1,-1$ è irriducibile se è divisibile solo per ± 1 e per $\pm p$. L'ultima caratterizzazione è quella comunemente utilizzata per definire, in $\mathbb{Z}$, i numeri *primi*. In questa prima parte del capitolo preferiamo però utilizzare la denominazione "irriducibile".

12.2 Il massimo Comune Divisore (MCD)

Definizione 12.3 Sia $(A,+,\cdot)$ un dominio di integrità e siano $a,b \in A$, $a,b \neq 0$. Un *Massimo Comune Divisore* (MCD) di a e b (se esiste) è un elemento $d \in A$ tale che:

1. $d|a \quad \wedge \quad d|b$
2. se $d'|a \quad \wedge \quad d'|b \quad \Rightarrow \quad d'|d$

Se d è un MCD di $a,b \in A$ allora anche $-d$ è un MCD.

Nel caso dei numeri interi $\mathbb{Z}$, essendo quest'ultimo totalmente ordinato, scegliamo il $\max\{d,-d\}$ e lo denotiamo con (a,b). Quindi in $\mathbb{Z}$, dati $a,b \in \mathbb{Z}^*$, il massimo comune divisore (a,b) è sempre positivo.

Definizione 12.4 Due numeri interi $a,b \in \mathbb{Z}^*$ si dicono *coprimi* (*primi fra loro*) se $(a,b) = 1$.

Proposizione 12.1 Siano $a,b,c \in \mathbb{Z}^*$. Allora

(a) se $c|a \quad \wedge \quad c|b \quad \Rightarrow \quad c|(ka+mb) \quad \forall k,m \in \mathbb{Z}$

(b) se $a|a' \quad \wedge \quad b|b' \quad \Rightarrow \quad ab|a'b'$

(c) se $d|a \quad \wedge \quad d|b \quad \wedge \quad d = ka+mb,\ k,m \in \mathbb{Z}, \quad \Rightarrow \quad d$ è un MCD

(d) se $d = (a,b) \quad \Rightarrow \quad a = da_1, b = db_1$ con $(a_1,b_1) = 1$

Dimostrazione. La (a) e la (b) sono lasciate per esercizio. Per la (c). Sia $d' \in \mathbb{Z}$ con $d'|a \quad \wedge \quad d'|b$. Allora, per la (a), $d'|(ka+mb) = d$ da cui segue, per la definizione di MCD, che d è un MCD. Dimostriamo adesso la (d). Dia $d = (a,b)$. Allora, per definizione, $a = da_1 \quad \wedge \quad b = db_1$ con $a_1,b_1 \in \mathbb{Z}$. Sia $d_1 = (a_1,b_1)$. Per concludere bisogna dimostrare che $d_1 = 1$. Poiché $d|d \quad \wedge \quad d_1|a_1$ si trova, per la (b), che $dd_1|da_1 = a$. Allo stesso modo $dd_1|b$. Poiché d è un MCD segue che $dd_1|d$. Ovviamente $d|dd_1$ da cui (poiché la divisione definisce un ordine parziale) $dd_1 = d$. Segue infine che $d_1 = 1$. ■

12.3 Il Teorema della Divisione Euclidea e il Teorema di Bézout

Se $b|a$ allora esiste un $q \in \mathbb{Z}$ tale che $a = bq$. L'intero a si chiama il *dividendo*, b il *divisore* e q il *quoziente*. Più in generale, ammettendo anche il caso in cui $b \nmid a$, si ha il seguente risultato fondamentale.

Teorema 12.1 — Della divisione Euclidea. Siano $a,b \in \mathbb{Z}, b \neq 0$. Allora esistono e sono unici $q,r \in \mathbb{Z}$ tali che

$$a = bq + r, \quad 0 \leq r < |b|$$

L'intero r si chiama *resto* della divisione di a per b.

Dimostrazione. Dimostriamo inizialmente l'esistenza. Supponiamo che $b > 0$. Quindi $|b| = b$. Sia

$$S = \{x \geq 0 \colon x = a - bz,\ z \in \mathbb{Z}\} = \{a - bz \geq 0 \colon z \in \mathbb{Z}\} \subseteq \mathbb{N}$$

L'insieme S è diverso dal vuoto, infatti (poiché $b \geq 1$) $a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$. Dal Principio del Buon Ordinamento esiste $r = \min S$ il quale si scrive come $r = a - bq$ per qualche $q \in \mathbb{Z}$. Segue che $a = bq + r$. Inoltre, se $r \geq b$ allora $0 \leq r - b = a - bq - b = a - b(q+1)$. Quindi $r - b \in S$ e $r - b < r$ il ché è assurdo poiché $r = \min S$. Conseguentemente $r < b$. Abbiamo così dimostrato l'esistenza nel caso $b > 0$. Se $b < 0$, allora $b' = -b > 0$ e per la coppia a,b' esistono q',r con $a = b'q' + r$ con $0 \leq r < b' = |b|$. Ponendo $q = -q'$ risulta che la coppia q,r soddisfa $a = bq + r$ con $0 \leq r < |b|$.

Mostriamo adesso l'unicità. Supponiamo che esistano due coppie q, r e q', r' tali che

$$a = bq + r = bq' + r' \quad \text{con} \quad 0 \leq r < |b| \quad \wedge \quad 0 \leq r' < |b| \tag{12.1}$$

Poiché $\mathbb{Z}$ è totalmente ordinato possiamo supporre che $r' \geq r$. Segue che

$$0 \leq r' - r = a - bq' - a + bq = b(q - q') \quad \Rightarrow \quad |b||q - q'| = |r' - r| = r' - r \leq r' < |b|$$

Quindi $|q - q'| < 1$ da cui $|q - q'| = 0 \quad \Rightarrow \quad q = q'$. Infine, sostituendo $q = q'$ nella (12.1), si ottiene $r = r'$. ■

▪ **Esempio 12.1** Siano $a = 19$ e $b = 6$, allora $19 = 6 \cdot 3 + 1$ quindi $q = 3$ e $r = 1$. Se $a = -19$ e $b = 6$ attenzione a non commettere l'errore di scrivere $-19 = 6 \cdot (-3) - 1$ poiché il Teorema della divisione Euclidea richiede che $r \geq 0$. La scrittura corretta è $-19 = 6 \cdot (-4) + 5$, quindi $q = -4$ e $r = 5$. ▪

Teorema 12.2 — Bézout. Siano $a, b \in \mathbb{Z}^*$. Allora esiste il MCD $d = (a, b)$ ed ha la forma $d = au + bv$ con $u, v \in \mathbb{Z}$.

Dimostrazione. Sia

$$S = \{ax + by > 0 \colon x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$$

L'insieme S non è vuoto (verificare per esercizio), quindi esiste $d = au + bv = \min S$, $u, v \in \mathbb{Z}$. Dimostriamo che $d = (a, b)$. Dal Teorema della divisione Euclidea si ha

$$a = dq + r \quad 0 \leq r < d$$

Se per assurdo $r > 0$ allora $0 < r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq)$. Segue che $r \in S$ con $r < d$ contro l'ipotesi che $d = \min S$. Quindi $r = 0$ e $a = dq$, cioè $d|a$. Allo stesso modo si dimostra che $d|b$. Adesso sia $d' \in \mathbb{Z}$ con $d'|a \quad \wedge \quad d'|b$ allora $d'|au + bv = d$. ■

Osservazione 12.2 Si noti che, combinando il Teorema di Bézout con la Proposizione 12.1–(c), si ottiene la seguente: dati $a, b \in \mathbb{Z}^*$ allora

$$(a, b) = 1 \quad \Leftrightarrow \quad \exists\, u, v \in \mathbb{Z} \text{ tali che } 1 = au + bv$$

Proposizione 12.2 Siano $a, b, b' \in \mathbb{Z}$ tali che $(a, b) = 1$ e $(a, b') = 1$. Allora $(a, bb') = 1$.

Dimostrazione. Dal Teorema di Bézout esistono $u, v, u', v' \in \mathbb{Z}$ tali che

$$1 = au + bv, \quad 1 = au' + b'v'$$

Moltiplicando le due quantità sopra si ottiene

$$1 = a(auu' + bvu' + ub'v') + bb'(vv')$$

Conseguentemente, per l'Osservazione 12.2, $(a, bb') = 1$. ■

Osservazione 12.3 — Algoritmo di Euclide per il calcolo del MCD. Esiste un algoritmo per il calcolo del MCD dovuto allo stesso Euclide. Invece di illustrare il metodo generale, che richiederebbe una notazione inutilmente complessa, mostriamo il funzionamento dell'algoritmo rimandando la sua dimostrazione formale al libro di testo. Siano $a = 72$ e $b = 22$. Dal Teorema delle divisione Euclidea si trova

$$72 = 22 \cdot 3 + 6$$

Applicando il Teorema delle divisione Euclidea alla coppia $22, 6$ si ottiene

$$22 = 6 \cdot 3 + 4$$

Continuando tale processo si ottiene

$$\begin{aligned} 72 =& 22 \cdot 3 + 6 \\ 22 =& 6 \cdot 3 + 4 \\ 6 =& 4 \cdot 1 + 2 \\ 4 =& 2 \cdot 2 + 0 \end{aligned}$$

L'ultimo resto diverso da zero, cioè 2, è il MCD tra 72 e 22. È un utile esercizio convincersi che il procedimento sopra descritto conduce realmente al MCD. Inoltre, risalendo la costruzione vista sopra, partendo dalla penultima riga, si ottiene

$$\begin{aligned} 2 =& 6 + 4(-1) \\ =& 6 + [22 + 6(-3)](-1) \\ =& 6 \cdot 4 + 22(-1) \\ =& [72 + 22(-3)]4 + 22(-1) \\ =& 72 \cdot 4 + 22(-13) \end{aligned}$$

la quale fornisce un metodo per ricavare gli interi u, v annunciati nel Teorema di Bézout.

! Attenzione che gli interi u, v nel Teorema di Bézout non sono unici. Ad esempio $1 = (3, 2)$ ma

$$1 = 3 \cdot 1 + 2(-1) = 3 \cdot 3 + 2(-4)$$

La seguente proposizione è una conseguenza del Teorema di Bézout ed avrà un ruolo fondamentale nel resto del capitolo.

Proposizione 12.3 Siano $a, b, c \in \mathbb{Z}^*$ e supponiamo che $(a, c) = 1$. Se $a|(bc)$ allora $a|b$.

Dimostrazione. Poiché $(a, c) = 1$ esistono $u, v \in \mathbb{Z}$ con $1 = au + cv$. Moltiplicando per b si ottiene $b = a(bu) + (bc)v$. Infine, poiché $a|a$ e $a|bc$ si conclude che $a|b$. ■

■ **Esempio 12.2** Se $(a, c) \neq 1$ allora la conclusione della Proposizione 12.3 non è vera. Per esempio, $8|(6 \cdot 4) = 24$ ma $8 \nmid 6 \quad \wedge \quad 8 \nmid 4$. ■

12.4 Numeri primi di un dominio di integrità

In questa sezione torniamo per un momento a considerare un qualunque dominio di integrità $(A, +, \cdot)$. Diamo la seguente

Definizione 12.5 Sia $(A, +, \cdot)$ un dominio di integrità e sia $p \in A$, $p \neq 0$, p non unità. L'elemento p si dice *primo* se vale la seguente proposizione

$$p|ab \quad \Leftrightarrow \quad p|a \quad \vee \quad p|b$$

In un dominio di integrità la nozione di primo è più forte di quella di irriducibile come risulta dalla seguente

Proposizione 12.4 Sia $(A,+,\cdot)$ un dominio di integrità e sia $p \in A$ un primo. Allora p è irriducibile.

Dimostrazione. Sia $p \in A$ un primo e supponiamo che $p = ab$, $a,b \in A$. Allora $p|p = ab$ e quindi $p|a$ o $p|b$. Supponiamo che $p|a$, cioè esiste $c \in A$ con $a = pc$. Segue che $p = pcb$, ovvero, $p - pcb = 0$ da cui $p(1-cb) = 0$. Essendo A un dominio di integrità ed essendo $p \neq 0$ si perviene a $1 - cb = 0$, cioè $1 = cb$ e quindi b è un'unità. ■

Il viceversa della Proposizione 12.4 non vale per un qualsiasi dominio di integrità, si veda l'Esempio 12.3. Fortunatamente per gli interi il viceversa vale come mostrato dalla seguente proposizione.

Proposizione 12.5 Sia $p \in \mathbb{Z}$ un elemento irriducibile, allora p è primo.

Dimostrazione. Sia $p \in \mathbb{Z}$ irriducibile e supponiamo che $p|ab$, $a,b \in \mathbb{Z}$. Dobbiamo dimostrare che $p|a \vee p|b$. Se $p \nmid a$ allora, essendo p irriducibile, $(p,a) = 1$ (il lettore deve fare tutti i passaggi logici per convincersi dell'ultima affermazione). Dalla Proposizione 12.3 segue che $p|b$. ■

▪ **Esempio 12.3** Si consideri l'insieme

$$\mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \colon a,b \in \mathbb{Z}\}$$

dove i è l'unità immaginaria, cioè $i^2 = -1$. Se definiamo somma e prodotto in $\mathbb{Z}[i\sqrt{5}]$ in analogia con la somma e il prodotto definite nei numeri complessi, si verifica facilmente che $\mathbb{Z}[i\sqrt{5}]$ è un dominio di integrità le cui uniche unità sono ± 1. Adesso $3 \in \mathbb{Z}[i\sqrt{5}]$ è irriducibile ma non è primo. Infatti, supponiamo che $3 = (a + i\sqrt{5}b)(c + i\sqrt{5}d)$. Allora

$$\begin{cases} ac - 5bd = 3 \\ ad + bc = 0 \end{cases}$$

Dalla seconda equazione segue che $(a,b) = \lambda(-c,d)$, $\lambda \in \mathbb{Z}$, la quale, sostituita nella prima, restituisce $-\lambda(c^2 + 5d^2) = 3$ da cui $\lambda = -3, c = \pm 1, d = 0$. Conseguentemente, $a + i\sqrt{5}b = \pm 3$ e $c + i\sqrt{5}d = \pm 1$. Abbiamo provato che 3 è irriducibile. Adesso $3|9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ in $\mathbb{Z}[i\sqrt{5}]$ ma $3 \nmid (2 + i\sqrt{5})$ e $3 \nmid (2 - i\sqrt{5})$. Quindi 3 non è primo. ▪

12.5 Il minimo comune multiplo (mcm)

Definizione 12.6 Sia $(A,+,\cdot)$ un dominio di integrità e siano $a,b \in A$, $a,b \neq 0$. Un minimo comune multiplo di a e b è un multiplo $m \in A$ di a e b tale che se $m' \in A$ è un altro multiplo di a e b allora $m|m'$.

Come nel caso del MCD se m è un mcm allora anche $-m$ è un mcm. Nel caso del dominio $\mathbb{Z}$ scegliamo, per convenzione, il massimo tra i due, quindi $mcm(a,b) = \max\{m,-m\}$ dove m è un minimo comune multiplo di a e b.

Proposizione 12.6 Siano $a,b \in \mathbb{Z}^*$ e sia $d = (a,b)$. Allora

$$m = \frac{ab}{(a,b)} = \frac{ab}{d}$$

è un minimo comune multiplo di a e b

Dimostrazione. Sia $d = (a,b)$ allora, per la Proposizione 12.1, $a = da_1$, $b = db_1$ con $(a_1,b_1) = 1$. Segue che

$$m = \frac{ab}{d} = a_1 b = ab_1$$

da cui m è un multiplo di a e b. Sia m' un altro multiplo di a e b. Per concludere dimostriamo che $m|m'$. Poiché m' è un multiplo di a e b esistono $x,y \in \mathbb{Z}$ tali che $m' = ax$ e $m' = by$ da cui $ax = by$. Sostituendo nell'ultima uguaglianza $a = da_1$ e $b = db_1$ si trova $a_1 x = b_1 y$. Quindi b_1 divide $a_1 x$ ed essendo $(a_1,b_1) = 1$, per la Proposizione 12.3, b_1 divide x. Esiste quindi un intero x_1 tale che $x = b_1 x_1$. Si trova infine, $m' = ax = ab_1 x_1 = mx_1$, cioè $m|m'$. ■

Proposizione 12.7 Siano $a,b \in \mathbb{Z}^*$ due interi primi fra loro, cioè $1 = (a,b)$. Allora

$$a|c \quad \wedge \quad b|c \quad \Rightarrow \quad ab|c \qquad \forall c \in \mathbb{Z}$$

Dimostrazione. Se $1 = (a,b)$ per la Proposizione 12.6 l'intero ab è un minimo comune multiplo di a e b. Adesso se $a|c$ e $b|c$ vuol dire che c è un multiplo di a e b da cui, per definizione di mcm, $ab|c$. ■

▪ **Esempio 12.4** Se $(a,b) \neq 1$ la Proposizione 12.7 non è più vera. Ad esempio, $4|12$ e $6|12$ ma $24 \nmid 12$. ▪

12.6 Il Teorema fondamentale dell'aritmetica

Il teorema che segue fornisce una chiave di lettura molto importante dei numeri interi. In un certo senso asserisce che tra tutti i numeri interi alcuni sono "privilegiati" e che tutti gli altri numeri interi sono ottenuti a partire da questi. Tali numeri privilegiati sono i numeri primi ed il teorema si enuncia nel modo seguente

Teorema 12.3 — Teorema Fondamentale dell'Aritmetica. Sia $a \in \mathbb{Z}$, $a \neq 0,1,-1$. Allora esistono k primi $p_1,\ldots,p_k$ tali che

$$a = p_1 \cdot p_2 \cdots p_k$$

Inoltre, se $a = q_1 \cdot q_2 \cdots q_s$ con $q_1,\ldots,q_s$ primi, allora $k = s$ e per ogni $i \in \{1,\ldots,k\}$ esiste un $j \in \{1,\ldots,k\}$ tale che $p_i = \pm q_j$.

Dimostrazione. Dimostriamo l'esistenza. Possiamo supporre che $a > 0$ (il lettore è tenuto a fare il giusto ragionamento per concludere che dimostrata l'esistenza per $a > 0$ allora è dimostrata anche per $a < 0$). Procediamo per induzione su a. La base induttiva è $a = 2$ la quale è vera poiché 2 è un numero primo. Supponiamo che sia vera per ogni b con $2 \leq b < a$ e dimostriamo che è vera per a (induzione forte). Se a è primo abbiamo terminato. Se a non è primo allora a è riducibile ed esistono $b,c \in \mathbb{Z}$ tali che

$$a = bc \quad \wedge \quad 1 < b < a \quad \wedge \quad 1 < c < a$$

Per ipotesi induttiva b e c sono prodotto di numeri primi e, conseguentemente, $a = bc$ è prodotto di numeri primi. Dimostriamo l'unicità. Supponiamo che

$$a = p_1 \cdots p_k = q_1 \cdots q_s$$

e dimostriamo per induzione su k l'unicità. Se $k = 1$ si avrebbe

$$p_1 = q_1 \cdots q_s$$

ed essendo p_1 primo (irriducibile) necessariamente $s = 1$ e $p_1 = q_1$. Supponiamo adesso che l'unicità sia vera per $k > 1$ e dimostriamo che è vera per $k+1$. Sia

$$p_1 \cdots p_{k+1} = q_1 \cdots q_s$$

Allora p_{k+1} divide $q_1 \cdots q_s$ da cui segue, poiché p_{k+1} è primo, che $p_{k+1} | q_j$ per qualche $j \in \{1, \ldots, s\}$. Supponiamo che $q_j = q_s$ (se non fosse basterebbe riordinare il prodotto $q_1 \cdots q_s$). Allora $p_{k+1} = \pm q_s$. Segue che

$$p_1 \cdots p_k (\pm q_s) = q_1 \cdots q_s$$

ovvero

$$p_1 \cdots p_k = \pm q_1 \cdots q_{s-1}$$

Applicando a questo punto l'ipotesi induttiva si conclude.

■

Osservazione 12.4 Il Teorema fondamentale dell'aritmetica non esclude che i numeri primi nella scomposizione siano uguali. Per esempio $9 = 3 \cdot 3 = 3^2$, $\quad 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$. Raccogliendo sotto forma di potenza i primi che compaiono più volte nella decomposizione possiamo enunciare il Teorema Fondamentale dell'Aritmetica dicendo che ogni intero $a \in \mathbb{Z}$, $a \neq 0, 1, -1$, si può decomporre come

$$a = p_1^{k_1} \cdots p_s^{k_s}, \quad k_1, \ldots, k_s \in \mathbb{N}$$

con $p_1, \ldots, p_s$ primi distinti.
Per confrontare interi distinti può essere utile inserire dei primi con esponente 0 in modo da avere gli stessi primi nella decomposizione di entrambi gli interi. Ad esempio, se $a = 2^3 \cdot 5^2 \cdot 7^4$ e $b = 2^2 \cdot 5 \cdot 9^4$ scriviamo

$$a = 2^3 \cdot 5^2 \cdot 7^4 \cdot 9^0, \quad b = 2^2 \cdot 5 \cdot 7^0 \cdot 9^4$$

In questo modo se

$$a = p_1^{k_1} \cdots p_s^{k_s} \quad \wedge \quad b = p_1^{m_1} \cdots p_s^{m_s}$$

possiamo scrivere

$$(a,b) = p_1^{r_1} \cdots p_s^{r_s} \quad \wedge \quad mcm(a,b) = p_1^{q_1} \cdots p_s^{q_s}$$

dove, per ogni $i \in \{1, \ldots, s\}$,

$$r_i = \min\{k_i, m_i\}, \quad q_i = \max\{k_i, m_i\}$$

Osservazione 12.5 Utilizzando il teorema fondamentale dell'aritmetica, possiamo stabilire una corrispondenza biunivoca tra l'insieme dei numeri naturali e l'insieme dei razionali positivi.
Per ogni naturale $n > 1$, scriviamo n come prodotto di primi, raggruppando separatamente i fattori primi con molteplicità pari e quelli con molteplicità dispari,

$$n = \left(p_1^{2a_1} \cdots p_r^{2a_r}\right) \left(q_1^{2b_1 - 1} \cdots q_s^{2b_s - 1}\right)$$

e definiamo

$$\varphi(n) = \frac{p_1^{a_1} \cdots p_r^{a_r}}{q_1^{b_1} \cdots q_s^{b_s}}.$$

Poniamo inoltre $\varphi(1) = 1$ e $\varphi(0) = 0$. È facile vedere che φ è la corrispondenza biunivoca richiesta. Infatti, poiché ogni naturale $n > 1$ ha una decomposizione in fattori primi unica, φ è iniettiva. Per dimostrare che φ è suriettiva, consideriamo un qualsiasi quoziente p/q di

numeri naturali p e q senza fattori comuni. Siano $p = p_1^{a_1} \cdots p_r^{a_r}$ e $q = q_1^{b_1} \cdots q_s^{b_s}$ le rispettive decomposizioni in fattori primi. Allora $\varphi\left(p_1^{2a_1} \cdots p_r^{2a_r}\, q_1^{2b_1-1} \cdots q_s^{2b_s-1}\right) = p/q$.

Enunciamo adesso il famoso Teorema di Euclide sull'infinità dei numeri primi.

Teorema 12.4 Esistono infiniti numeri primi.

Dimostrazione. Sia $\mathbb{P} = \{\text{l'insieme dei numeri primi}\}$. Supponiamo per assurdo che $\mathbb{P}$ sia finito. Allora esiste $n \in \mathbb{N}^*$ e una biezione $\{1,\ldots,n\} \leftrightarrow \mathbb{P}$. Sia quindi $\mathbb{P} = \{p_1,\ldots,p_n\}$ e sia $N = p_1 \cdots p_n + 1$. Poiché $N > 1$, per il Teorema Fondamentale dell'aritmetica, esiste un primo p che divide N. Dimostriamo che $p \notin \mathbb{P} = \{p_1,\ldots,p_n\}$. Infatti, se per assurdo $p \in \mathbb{P} = \{p_1,\ldots,p_n\}$, allora p dividerebbe $N - p_1 \cdots p_n = 1$ che conduce ad una contraddizione. Quindi $p \notin \mathbb{P} = \{p_1,\ldots,p_n\}$ contro l'ipotesi che $\mathbb{P}$ è l'insieme di tutti i numeri primi. ■

Vediamo ora il *crivello di Eratostene* (276-194 a.C.) che consente, in linea di principio, di determinare tutti i numeri primi minori o uguali di un dato numero intero positivo n. Il modo più naturale, ma di gran lunga non il più efficiente, per determinare se un numero n è primo consiste nel verificare che non sia divisibile per alcun numero che sia minore di $(n+1)/2$. Il seguente risultato, basato sul Teorema Fondamentale dell'aritmetica, riduce il numero di divisioni necessarie.

Proposizione 12.8 Se un intero positivo n non è divisibile per nessun numero primo minore o uguale di $\sqrt{n}$, allora n è primo.

Dimostrazione. Dimostriamo la contronominale. Supponiamo che n non sia primo. Allora n è riducibile, cioè $n = ab$ con a e b numeri interi tali che $1 < a < n$ e $1 < b < n$. Uno dei fattori, a o b, è necessariamente minore o uguale di $\sqrt{n}$: altrimenti si avrebbe $n = ab > \sqrt{n}\sqrt{n} = n$, che conduce ad un assurdo. Quindi n ha un fattore, diciamo a, minore o uguale di $\sqrt{n}$. Se a è primo, la proposizione è dimostrata. Altrimenti, per il Teorema Fondamentale dell'aritmetica, a ha un fattore primo p e $p < a \leq \sqrt{n}$ con $p|a|n$. ■

▪ **Esempio 12.5** Per dimostrare che il numero 397 è primo, è sufficiente dimostrare che non è divisibile per alcun numero primo minore o uguale a $\sqrt{397}$, vale a dire che non è divisibile per $2,3,5,7,11,13,17$ e 19. Il lettore può facilmente verificare che questo sia il caso. ▪

La Proposizione 12.8 potrebbe sembrare poco importante quando si tratta di numeri piccoli, ma quando i numeri sono molto grandi diventa evidente il tempo risparmiato nei calcoli necessari per verificare che un numero sia primo. Per poter utilizzare l'ultimo risultato, tuttavia, dobbiamo conoscere i numeri primi minore o uguali di $\sqrt{n}$, e questo può risultare laborioso. Per ovviare a questo possiamo utilizzare una forma più debole, e controllare se n è divisibile per tutti i numeri interi minori o uguali di $\sqrt{n}$.
È necessario sottolineare che questa procedura non solo è un test di primalità, nel senso che determina se un dato numero è primo, ma fornisce anche una fattorizzazione nel caso in cui fosse riducibile.

Per determinare tutti i numeri primi minori o uguali di un dato numero n, possiamo procedere nel modo seguente. Si annotano tutti i numeri minori o uguali di n. Si sottolinea 2 poiché è primo. Quindi si eliminano tutti i multipli di 2 (poiché non sono primi). Di seguito si sottolinea il successivo numero primo, ovvero 3, quindi si eliminano tutti i multipli di 3, perché ancora una volta non sono primi, e così via fino all'ultimo primo minore o uguale di $\sqrt{n}$.
Ora, tutti i numeri sottolineati, assieme a tutti i numeri che non sono stati eliminati, forniscono l'elenco completo di tutti i numeri primi inferiori o uguale di n. I numeri non cancellati sono primi

perché non sono divisibili per qualsiasi primo minore o uguale di $\sqrt{n}$. Il termine crivello descrive precisamente questa procedura di cancellazione successiva di numeri non primi.

■ **Esempio 12.6** Vediamo passo passo come funziona la procedura quando vogliamo trovare tutti i numeri primi minori o uguali a 100. La prima tabella mostra tutti i numeri da 1 di 100. Nelle tabelle successive vengono eliminati, rispettivamente, i multipli di 2, di 3, di 5 e di 7. I numeri rimanenti nell'ultima tabella rappresentano tutti i numeri primi minori di 100.

$$\begin{bmatrix}
 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\
21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\
31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\
41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 \\
51 & 52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 \\
61 & 62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 \\
71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 \\
81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 \\
91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100
\end{bmatrix}
\quad
\begin{bmatrix}
 & \underline{2} & 3 & 5 & 7 & 9 \\
11 & & 13 & 15 & 17 & 19 \\
21 & & 23 & 25 & 27 & 29 \\
31 & & 33 & 35 & 37 & 39 \\
41 & & 43 & 45 & 47 & 49 \\
51 & & 53 & 55 & 57 & 59 \\
61 & & 63 & 65 & 67 & 69 \\
71 & & 73 & 75 & 77 & 79 \\
81 & & 83 & 85 & 87 & 89 \\
91 & & 93 & 95 & 97 & 99
\end{bmatrix}$$

$$\begin{bmatrix}
 & \underline{2} & \underline{3} & 5 & 7 & \\
11 & & 13 & & 17 & 19 \\
 & & 23 & 25 & & 29 \\
31 & & & 35 & 37 & \\
41 & & 43 & & 47 & 49 \\
 & & 53 & 55 & & 59 \\
61 & & & 65 & 67 & \\
71 & & 73 & & 77 & 79 \\
 & & 83 & 85 & & 89 \\
91 & & & 95 & 97 &
\end{bmatrix}
\quad
\begin{bmatrix}
 & \underline{2} & \underline{3} & \underline{5} & 7 & \\
11 & & 13 & & 17 & 19 \\
 & & 23 & & & 29 \\
31 & & & & 37 & \\
41 & & 43 & & 47 & 49 \\
 & & 53 & & & 59 \\
61 & & & & 67 & \\
71 & & 73 & & 77 & 79 \\
 & & 83 & & & 89 \\
91 & & & & 97 &
\end{bmatrix}$$

$$\begin{bmatrix}
 & \underline{2} & \underline{3} & \underline{5} & \underline{7} & \\
11 & & 13 & & 17 & 19 \\
 & & 23 & & & 29 \\
31 & & & & 37 & \\
41 & & 43 & & 47 & \\
 & & 53 & & & 59 \\
61 & & & & 67 & \\
71 & & 73 & & & 79 \\
 & & 83 & & & 89 \\
 & & & & 97 &
\end{bmatrix}$$

■

12.7 Equazioni diofantee

In questa sezione considereremo le *equazioni diofantee* (che prendono il nome dal matematico Diofanto di Alessandria[1] del III secolo): si tratta di equazioni in una o più variabili, per le quali cerchiamo soluzioni a valori interi. Una delle più semplici è l'equazione diofantea lineare $ax+by=c$. Il seguente risultato era già noto al matematico indiano *Brahmagupta*, intorno al 628 d.C.

Proposizione 12.9 Siano a,b e c interi, con a e b non nulli, e sia $d=(a,b)$. Allora l'equazione

$$ax+by=c$$

[1] L'epitaffio nella tomba di Diofanto recita: «Questa tomba racchiude Diofanto, meraviglia da contemplare! Per mezzo dell'arte aritmetica insegna la misura della sua vita. Dio gli concesse la fanciullezza per un sesto della sua vita; dopo un altro dodicesimo la barba coprì le sue guance; dopo un settimo accese la fiaccola nuziale, e dopo cinque anni ebbe un figlio. Ahimè! il misero fanciullo, pur tanto amato, appena raggiunta la metà degli anni di vita del padre, morì. Quattro anni ancora, mitigando il proprio dolore con la scienza dei numeri, visse Diofanto a raggiungere il termine della sua vita» Quanti anni ha vissuto Diofanto?

ha una soluzione intera x, y se e solo se d divide c. Inoltre, se esiste una soluzione esistono infinite soluzioni date da

$$x = x_0 + \frac{bk}{d}, \quad y = y_0 - \frac{ak}{d} \quad (k \in \mathbb{Z}),$$

dove x_0, y_0 è una soluzione particolare.

Dimostrazione. Il fatto che esiste una soluzione se e solo se $d \mid c$ è conseguenza immediata del Teorema di Bézout 12.2. Infatti, sia $d = (a,b) = au + bv$. Se $d|c$ allora $c = dc_1$ da cui $c = dc_1 = a(uc_1) + b(vc_1)$. Segue che uc_1, vc_1 è una soluzione dell'equazione $ax + by = c$. Viceversa, se x_0, y_0 è una soluzione allora $ax_0 + bx_0 = c$ e chiaramente $d = (a,b)|c$. Per la seconda parte, sia x_0, y_0 una soluzione particolare, allora

$$ax_0 + by_0 = c.$$

Se poniamo

$$x = x_0 + \frac{bk}{d}, \quad y = y_0 - \frac{ak}{d}$$

dove k è un intero, si trova

$$ax + by = a\left(x_0 + \frac{bk}{d}\right) + b\left(y_0 - \frac{ak}{d}\right) = ax_0 + by_0 = c,$$

quindi x, y è una soluzione per ogni $k \in \mathbb{Z}$ (si osservi che x e y sono interi poiché d divide sia a che b). Mostriamo adesso che tutte le soluzioni sono di questa forma. Sia x, y un'altra soluzione intera, quindi $ax + by = c$. Siccome $ax + by = c = ax_0 + by_0$ si ha

$$a(x - x_0) + b(y - y_0) = 0,$$

dividendo per d si ottiene

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{12.2}$$

Segue che b/d divide la quantità a sinistra della (12.2) ed essendo coprimo con a/d si trova che b/d divide $x - x_0$. Ne consegue che $x - x_0 = bk/d$ per qualche intero k, da cui

$$x = x_0 + \frac{bk}{d}.$$

Sostituendo il valore trovato per $x - x_0$ in (12.2) otteniamo

$$-\frac{b}{d}(y - y_0) = \frac{a}{d}(x - x_0) = \frac{a}{d} \cdot \frac{bk}{d},$$

che dividendo per b/d conduce a

$$y = y_0 - \frac{ak}{d}.$$

■

Osservazione 12.6 Riassumendo, possiamo determinare le soluzioni dell'equazione diofantea

$$ax + by = c$$

seguendo i seguenti passi:

(1) si calcola $d = (a,b)$
(2) se d non divide c allora non ci sono soluzioni
(3) se $d \mid c$, si scrive $c = dc_1$ e si determinano due interi u e v tali che $au + bv = d$
(4) allora $x_0 = uc_1, y_0 = vc_1$ è una soluzione particolare dell'equazione $ax + by = c$

(4) infine si usa la Proposizione 12.9 per determinare la soluzione generale x, y.

■ **Esempio 12.7** Consideriamo l'equazione diofantea

$$1492x + 1066y = -4$$

Usando l'algoritmo euclideo si trova $d = (a,b) = (1492, 1066) = 2$ il quale divide $c = -4$. Inoltre $-4 = 2(-2)$, cioè $c_1 = -2$. Sempre tramite l'algoritmo euclideo si trova $2 = (-5)\,1492 + (7)\,1066$. Quindi $u = -5$ e $v = 7$, da cui $x_0 = (-5)(-2) = 10$ e $y_0 = 7(-2) = -14$ fornisce una soluzione particolare. Dalla Proposizione 12.9 la soluzione generale ha la forma

$$x = 10 + \frac{1066k}{2} = 10 + 533k, \quad y = -14 - \frac{1492k}{2} = -14 - 746k \quad (k \in \mathbb{Z})$$

■

12.8 Problemi proposti

Problema 12.1 Calcolare il MCD di 4415 e 1554 e scriverlo come combinazione lineare degli stessi numeri.

Problema 12.2 Siano a, b, c numeri interi non nulli. Si dimostri che $(a,(b,c)) = ((a,b),c)$.

Problema 12.3 Siano $a, b, c \in \mathbb{Z}^*$. Dimostrare che se $(a,b) = 1$ e se $c|a$ allora anche $(c,b) = 1$.

Problema 12.4 Siano a, b, c numeri interi non nulli. Si dimostri che se a divide bc allora $a/(a,b)$ divide c.

Problema 12.5 Nelle divisione euclidea ($a = bq + r$) come si modificano q ed r se si sostituiscono a e b con i multipli ma e mb?

Problema 12.6 Supponiamo di dover dividere 123456 per 365, cioè di voler trovare gli interi q e r tali che $123456 = 365q + r$, con $0 \leq r < 365$. Non ci va di calcolarli a mano, quindi prendiamo una calcolatrice e troviamo che il risultato della divisione di 123456 per 365 è $338,23561644$. Come possiamo determinare q e r come richiesto?

Problema 12.7 Dimostra per induzione che due numeri di Fibonacci consecutivi sono primi tra loro.

Problema 12.8 Si trovino tre interi a, b, c tali che $a \nmid b$, $a \nmid c$ e $a|bc$.

Problema 12.9 Siano $a_1, a_2 \ldots a_n \in \mathbb{Z}$ non tutti nulli. Il MCD degli interi $a_1, a_2 \ldots a_n$ è un numero d tale che: (i) d divide ciascuno degli a_i, $i = 1, 2 \ldots, n$; (ii) d è un multiplo di ogni intero che divide ciascuno degli a_i, $i = 1, 2 \ldots, n$. Dimostrare che d esiste e applicare il Problema 12.2 per determinare d.

Problema 12.10 Determinare, se esiste, la soluzione generale delle seguenti equazioni diofantee

$$8x + 5y = 81\,, \quad 5x + 10y = 100\,, \quad 51x + 132y = 9$$

Problema 12.11 Utilizzando il Teorema Fondamentale dell'Aritmetica dimostrare che $\log_2 3$ è un numero irrazionale.

Problema 12.12 Siano $a, b \in \mathbb{Z}, a, b \neq 0, a \neq b$. Mostrare che $(a,b) = (b, a-b)$.

Problema 12.13 Mostrare che due interi a, b consecutivi hanno $(a,b) = 1$.

Problema 12.14 Siano $a, b \in \mathbb{Z}, a, b \neq 0, a > b$ e sia r il resto della divisione di a per b. Mostrare che $(a,b) = (b,r)$.

13. Aritmetica in $\mathbb{Z}$ - parte II

13.1 Congruenze

Sia $m > 1$ un intero.

Definizione 13.1 Siano $a, b \in \mathbb{Z}$. Diciamo che a è *congruo* a b *modulo* m, in formula

$$a \equiv_m b$$

se $m|(a-b)$.

Esercizio 13.1 Dimostrare che la relazione in $\mathbb{Z}$

$$aRb \quad \Leftrightarrow \quad a \equiv_m b$$

è di equivalenza

Indichiamo con

$$\mathbb{Z}_m = \mathbb{Z}/R$$

l'insieme quoziente ottenuto considerando le classi di equivalenza modulo m. Gli elementi di $\mathbb{Z}_m$ sono indicati con $[a]_m$, quindi

$$[a]_m = \{b \in \mathbb{Z} \colon aRb\} = \{b \in \mathbb{Z} \colon a \equiv_m b\} = \{b \in \mathbb{Z} \colon m|(a-b)\} = \{a+mk \colon k \in \mathbb{Z}\}$$

Per comprendere la natura degli elementi delle classi modulo m osserviamo i seguenti fatti.

- Sia $a \in \mathbb{Z}$, allora $a = mq + r$ con $q, r \in \mathbb{Z} \quad \wedge \quad 0 \leq r < m$. Segue che $a - r = mq$ e quindi $m|(a-r)$, ovvero $r \in [a]_m$.
- Sia $b \in [a]_m$. Allora $m|(a-b)$, cioè $b = a + mk$ per qualche $k \in \mathbb{Z}$. Sia $a = mq + r$ con $0 \leq r < m$. Segue che $b = m(k+q) + r$ da cui il resto della divisione di b per m è r.

In conclusione se $b \in [a]_m$ allora a e b hanno lo stesso resto nella divisione per m. Possiamo quindi rappresentare le classi modulo m tramite il resto della divisione per m. Essendo il resto della divisione per m un numero minore di m si ottengono esattamente m classi di equivalenza. Più precisamente

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

Con la notazione vista sopra si parlerà di *classi di resto modulo m*. Si osservi che $\mathbb{Z}_m$ è un insieme finito la cui cardinalità è proprio m.

Esercizio 13.2 Dimostrare che se $n|m$ allora, per ogni $a,b \in \mathbb{Z}$,

$$a \equiv_m b \quad \Rightarrow \quad a \equiv_n b$$

Esercizio 13.3 Dimostrare che se $(m,n) = 1$ allora, per ogni $a,b \in \mathbb{Z}$,

$$a \equiv_{mn} b \quad \Leftrightarrow \quad a \equiv_m b \quad \wedge \quad a \equiv_n b$$

Esercizio 13.4 Dimostrare che se $(m,a) = 1$ allora, per ogni $b,c \in \mathbb{Z}$,

$$ab \equiv_m ac \quad \Leftrightarrow \quad b \equiv_m c$$

Dati $[a]_m, [b]_m \in \mathbb{Z}_m$ definiamo le seguenti operazioni di somma e prodotto

$$[a]_m + [b]_m = [a+b]_m\,, \quad [a]_m \cdot [b]_m = [a \cdot b]_m$$

Affinché le operazioni sopra siano *ben definite* bisogna verificare che non dipendono dal rappresentante scelto. Cioè che se $a' \in [a]_m$ e $b' \in [b]_m$ allora $a'+b' \in [a+b]_m$ e $a' \cdot b' \in [a \cdot b]_m$ o, equivalentemente, che

$$a' \equiv_m a \quad \wedge \quad b' \equiv_m b \quad \Rightarrow \quad (i) \quad a'+b' \equiv_m a+b \quad \wedge \quad (ii) \quad a' \cdot b' \equiv_m a \cdot b$$

Per dimostrare la (i) se $m|(a'-a)$ e $m|(b'-b)$ allora $m|(a'-a+b'-b) = (a'+b') - (a+b)$. Per la (ii) bisogna verificare che $m|(a' \cdot b' - a \cdot b)$. Adesso

$$a' \cdot b' - a \cdot b = a' \cdot b' - a \cdot b + a \cdot b' - a \cdot b' = a(b'-b) + b'(a'-a)$$

da cui segue la tesi.

Osservazione 13.1 Quanto visto sopra garantisce che se $a' \equiv_m a$ e $b' \equiv_m ab$ allora

$$a'+b' \equiv_m a+b \quad \wedge \quad a' \cdot b' \equiv_m a \cdot b$$

Esercizio 13.5 Dimostrare che $\mathbb{Z}_m$ con le operazioni di somma e prodotto sopra definite è un anello unitario commutativo dove: l'elemento neutro per la somma è la classe $[0]_m$; l'elemento neutro per la moltiplicazione è la classe $[1]_m$.

Esercizio 13.6 Determinare le unità di $\mathbb{Z}_{12}$ e di $\mathbb{Z}_{15}$.

L'anello $(\mathbb{Z}_m, +, \cdot)$ non è necessariamente un dominio di integrità. Ad esempio, in $\mathbb{Z}_6$ si ha $[3]_6 \cdot [2]_6 = [6]_6 = [0]_6$ ma $[3]_6, [2]_6 \neq [0]_6$.

Se p è primo vale invece la seguente

Proposizione 13.1 Sia p un numero primo positivo. Allora $(\mathbb{Z}_p, +, \cdot)$ è un campo.

Dimostrazione. Verifichiamo per prima cosa che $\mathbb{Z}_p$ è un dominio di integrità. Infatti, se $[a]_p \cdot [b]_p = [0]_p$ allora $[a \cdot b]_p = [0]_p$ il che significa che $a \cdot b$ è un multiplo di p, ovvero $p|a \cdot b$. Poiché p è primo si conclude che $p|a$ o $p|b$, cioè che $[a]_p = [0]_p$ o $[b]_p = [0]_p$. Per concludere che $\mathbb{Z}_p$ è un campo dimostriamo che ogni elemento $[a]_p$ diverso dalla classe $[0]_p$ ha un inverso moltiplicativo. Per questo basta verificare che per ogni a, $1 \leq a < p$, esiste un x, $1 \leq x < p$, tale che $ax \equiv_p 1$. Poiché $a < p$ e p è primo si ha $(a,p) = 1$, cioè esistono $x,y \in \mathbb{Z}$ tali che $1 = ax + py$ (utilizzando la Proposizione 12.9 il lettore deve convincersi che tale x può essere scelto minore di p). Segue che $1 - ax = py$ da cui $p|(1-ax)$ cioè $ax \equiv_p 1$. ■

Osservazione 13.2 Nell'anello $(\mathbb{Z}_m, +, \cdot)$ non tutti gli elementi sono invertibili. Per esempio in $\mathbb{Z}_6$ la classe $[2]_6$ non ha un inverso moltiplicativo, infatti $[2]_6[2]_6 = [4]_6$, $[2]_6[4]_6 = [8]_6 = [2]_6$, $[2]_6[5]_6 = [10]_6 = [4]_6$. Seguendo la dimostrazione della Proposizione 13.1 si dimostra (esercizio) che $[a]_m \in \mathbb{Z}_m$ è invertibile se e solo se $(a,m) = 1$.

Concludiamo il paragrafo con un elegante teorema dovuto a Fermat. Per comprendere il significato del teorema pensiamo al seguente enunciato:

$$p \text{ è primo} \quad \Leftrightarrow \quad 2^p \equiv_p 2$$

Per un certo periodo nella storia si credeva che tale risultato fosse vero, in particolare che l'implicazione "$\Leftarrow$" fosse vera. Infatti,

$2^2 = 4 \equiv_2 2$ 2 è primo,
$2^3 = 8 \equiv_3 2$ 3 è primo,
$2^4 = 16 \not\equiv_4 2$ 4 non è primo,
$2^5 = 32 \equiv_5 2$ 5 è primo,
$2^6 = 64 \not\equiv_6 2$ 6 non è primo,
$2^7 = 128 \equiv_7 2$ 7 è primo ...

da cui sembra che si possa concludere che l'implicazione "$\Leftarrow$" sia vera. Di fatto si potrebbe andare avanti per un bel po' e solo arrivati a 2^{341} si scoprirebbe che $2^{341} \equiv_{341} 2$ ma $341 = 11 \cdot 31$. Confermato che l'implicazione "$\Leftarrow$" non è vera rimane aperta la domanda se almeno l'implicazione "$\Rightarrow$" sia vera. Il teorema seguente mostra addirittura qualcosa di più

Teorema 13.1 — Piccolo teorema di Fermat. Sia $a \in \mathbb{Z}$ e sia p un numero primo positivo. Allora

$$a^p \equiv_p a$$

Dimostrazione. Dimostriamo preliminarmente il seguente fatto: se $a, b \in \mathbb{Z}$, $a, b \neq 0$, e p è un primo positivo, allora

$$(a+b)^p \equiv_p a^p + b^p \tag{13.1}$$

Infatti, dalla formula del binomio di Newton, si ha

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i$$

Per concludere basta provare che, per ogni $i = 1, \dots p-1$, $\binom{p}{i}$ è divisibile per p. Ricordando la (7.1) si ha

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!} \quad \Rightarrow \quad \binom{p}{i} i!\,(p-i)! = p(p-1)! \quad \Rightarrow \quad p \Big| \binom{p}{i} i!\,(p-i)!$$

Adesso, tenendo in considerazione che $1 \leq i \leq p-1$, si evince che p non divide $i!$. Infatti, se p dovesse dividere $i!$ allora (poiché p è primo) dovrebbe dividere uno dei numeri tra 1 e i, fatto impossibile poiché $1 \leq i \leq p-1$. Allo stesso modo p non divide $(p-i)!$. Segue, che $p \big| \binom{p}{i}$. Dimostrata la (13.1) procediamo con la dimostrazione del teorema. Supponiamo inizialmente che $a \geq 0$ e procediamo per induzione su a. Se $a = 0$ la proposizione è vera $0^p = 0 \equiv_p 0$. Supponiamo che sia vera per a e dimostriamola per $a+1$. Si ha

$$(a+1)^p \equiv_p a^p + 1 \equiv_p a + 1$$

dove nella prima congruenza abbiamo usato la (13.1) mentre nella seconda l'ipotesi induttiva. Se $a < 0$ allora $-a > 0$ e

$$0 = (a + (-a))^p \equiv_p a^p + (-a)^p \equiv_p a^p + (-a) \tag{13.2}$$

dove nel primo passaggio abbiamo utilizzato la (13.1) mentre nel secondo il fatto che il teorema è stato dimostrato vero per un intero positivo. La (13.2) implica immediatamente che $a^p \equiv_p a$. ■

Il seguente corollario è anch'esso noto con il nome "Piccolo Teorema di Fermat".

Corollario 13.1 Sia $a \in \mathbb{Z}$ e sia p un numero primo positivo con $(a,p) = 1$. Allora

$$a^{p-1} \equiv_p 1$$

Dimostrazione. Dal Teorema 13.1 si ha che $p|(a^p - a) = a(a^{p-1} - 1)$. Poiché $(a,p) = 1$ si conclude dalla Proposizione 12.3 che $p|(a^{p-1} - 1)$. ■

Osservazione 13.3 Dimostrato il piccolo teorema di Fermat e il suo corollario sorge spontanea la seguente domanda:

$$\textit{se } p \textit{ è tale che } a^{p-1} \equiv_p 1 \textit{ per ogni } a \in \mathbb{Z} \textit{ con } (a,p) = 1 \quad \Rightarrow \quad p \textit{ è primo?}$$

Ancora una volta la risposta è negativa e bisogna arrivare sino a 561. Infatti, per ogni $a \in \mathbb{Z}$ con $(a,561) = 1$ si ha che $a^{560} \equiv_{561} 1$ ma $561 = 3 \cdot 11 \cdot 17$. Per verificare che $a^{560} \equiv_{561} 1$ per ogni $a \in \mathbb{Z}$ con $(a,561) = 1$ si osservi preliminarmente che $560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$. Utilizzando il Corollario 13.1 si trova

$$a^{560} = a^{2 \cdot 280} = \left(a^{280}\right)^2 \equiv_3 1$$
$$a^{560} = a^{10 \cdot 56} = \left(a^{56}\right)^{10} \equiv_{11} 1$$
$$a^{560} = a^{16 \cdot 35} = \left(a^{35}\right)^{16} \equiv_{17} 1$$

quindi

$$3|(a^{560} - 1), \quad 11|(a^{560} - 1), \quad 17|(a^{560} - 1)$$

da cui, per la Proposizione 12.7, $3 \cdot 11 \cdot 17|(a^{560} - 1)$, cioè $561|(a^{560} - 1)$. Un numero naturale n, non primo, tale che $a^{n-1} \equiv_n 1$ per ogni $a \in \mathbb{Z}$, $(a,n) = 1$, si chiama *numero di Carmichael*.

13.2 Equazioni congruenzali

Consideriamo l'equazione $ax = b$ con $a,b \in \mathbb{Z}^*$. Se cerchiamo soluzioni intere di tale equazione notiamo subito che, in accordo con la Proposizione 12.9, se a non divide b tali soluzioni non esistono. Quindi appare poco utile considerare la teoria delle equazioni di primo grado in una variabile in $\mathbb{Z}$. Invece l'equazione naturale da considerare in $\mathbb{Z}$ è un'equazione *congruenzale* del tipo

$$ax \equiv_m b$$

Per esempio l'equazione $2x = 3$ non ammette alcuna soluzione intera mentre l'equazione congruenzale $2x \equiv_5 3$ ha, per esempio, la soluzione $x = 4$. In generale si ha il seguente risultato.

Proposizione 13.2 Sia $a \in \mathbb{Z}^*$ e sia $m > 1$. Allora l'equazione $ax \equiv_m b$, $b \in \mathbb{Z}$, ammette una soluzione se e solo se $d = (a,m)|b$.

Inoltre se x_o è una soluzione allora l'insieme di tutte le soluzioni è

$$Sol = \{x_o + km_1 : m = dm_1\,,\ k \in \mathbb{Z}\}$$

Dimostrazione. Se esiste una soluzione x_o allora $m|(ax_o - b)$. Segue che $d = (a,m)|m|(ax_o - b)$ e $d|a$, conseguentemente $d|b$. Viceversa, se $d|b$ allora $b = db_1$, $b_1 \in \mathbb{Z}$. Inoltre, dal Teorema di

Bézout, $d = au + mv$, $u, v \in \mathbb{Z}$. Infine

$$b = db_1 = (au + mv)b_1 = ab_1u + mb_1v \equiv_m a(b_1u)$$

quindi b_1u è una soluzione dell'equazione congruenzale $ax \equiv_m b$.

Supponiamo adesso che x_o sia una soluzione particolare. Allora, per ogni $k \in \mathbb{Z}$,

$$a(x_o + km_1) = ax_o + a_1dkm_1 = ax_o + a_1km \equiv_m ax_o \equiv_m b$$

quindi $x_o + km_1$ è una soluzione per ogni $k \in \mathbb{Z}$. Questo mostra che $\{x_o + km_1 \colon m = dm_1\,,\ k \in \mathbb{Z}\} \subseteq Sol$. Mostriamo adesso l'altra inclusione. Sia $x_1 \in Sol$ un'altra soluzione. Si ha

$$\begin{cases} ax_0 \equiv_m b \\ ax_1 \equiv_m b \end{cases} \quad \Rightarrow \quad ax_0 \equiv_m ax_1 \quad \Rightarrow \quad m|a(x_1 - x_o) \quad \Rightarrow \quad a(x_1 - x_o) = k_1m\,,\ k_1 \in \mathbb{Z}$$

Segue che, scrivendo $a = a_1d$ e $m = m_1d$,

$$a_1d(x_1 - x_o) = k_1m_1d \quad \Rightarrow \quad a_1(x_1 - x_o) = k_1m_1 \quad \Rightarrow \quad a_1|k_1 \quad \Rightarrow \quad k_1 = a_1k\,,\ k \in \mathbb{Z}$$

dove nella penultima implicazione si è usato che $(a_1, m_1) = 1$. Sostituendo il valore trovato per k_1 in $a_1(x_1 - x_o) = k_1m_1$ si perviene a $x_1 = x_o + km_1$. ■

■ **Esempio 13.1** Troviamo tutte le soluzioni intere dell'equazione $3x \equiv_9 6$. Osserviamo subito che $(3,9) = 3$ e $3|6$ quindi esiste almeno una soluzione. Dalla dimostrazione della Proposizione 13.2 sappiamo che una soluzione particolare è $x_o = ub_1$ dove $d = au + mv$ e $b = db_1$. Nel nostro caso si ha

$$3 = 3 \cdot 4 + 9(-1)\,, \quad 6 = 3 \cdot 2$$

quindi $u = 4$ e $b_1 = 2$. Segue che una soluzione particolare è $4 \cdot 2 = 8$. Tutte le soluzioni sono

$$Sol = \{8 + 3k \colon k \in \mathbb{Z}\} = \{2 + 3k \colon k \in \mathbb{Z}\}$$

■

Esercizio 13.7 Siano $m, n \in \mathbb{Z}, m, n \neq 0$. Dimostrare che le soluzioni dell'equazione

$$max \equiv_{mn} mb$$

coincidono con le soluzioni dell'equazione $ax \equiv_n b$. Per esempio, le soluzioni dell'equazione $2x \equiv_6 10$ sono le soluzioni dell'equazione $x \equiv_3 5$, cioè $Sol = \{5 + 3k \colon k \in \mathbb{Z}\}$.

Osservazione 13.4 In $\mathbb{Z}_m$ un equazione di primo grado in una variabile è del tipo $[a]_m[x]_m = [b]_m$ che si può riscrivere come $[ax]_m = [b]_m$, ovvero, $ax \equiv_m b$. Quindi l'equazione congruenzale $ax \equiv_m b$ è la naturale estensione delle equazioni di primo grado nell'insieme $\mathbb{Z}_m$ degli interi modulo m. Per esempio, se consideriamo l'equazione $[3]_9[x]_9 = [6]_9$ in $\mathbb{Z}_9$ le soluzioni sono

$$\{[2]_9, [5]_9, [8]_9\}$$

Come è facile immaginare un ruolo particolare spetta al caso in cui il modulo è un numero primo. Infatti si ha:

Proposizione 13.3 Sia p un numero primo positivo e sia $a \in \mathbb{Z}$ tale che $p \nmid a$. Allora l'equazione $ax \equiv_p b$ ammette sempre una soluzione per ogni $b \in \mathbb{Z}$. Inoltre in $\mathbb{Z}_p$ l'equazione $[a]_p[x]_p = [b]_p$ ammette un'unica soluzione.

Dimostrazione. Esercizio per il lettore. ■

13.3 Sistemi di congruenze

Oltre alle equazioni congruenzali si possono considerare i sistemi di equazioni congruenzali. Ad esempio si potrebbe considerare il sistema

$$\begin{cases} 2x \equiv_3 1 \\ 3x \equiv_5 1 \end{cases}$$

Le soluzioni della prima equazione sono $x = 2+3k$, $k \in \mathbb{Z}$. Sostituendo la generica soluzione nella seconda si ottiene $3(2+3k) = 6+9k \equiv_5 1$, ovvero $1+9k \equiv_5 1$ (dove, nell'ultimo passaggio si è usato che $1 \equiv_5 6$ e l'Osservazione 13.1). Segue che $9k \equiv_5 0$, cioè essendo $(9,5) = 1$, $k \equiv_5 0$. Abbiamo quindi ottenuto che k deve essere un multiplo di 5, cioè $k = 5\lambda$, $\lambda \in \mathbb{Z}$. In conclusione la soluzione x del sistema è del tipo $x = 2+3k = 2+3\cdot 5\lambda = 2+15\lambda$, $\lambda \in \mathbb{Z}$.

Vediamo un altro esempio. Si consideri il sistema

$$\begin{cases} 2x \equiv_3 2 \\ x \equiv_6 2 \end{cases}$$

Procedendo come nell'esempio precedente, la soluzione della seconda equazione è $x = 2+6k$, $k \in \mathbb{Z}$, che, sostituita nella seconda, diventa $4+12k \equiv_3 2$, ovvero $12k \equiv_3 -2 \equiv_3 1$ la quale produce un assurdo poiché $12k \equiv_3 0$ mentre $0 \not\equiv_3 1$. Quindi il sistema non ammette soluzioni intere.

Vi è una particolare circostanza nella quale un sistema congruenzale ammette sempre una soluzione come mostrato dal seguente

Teorema 13.2 — Teorema cinese del resto. Siano $m_1, \ldots, m_n \in \mathbb{Z}$, interi maggiori di 1 tali che $(m_i, m_j) = 1$ per ogni $i, j \in \{1, \ldots, n\}$, $i \neq j$ (diciamo che $m_1, \ldots, m_n$ sono a due a due primi fra loro). Allora il sistema

$$\begin{cases} x \equiv_{m_1} a_1 \\ \vdots \\ x \equiv_{m_n} a_n \end{cases}$$

ammette una soluzione per ogni n-upla $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Inoltre se x_o è una soluzione, l'insieme delle soluzione è

$$Sol = \{x_o + Mk \colon M = m_1 \cdots m_n,\ k \in \mathbb{Z}\}$$

Dimostrazione. Sia $M_i = m_1 \cdots \widehat{m_i} \cdots m_n$ dove con $\widehat{m_i}$ indichiamo che il modulo m_i viene omesso. Consideriamo per ogni $i \in \{1, \ldots, n\}$ l'equazione congruenzale

$$M_i x \equiv_{m_i} a_i \tag{13.3}$$

Poiché i moduli sono a due a due primi fra loro si ricava che $(M_i, m_i) = 1\,, \forall i \in \{1,\dots,n\}$[1]. Dalla Proposizione 13.2 la (13.3) ammette una soluzione che chiamiamo C_i, cioè $M_i C_i \equiv_{m_i} a_i$. Sia

$$C = \sum_{j=1}^{n} M_j C_j$$

allora, per ogni $i \in \{1,\dots,n\}$,

$$C = M_i C_i + \sum_{j \neq i} M_j C_j \equiv_{m_i} M_i C_i \equiv_{m_i} a_i$$

dove per la prima congruenza abbiamo usato che $m_i | M_j$ per ogni $j \neq i$, mentre nell'ultima che C_i è soluzione della (13.3). Abbiamo così dimostrato l'esistenza. Mostriamo adesso che l'insieme delle soluzioni è

$$Sol = \{x_o + Mk \colon M = m_1 \cdots m_n\,,\ k \in \mathbb{Z}\}$$

Se x_o è una soluzione allora

$$x_o + Mk \equiv_{m_i} x_o \equiv_{m_i} a_i\,, \quad \forall i \in \{1,\dots,n\}$$

Per dimostrare l'altra inclusione, sia x' un'altra soluzione. Allora $x' \equiv_{m_i} a_i\ \forall i \in \{1,\dots,n\}$ da cui $x' \equiv_{m_i} x_o\ \forall i \in \{1,\dots,n\}$. Segue che $m_i | (x' - x_o)\,, \forall i \in \{1,\dots,n\}$ e, dalla Proposizione 12.7, il prodotto dei moduli divide $x' - x_o$, cioè esiste $k \in \mathbb{Z}$ con $x' - x_o = kM$, ovvero $x' = x_o + kM$. ■

Esercizio 13.8 Dimostrare il viceversa del Teorema Cinese del Resto: se il sistema

$$\begin{cases} x \equiv_{m_1} a_1 \\ \vdots \\ x \equiv_{m_n} a_n \end{cases}$$

ammette una soluzione per ogni n-upla $(a_1,\dots,a_n) \in \mathbb{Z}^n$ allora $(m_i, m_j) = 1$ per ogni $i, j \in \{1,\dots,n\}$, $i \neq j$.

13.4 La funzione di Eulero

Consideriamo l'equazione $ax \equiv_m 1$ o l'equivalente equazione in $\mathbb{Z}_m$

$$[a]_m [x]_m = [1]_m \tag{13.4}$$

L'equazione (13.4) ammette una soluzione se e solo se $(a,m) = 1$, cioè una classe di resto $[a]_m$ in $\mathbb{Z}_m$ è invertibile se e solo se $(a,m) = 1$. Ad esempio, in $\mathbb{Z}_6$ la (13.4) ammette soluzioni solo se $[a]_6 = [1]_6$ o $[a]_6 = [5]_6$ che rappresentano le due unità di $\mathbb{Z}_6$ (gli elementi invertibili). Quindi il numero di elementi in $\mathbb{Z}_m$ invertibili è pari al numero di interi minori di m coprimi con m. Forti di questo fatto diamo la seguente

Definizione 13.2 La funzione $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ definita da

$$\varphi(m) = \begin{cases} 1 & \text{se } m = 1 \\ |\xi| & \text{se } m > 1 \end{cases}$$

dove $\xi = \{a \in \mathbb{Z} \colon 1 \leq a < m \quad \wedge \quad (a,m) = 1\}$, prende il nome di *funzione di Eulero*.

[1] Sia $d = (M_i, m_i)$ allora $d | M_i$ e $d | m_i$ e supponiamo che $d \neq 1$. Allora $d = p_1 \cdots p_s$ con $p_1,\dots,p_s$ primi. Segue che esiste un primo p che divide M_i e m_i. Poiché $p | M_i$ segue che p divide un m_j con $j \neq i$ contro l'ipotesi che $(m_i, m_j) = 1$.

■ **Esempio 13.2** Se $p > 1$ è primo, allora $\varphi(p) = p - 1$. In più

$$\varphi(p^n) = p^n - p^{n-1}, \quad \forall\, n \geq 1$$

Per verificare l'ultima relazione, si osservi che i numeri da 1 a p^n sono p^n e calcoliamo il numero di interi positivi minori di p^n che *non sono* coprimi con p^n. Se $1 \leq a \leq p^n$ con $(a, p^n) \neq 1 \quad \Rightarrow \quad p|a \quad \Rightarrow \quad a = pk$ con $1 \leq k \leq p^{n-1}$, quindi ci sono al massimo p^{n-1} numeri che non sono coprimi con p^n. Inoltre se $a = pk$, con $1 \leq k \leq p^{n-1}$, allora $(a, p^n) \neq 1$. Segue che i numeri che non sono coprimi con p^n sono esattamente p^{n-1}. ■

La prossima proposizione mostra una proprietà sorprendente della funzione di Eulero, cioè che gode di una certa proprietà moltiplicativa. Si osservi che non è affato comune incontrare funzioni che godono di proprietà simili.

Proposizione 13.4 Siano $m, n \in \mathbb{N}^*$ con $(n, m) = 1$. Allora

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Dimostrazione. Siano

$$\begin{array}{lll} U = \{u_1, \ldots, u_{\varphi(m)}\} & 1 \leq u_i < m & (u_i, m) = 1 \\ V = \{v_1, \ldots, v_{\varphi(n)}\} & 1 \leq v_j < n & (v_j, n) = 1 \\ W = \{w_1, \ldots, w_{\varphi(mn)}\} & 1 \leq w_k < mn & (w_k, mn) = 1 \end{array}$$

Allora

$$|U| = \varphi(m), \quad |V| = \varphi(n), \quad |W| = \varphi(mn)$$

Se esistesse una funzione biettiva da $U \times V$ in W allora

$$\varphi(mn) = |W| = |U \times V| = |U|\,|V| = \varphi(m)\varphi(n)$$

da cui la tesi. Costruiamo quindi tale biezione. Sia $(u, v) \in U \times V$ e si consideri il sistema

$$\begin{cases} x \equiv_m u \\ x \equiv_n v \end{cases} \tag{13.5}$$

Dal Teorema cinese del resto esiste un'unica soluzione w tale che $1 \leq w < mn$. Mostriamo che $(w, mn) = 1$. Infatti, $(w, m) = 1$ e $(w, n) = 1$ (esercizio!) quindi, dalla Proposizione 12.2, $(w, mn) = 1$. Definiamo quindi la funzione

$$\begin{array}{rccc} F: & U \times V & \to & W \\ & (u, v) & \mapsto & w \end{array}$$

dove w è l'unica soluzione di (13.5) tale che $1 \leq w < mn$. Mostriamo che F è biettiva. Se $w = F(u, v) = F(u', v')$ allora

$$\begin{cases} w \equiv_m u \\ w \equiv_n v \end{cases} \quad \wedge \quad \begin{cases} w \equiv_m u' \\ w \equiv_n v' \end{cases} \quad \Rightarrow \quad \begin{cases} u \equiv_m u' \\ v \equiv_n v' \end{cases} \quad \Rightarrow \quad \begin{cases} u = u' \\ v = v' \end{cases}$$

quindi F è iniettiva. Per la suriettività, sia $w \in W$. Dal Teorema della divisione euclidea esistono u e v tali che

$$\begin{cases} w = mq + u \\ w = nq' + v \end{cases} \quad \Rightarrow \quad \begin{cases} w \equiv_m u, & 0 \leq u < m \\ w \equiv_n v, & 0 \leq v < n \end{cases}$$

Se mostriamo che $u \in U$ e $v \in V$ allora $F(u, v) = w$. Mostriamo che $(u, m) = 1$. Poiché $w \in W$ si ha $1 = (w, mn) = wx + mny$ per qualche $x, y \in \mathbb{Z}$. Inoltre $w = u + mk$ per qualche $k \in \mathbb{Z}$. Segue che $1 = ux + m(kx + ny)$ da cui $1 = (u, m)$. Allo stesso modo si dimostra che $(v, n) = 1$. ■

Osservazione 13.5 Sia $m \in \mathbb{Z}$. Allora, dal Teorema fondamentale dell'aritmetica, esistono $p_1, \ldots, p_s$ primi e $r_1, \ldots r_s \in \mathbb{Z}$, tali che

$$m = p_1^{r_1} \cdots p_s^{r_s}$$

Segue che

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{r_1} \cdots p_s^{r_s}) = \varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s}) \\ &= (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_s^{r_s} - p_s^{r_s-1}) \\ &= p_1^{r_1}\left(1 - \frac{1}{p_1}\right) \cdots p_s^{r_s}\left(1 - \frac{1}{p_s}\right) \\ &= m \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).\end{aligned}$$

Ad esempio, per calcolare la funzione di Eulero di $120 = 2^3 \cdot 3 \cdot 5$ si trova

$$\varphi(120) = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 120\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = \frac{2^6 \cdot 3 \cdot 5}{2 \cdot 3 \cdot 5} = 2^5 = 32$$

La funzione di Eulero permette di generalizzare il Corollario 13.1 come enunciato nel seguente

Teorema 13.3 — Teorema di Eulero. Siano $a \geq 1$ e $m > 1$ due interi con $(m,a) = 1$. Allora

$$a^{\varphi(m)} \equiv_m 1$$

Dimostrazione. Sia

$$R = \{u_1, \ldots, u_{\varphi(m)}\} \quad 1 \leq u_i < m \quad (m, u_i) = 1$$

Per ogni u_i, dal Teorema della divisione Euclidea, $au_i = mq_i + r_i$ con $0 \leq r_i < m$. Inoltre, da $(m,a) = 1$ e $(m,u_i) = 1$ segue, dalla Proposizione 12.2, che $(m, au_i) = 1$ la quale implica che $(m,r_i) = 1$. Infatti, dal Teorema di Bézout, $1 = mx + (au_i)y$, $x, y \in \mathbb{Z}$, da cui $1 = m(x + q_i y) + r_i y$. Quindi $r_i \in R$ e possiamo definire la funzione

$$\begin{array}{rccc} \alpha: & R & \to & R \\ & u_i & \mapsto & r_i \end{array}$$

La funzione α è iniettiva. Infatti se $\alpha(u_i) = \alpha(u_j)$ allora $au_i \equiv_m r_i = \alpha(u_i) = \alpha(u_j) = r_j \equiv_m au_j$. Segue che

$$au_i \equiv_m au_j \quad \Rightarrow \quad m | a(u_i - u_j) \quad \Rightarrow \quad m | (u_i - u_j) \quad \Rightarrow \quad u_i \equiv_m u_j \quad \Rightarrow \quad u_i = u_j$$

dove nella seconda implicazione si è utilizzato che $(m,a) = 1$. Poiché R è un insieme finito segue, dalla Proposizione 4.4, che α è biettiva. In particolare

$$u_1 \cdots u_{\varphi(m)} = r_1 \cdots r_{\varphi(m)} \tag{13.6}$$

Consideriamo le congruenze

$$\begin{aligned} au_1 &\equiv_m r_1 \\ &\vdots \\ au_{\varphi(m)} &\equiv_m r_{\varphi(m)} \end{aligned}$$

moltiplicando le congruenze sopra e tenendo conto della (13.6), si ottiene

$$a^{\varphi(m)} u_1 \cdots u_{\varphi(m)} = a^{\varphi(m)} r_1 \cdots r_{\varphi(m)} \equiv_m r_1 \cdots r_{\varphi(m)}$$

Infine, essendo $r_1 \cdots r_{\varphi(m)}$ coprimo con m si conclude che $a^{\varphi(m)} \equiv_m 1$. ■

13.5 Il sistema RSA

Diamo un'applicazione di uso comune nei sistemi di crittografia del Teorema di Eulero. Il sistema di crittografia che descriviamo nel seguito è dovuto a *Ronald Rivest, Adi Shamir e Leonard Adleman* da cui il nome RSA.

Supponiamo che Sara (S) voglia inviare un messaggio sicuro a Roberto (R). Si procede nel modo seguente.

- R sceglie due numeri primi distinti p e q (generalmente molto grandi) e calcola $n = pq$. Poi sceglie un numero e tale che $(e, \varphi(n)) = 1$ e calcola d tale che $ed \equiv_{\varphi(n)} 1$ il quale esiste poiché $(e, \varphi(n)) = 1$.
- A questo punto R pubblica le chiavi n e e che sono visibili a tutti.
- Supponiamo adesso che S voglia spedire un un messaggio sicuro ad R e sia m il numero che rappresenta il messaggio. Allora S procede come segue:
  1. calcola il resto c della divisione di m^e per n, quindi $c \equiv_n m^e$
  2. S spedisce c.
- R riceve c e calcola il resto di c^d modulo n ottenendo m. Infatti

$$c \equiv_n m^e \quad \Rightarrow \quad c^d \equiv_n (m^e)^d = m^{ed} = m^{1+k\varphi(n)} = m\left[m^{\varphi(n)}\right]^k \equiv_n m$$

  dove nell'ultimo passaggio si è utilizzato il Teorema di Eulero.

A questo punto la domanda spontanea è: ma se uno conosce n e sa che è dato come prodotto di due primi, quanto ci vorrà per scoprire p e q. Se ci volesse poco il sistema descritto sopra non sarebbe affatto sicuro. Infatti noti p e q sarebbe semplicissimo calcolare $\varphi(n)$ e quindi d per decodificare il messaggio c. Il problema (o la fortuna) è che se n è molto grande decomporlo in prodotto di primi richiede moltissimo tempo anche per il più potente computer esistente (al momento!!!).

13.6 Rappresentazione b-adica dei numeri

Quando scriviamo il numero 3013 in base 10 intendiamo la seguente espressione:

$$3013 = 3 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10 + 3 \cdot 10^0$$

In questo esempio è chiaro che cifre uguali, ad esempio 3, rappresentano numeri differenti, a seconda della posizione che occupa all'interno del numero. Infatti, rappresenta il numero 3 se 3 è il coefficiente di 10^0 e il numero 3000 se è 3 moltiplica 10^3. Quindi è una notazione posizionale in base 10, in cui vengono utilizzate le dieci cifre da 0 a 9. Esaminiamo ulteriormente questo esempio, se dividiamo 3013 per 10 si ottiene

$$3013 = 10 \cdot 301 + 3$$

cioè il resto della divisione è 3. Quindi la cifra più a destra fornisce il resto della divisione per 10 del numero originale. Proseguendo, dividiamo nuovamente per 10 il quoziente trovato. Otteniamo

$$301 = 10 \cdot 30 + 1$$

Quindi la seconda cifra da destra, cioè 1, dà ancora una volta il resto di una divisione ed è determinata in modo univoco. In conclusione, le cifre che compaiono nella rappresentazione decimale del numero sono determinate in modo univoco da divisioni successive. La scelta del 10 come base notazionale è puramente convenzionale. Nel corso dei secoli culture diverse hanno utilizzato basi differenti nei loro sistemi numerici: i Babilonesi usavano la base 60, i Maya la base 20 e così via. I computer usano la base 2, cioè usano solo due cifre, 0 e 1, per rappresentare un numero. Infatti, nel sistema binario, cioè in base 2, ogni cifra occupa un bit di informazione: il simbolo 0

viene interpretato dal computer come comando *off* e il simbolo 1 come comando *on*. Quindi il ruolo svolto nei sistemi numerici dal numero 10 può essere assegnato a qualsiasi altro numero intero maggiore di 1. Ad esempio, se scegliamo 9 come base, il numero $3\cdot 9^3+0\cdot 9^2+1\cdot 9^1+3\cdot 9^0$ è rappresentato in base 10 come 2199. D'altra parte, il numero 3013 è rappresentato in base 9 da 4117, infatti

$$\begin{aligned} 3013 &= 9\cdot 334+7\\ 334 &= 9\cdot 37+1\\ 37 &= 9\cdot 4+1\\ 4 &= 9\cdot 0+4 \end{aligned}$$

Il risultato seguente garantisce la possibilità di contare in qualsiasi base.

Teorema 13.4 Sia b un numero intero maggiore o uguale a 2. Allora, per ogni $n\in\mathbb{N}$, esistono e sono unici un numero intero non negativo k e $k+1$ interi $a_0,a_1,\ldots,a_k$ con $0\le a_i<b$, per ogni $i=0,\ldots,k$, tali che:

$$n=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_2b^2+a_1b+a_0 \tag{13.7}$$

Dimostrazione. Dividendo n per b otteniamo

$$n=bq_0+a_0\,,\quad 0\le a_0<b$$

Ora, se $q_0\neq 0$, si divide di nuovo q_0 per b ottenendo

$$q_0=bq_1+a_1\,,\quad 0\le a_1<b$$

Andando avanti allo stesso modo si ottiene

$$\begin{aligned} q_1 &= bq_2+a_2 && 0\le a_2<b\\ &\vdots\\ q_{s-2} &= bq_{s-1}+a_{s-1} && 0\le a_{s-1}<b\\ q_{s-1} &= bq_s+a_s && 0\le a_s<b \end{aligned}$$

Siccome $n>q_0>q_1>\cdots>q_s\ge 0$ è una sequenza rigorosamente decrescente di interi non negativi, arriva necessariamente a zero. Sia k il primo numero intero tale che $q_k=0$. Riscriviamo l'elenco delle relazioni ottenuto sopra:

$$\begin{aligned} n &= bq_0+a_0 && 0\le a_0<b\\ q_0 &= bq_1+a_1 && 0\le a_1<b\\ q_1 &= bq_2+a_2 && 0\le a_2<b\\ &\vdots\\ q_{k-3} &= bq_{k-2}+a_{k-2} && 0\le a_{k-2}<b\\ q_{k-2} &= bq_{k-1}+a_{k-1} && 0\le a_{k-1}<b\\ q_{k-1} &= b0+a_k && 0\le a_k<b \end{aligned}$$

Procedendo all'indietro sostituendo il valore $q_{k-1}=a_k$, ottenuto da l'ultima equazione, nella precedente, troviamo

$$q_{k-2}=ba_k+a_{k-1}$$

Sostituendo nell'equazione ancora precedente troviamo

$$q_{k-3}=b(ba_k+a_{k-1})+a_{k-2}=b^2a_k+ba_{k-1}+a_{k-2}$$

Andando avanti così fino alla prima equazione si ottiene finalmente l'espressione (13.7). L'unicità di questa espressione è chiara, poiché le cifre a_i che compaiono in essa sono determinate in modo univoco come il resto delle divisioni successive. ■

13.7 Problemi proposti

Problema 13.1 Risolvere, se possibile, le seguenti equazioni congruenziali
$2x \equiv_{10} 4$
$16x \equiv_{18} 3$
$455x \equiv_{130} 325$
$285x \equiv_{165} 30$
$12x \equiv_{21} 7$
$12x \equiv_{84} 7$
$10x \equiv_{18} 14$.

Problema 13.2 Risolvere, se possibile, i seguenti sistemi di congruenze

$$\begin{cases} 3x \equiv_5 2 \\ 2x \equiv_6 14 \end{cases} \qquad \begin{cases} 6x \equiv_{14} 8 \\ 3x \equiv_5 4 \end{cases} \qquad \begin{cases} x \equiv_3 2 \\ x \equiv_7 3 \\ x \equiv_5 6 \end{cases}$$

Problema 13.3 Siano $a,b,n \in \mathbb{Z}$ con a ed n interi positivi e $(a,n) = 1$.

1. Mostrare che se $x \in \mathbb{Z}$ è la soluzione della congruenza:

   $$ax \equiv_n b$$

   allora x è anche soluzione della congruenza:

   $$rx \equiv_n -bq,$$

   dove $n = aq + r$ con $q, r \in \mathbb{Z}$ ed $0 < r < a$.
2. Mostrare che, se si può iterare la procedura descritta in (a), dopo un numero finito di passi la soluzione di $ax \equiv_n b$ è anche soluzione di una congruenza del tipo:

   $$x \equiv_n c,$$

   per un qualche $c \in \mathbb{Z}$.
3. Risolvere, con il metodo sopra descritto, la congruenza

   $$6x \equiv_{23} 7.$$

Problema 13.4 Determinare il più piccolo intero positivo k tale che il seguente sistema di congruenze ammetta soluzione

$$\begin{cases} x \equiv_2 1 \\ x \equiv_3 2 \\ x \equiv_6 k \end{cases}$$

Problema 13.5 Determinare tutte le soluzioni intere del seguente sistema di congruenze

$$\begin{cases} 40x \equiv_3 16 \\ 20x \equiv_7 25 \end{cases}$$

Problema 13.6 Si consideri il sistema di congruenze

$$\begin{cases} x \equiv_m a \\ x \equiv_n b \end{cases}$$

Trovare le condizioni affinché il sistema ammetta soluzione. (Suggerimento: il problema è equivalente all'esistenza di un intero t tale che $a - b + tm \equiv_n 0$. Quindi applicare la Proposizione 13.2).

Problema 13.7 Usando il principio di induzione mostrare che per ogni $n \geq 1$ vale la relazione:

$$10^n \equiv_9 1$$

Problema 13.8 Siano $a_0, \ldots, a_k$ le cifre in base 10 di un dato numero intero positivo a e sia

$$S = a_1 + a_2 + \cdots + a_k$$

Dimostrare che

1. $a \equiv_9 S$
2. $3|a \quad \Leftrightarrow \quad 3|S$

Problema 13.9 Dimostrare che un numero è divisibile per 11 se e solo se nella espressione in base 10 la somma delle cifre di posto dispari è congrua modulo 11 alla somma delle cifre di posto pari.

Problema 13.10 Determinare, calcolando la soluzione particolare come nella dimostrazione del Teorema Cinese del Resto, tutte le soluzioni intere del seguente sistema di congruenze

$$\begin{cases} x \equiv_7 2 \\ x \equiv_{23} 2^{22} \end{cases}$$

14. Algebra dei polinomi

In questo capitolo, poniamo alcune basi algebriche per uno studio sistematico dei polinomi. Iniziamo discutendo il concetto astratto di fattorizzazione in un dominio arbitrario. Nella sezione successiva ricordiamo l'algebra elementare associata ai polinomi in una variabile la quale fornisce un modello per l'algebra dei polinomi in più variabili. Dedichiamo una sezione separata ai polinomi omogenei.

14.1 Fattorizzazione in un dominio

Sia $(D,+,\cdot)$ un dominio di integrità. Ricordiamo che $a \in D$ *divide* $b \in D$, scriviamo $a|b$, se esiste $c \in D$ con $b = a \cdot c$. Se $b = a \cdot c$ diciamo altresì che b è un *multiplo* di a. Inoltre le *unità* sono gli elementi invertibili rispetto alla moltiplicazione. Ricordiamo inoltre la definizione di elemento irriducibile e elemento primo di un dominio.

Definizione 14.1 Sia $(D,+,\cdot)$ un dominio di integrità. Un elemento $p \in D$, $p \neq 0$, p non un'unità, si dice

(a) *irriducibile* se $p = a \cdot b$, $a,b \in D$, implica che a o b sono una unità.

(b) *primo* se vale la seguente implicazione

$$p|ab \quad \Leftrightarrow \quad p|a \quad \vee \quad p|b\,.$$

Come visto nella Proposizione 12.4 ogni primo è irriducibile mentre il viceversa, come mostrato nell'Esempio 12.3, non è vero.
La prossima definizione offre la classe di dominii dove vale il viceversa della Proposizione 12.4.

Definizione 14.2 Un dominio D si dice a *fattorizzazione unica* (UFD) se per ogni $a \in D$, $a \neq 0$, a non un'unità, valgono le seguenti

(a) esistono $a_1,\ldots,a_p \in D$ irriducibili con

$$a = a_1 \cdots a_p$$

(b) se $a = a_1 \cdots a_p = a'_1 \cdots a'_q$ allora $p = q$ e per ogni $i \in \{1,\ldots p\}$ esiste a'_j con $a_i = u a'_j$ e u unità.

Per esempio l'anello degli interi $\mathbb{Z}$, in virtù del Teorema 12.3, è UFD.
L'importanza dei domini a fattorizzazione unica risiede, come annunciato, nella seguente proposizione

Proposizione 14.1 Sia D un UFD. Allora ogni elemento irriducibile è primo.

Dimostrazione. Sia p irriducibile e supponiamo che $p|ab$. Allora $ab = pc$, cioè

$$pc_1 \cdots c_t = a_1 \cdots a_r b_1 \cdots b_s$$

dove abbiamo indicato con $a_1 \cdots a_r$, $b_1 \cdots b_s$ e $c_1 \cdots c_t$ le decomposizioni in irriducibili di a, b e c rispettivamente. Dall'unicità degli elementi irriducibili segue che o $p = a_i u$ o $p = b_j u$ per qualche i o j con u unità. Se $p = a_i u$ allora $a_i = pu^{-1}$ da cui $p|a$, mentre se $p = b_j u$ si ottiene che $p|b$. ■

Definizione 14.3 Sia D un dominio. Una *funzione grado* su D è una funzione $d : D \to \mathbb{N}$ tale che per ogni $a \in D$ e per ogni $b \in D \setminus \{0\}$, b non un'unità, si ha $d(a) < d(ab)$.

■ **Esempio 14.1** La funzione $d : \mathbb{Z} \to \mathbb{N}$ definita da $d(a) = |a|$ è una funzione grado. ■

Proposizione 14.2 Dia D un dominio con una funzione grado. Allora ogni elemento $a \in D$, $a \neq 0$, a non un'unità, si scrive come $a = a_1 \cdots a_p$ con a_i irriducibili.

Dimostrazione. Se a è irriducibile, abbiamo finito. Altrimenti scriviamo $a = bc$ dove b, c non sono unità, quindi $d(b) < d(bc) = d(a)$ e $d(c) < d(bc) = d(a)$. Ora ripetiamo questo processo a b e c; se uno dei due non è irriducibile lo fattorizziamo in fattori propri (non unità) sui quali d assume valori strettamente inferiori. Il processo può essere ripetuto al massimo un numero finito di volte, poiché in ogni fase la funzione grado diminuisce di almeno 1. ■

Proposizione 14.3 Dia D un dominio e sia $a \neq 0$, a non unità. Siano $a = a_1 \cdots a_p = a'_1 \cdots a'_q$ due fattorizzazioni di a in primi. Allora $p = q$ e per ogni $i \in \{1, \dots p\}$ esiste a'_j con $a_i = u a'_j$ e u unità.

Dimostrazione. Si può ripetere la stessa dimostrazione fatta per dimostrare l'unicità nel Teorema Fondamentale dell'Aritmetica 12.3 ricordando che in un qualunque dominio un primo è irriducibile. ■

Combinando gli ultimi due risultati, otteniamo la seguente condizione sufficiente affinché un dominio sia un UFD.

Teorema 14.1 Dia D un dominio con una funzione grado. Supponiamo che ogni elemento irriducibile sia primo. Allora D è un UFD. In particolare ogni elemento $a \in D$, $a \neq 0$, a non un'unità, si scrive come

$$a = u a_1^{r_1} \cdots a_s^{r_s}, \quad r_i \in \mathbb{N}^*$$

con a_i irriducibili distinti e u unità.

14.2 Polinomi in una variabile

Iniziamo con la seguente definizione

Definizione 14.4 Sia D un dominio. Un *polinomio* a coefficienti in D è una funzione

$$\begin{array}{rccl} P: & D & \to & D \\ & x & \mapsto & a_0 + a_1 x + \cdots + a_d x^d, \quad a_i \in D, d \in \mathbb{N} \end{array}$$

Solitamente indichiamo i polinomi con $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ e chiamiamo il numero naturale d il *grado* del polinomio e lo indichiamo con grado(P). Un polinomio di grado $d = 0$ è una funzione costante. I singoli addendi $a_j x^j$ sono chiamati *monomi*. Dati due polinomi

$$P(x) = a_0 + a_1 x + \cdots + a_d x^d, \quad Q(x) = b_0 + b_1 x + \cdots + b_d x^s$$

definiamo il polinomio somma e il polinomio prodotto nel modo seguente

$$(P+Q)(x) := P(x)+Q(x) = a_0 + a_1x + \cdots + a_dx^d + b_0 + b_1x + \cdots + b_dx^s$$

$$(PQ)(x) := P(x)Q(x) = (a_0 + a_1x + \cdots + a_dx^d)(b_0 + b_1x + \cdots + b_dx^s)$$

Esercizio 14.1 Sia $D[x]$ l'insieme di tutti i polinomi in una variabile. Dimostrare che $(D[x],+,\cdot)$ è un dominio dove

$$\begin{array}{rccc} 0: & D & \to & D \\ & x & \mapsto & 0 \end{array}$$

$$\begin{array}{rccc} 1: & D & \to & D \\ & x & \mapsto & 1 \end{array}$$

e le unità sono i polinomi costanti

$$\begin{array}{rccc} c: & D & \to & D \\ & x & \mapsto & c \end{array}$$

con $c \in D$ unità.

Esercizio 14.2 Dimostrare che se $P(x)$ e $Q(x)$ sono due polinomio non nulli allora

$$\text{grado}(P+Q) \leq \max\{\text{grado}(P), \text{grado}(Q)\}, \quad \text{grado}(PQ) = \text{grado}(P) + \text{grado}(Q).$$

Dedurre che, nel caso D sia un campo, il grado di un polinomio definisce una funzione grado su $D[x]$.

Si osservi che nel dominio $D[x]$ la nozione di irriducibile dipende dal dominio. Per esempio il polinomio $P(x) = x^2+1$ è irriducibile in $\mathbb{R}[x]$. Infatti se $x^2+1 = (ax+b)(cx+d) = acx^2 + (ad+bc)x + bd$ allora

$$\begin{cases} ac = 1 \\ bd = 1 \\ ad + bc = 0 \end{cases}$$

che conduce facilmente ad un assurdo (esercizio). Mentre in $\mathbb{C}[x]$ il polinomio x^2+1 si decompone come $x^2+1 = (x-i)(x+i)$.

Proposizione 14.4 Sia D un dominio, $P(x) = \sum_{i=0}^{d} a_i x^i \in D[x]$ un polinomio e sia $c \in D$. Allora esiste un polinomio $Q(x) \in D[x]$ di grado $d-1$ e un elemento $r \in D$ tali che

$$P(x) = (x-c)Q(x) + r$$

Dimostrazione. Basta mostrare che ciascun monomio x^i, $i \geq 1$, si scrive come

$$x^i = (x-c)Q_i(x) + r_i$$

con $Q_i(x)$ polinomio di grado $i-1$ e $r_i \in D$. Infatti, se così fosse si avrebbe

$$\begin{aligned} P(x) &= \sum_{i=0}^{d} a_i x^i = a_0 + \sum_{i=1}^{d} a_i[(x-c)Q_i(x) + r_i] \\ &= (x-c)\left[\sum_{i=1}^{d} a_i Q_i(x)\right] + a_0 + \sum_{i=1}^{d} a_i r_i \\ &= (x-c)Q(x) + r\,. \end{aligned}$$

Adesso, per ogni $i \geq 1$,

$$x^i = (x-c)[x^{i-1} + x^{i-2}c + \cdots + xc^{i-2} + c^{i-1}] + c^i = (x-c)Q_i(x) + r_i\,.$$

■

Definizione 14.5 Un elemento $c \in D$ è una *radice* (zero) di un polinomio $P(x) \in D[x]$ se $P(c) = 0$.

Si ottiene immediatamente il famoso teorema

Teorema 14.2 — Teorema di Ruffini. Sia c una radice di un polinomio $P(x) \in D[x]$. Allora $(x-c)$ è un divisore di $P(x)$.

Dimostrazione. Dalla Proposizione 14.4 $P(x) = (x-c)Q(x) + r$ ma, essendo c una radice, si trova $0 = P(c) = (c-c)Q(x) + r = r$. Segue che $P(x) = (x-c)Q(x)$ da cui $(x-c)$ divide $P(x)$. ■

Definizione 14.6 Sia c una radice di un polinomio $P(x) \in D[x]$. Diciamo che c ha *molteplicità* m se $(x-c)^m | P(x)$ ma $(x-c)^{m+1} \nmid P(x)$.

▪ **Esempio 14.2** Per esempio il polinomio $P(x) = x^3 - 2x^2 + x \in \mathbb{Z}[x]$ ha la radice $c = 1$ con molteplicità 2. Infatti, $P(x) = x^3 - 2x^2 + x = (x-1)^2 x$ da cui $(x-1)^2 | P(x)$ ma è facile verificare che $(x-1)^3 \nmid P(x)$. ▪

Proposizione 14.5 Un polinomio non-costante $P(x)$ di grado d su un dominio D ha al massimo d radici distinte.

Dimostrazione. Supponiamo per assurdo che $c_1, \ldots, c_d, c_{d+1}$ siano $d+1$ radici distinte di un polinomio $P(x)$ di grado d. Allora $P(x) = (x-c_1)G_1(x)$. Adesso $0 = P(c_2) = (c_2 - c_1)G_1(c_2)$ ed essendo $c_1 \neq c_2$ segue che $G_1(c_2) = 0$. Quindi $P(x) = (x-c_1)(x-c_2)G_2(x)$ e così via sino a

$$P(x) = (x-c_1)(x-c_2)\cdots(x-c_d)c\,, \quad c \in D, c \neq 0\,.$$

Si trova, poiché D è un dominio, $0 = P(c_{d+1}) = (c_{d+1} - c_1)\cdots(c_{d+1} - c_d)c \neq 0$ da cui l'assurdo. ■

! Se D non è un dominio la Proposizione 14.5 non è necessariamente vera. Per esempio in $\mathbb{Z}_9$ il polinomio $P(x) = x^2$ ha 3 radici: $[0], [3], [6]$.

14.3 Problemi proposti

Problema 14.1 Mostra che le unità nel dominio$D[x]$ sono precisamente i polinomi costanti con valore un'unità in D.

Problema 14.2 Trovare gli zeri del polinomio $P(x) = 2x(x-1)$ in $\mathbb{Z}_4$.

14.4 Polinomi in una variabile in un campo

In questa sezione supponiamo che D sia un campo $\mathbb{K}$. Mostriamo subito che con tale ipotesi vale il viceversa del Teorema di Ruffini

Proposizione 14.6 Sia $\mathbb{K}$ un campo e sia $P(x) \in \mathbb{K}[x]$. Allora $P(x)$ ha una radice in $\mathbb{K}$ se e solo se $P(x)$ è divisibile per un polinomio di grado 1.

Dimostrazione. Se c è una radice allora $(x-c)|P(x)$ per il Teorema di Ruffini. Viceversa se $(ax+b)|P(x)$, $a \neq 0$, allora $P(x) = Q(x)(ax+b) = Q(x)(x+ba^{-1})a$ da cui segue che $x = -ba^{-1}$ è una radice. ■

Sempre nel caso di polinomi a coefficienti su un campo vale l'analogo del Teorema della divisione Euclidea, più precisamente si ha il seguente risultato

Teorema 14.3 Sia $\mathbb{K}$ un campo e siano $P(x), P'(x) \in \mathbb{K}[x]$ con grado$(P) \geq 1$ e $P'(x) \neq 0$. Allora esistono due polinomi $Q(x), R(x) \in \mathbb{K}[x]$ tale

$$P(x) = P'(x)Q(x) + R(x)$$

con grado$(R) <$ grado(P') o $R(x) = 0$ se grado$(P') = 0$. Inoltre $Q(x)$ e $R(x)$ sono unici.

Dimostrazione. Dimostriamo prima l'esistenza.
Se grado$(P) <$ grado(P') allora $P(x) = P'(x)0 + P(x)$.
Se grado$(P) = d \geq$ grado(P') procediamo per induzione su d.
Caso $d = 1$. Sia $P(x) = ax+b$, $a,b \in \mathbb{K}$, $a \neq 0$. Sia $P'(x) = a'x+b'$, $a',b' \in \mathbb{K}$. Si presentano due casi
$a' = 0$ - Allora $P'(x) = b' \neq 0$ e

$$P(x) = ax+b = b'\left[\frac{a}{b'}x + \frac{b}{b'}\right] + 0\,.$$

$a' \neq 0$ - In questo caso

$$P(x) - \frac{a}{a'}P'(x) = ax+b-ax-\frac{ab'}{a'} = \frac{ba'-ab'}{a'}$$

Segue che

$$P(x) = P'(x)\frac{a}{a'} + \frac{ba'-ab'}{a'} = P'(x)Q(x) + R(x)\,.$$

Caso $d > 1$. Supponiamo la proposizione vera per ogni grado $k \in \{1,\ldots,d-1\}$ di $P(x)$ e dimostriamo che è vera per d (induzione forte). Siano

$$P(x) = a_0 + \cdots + a_d x^d\,, \quad P'(x) = a'_0 + \cdots + a'_{d'}x^{d'}\,, \quad a_d, a'_{d'} \neq 0,\ d \geq d'$$

Allora poniamo

$$R(x) = P(x) - \frac{a_d}{a_{d'}}x^{d-d'}P'(x)\,,$$

dove, avendo eliminato il monomio $a_d x^d$ in $P(x)$, risulta che grado$(R) <$ grado(P). Se grado$(R) <$ grado(P') abbiamo finito. Se grado$(R) \geq$ grado(P') si usa l'ipotesi induttiva su $R(x)$ e si trova che $R(x) = P'(x)Q(x) + R'(x)$ con grado$(R') <$ grado(P'). Segue che

$$P(x) = P'(x)\left(\frac{a_d}{a_{d'}}x^{d-d'} + Q(x)\right) + R'(x)\,.$$

Dimostriamo adesso l'unicità. Supponiamo che

$$P(x)=P'(x)Q(x)+R(x) \quad \wedge \quad P(x)=P'(x)\bar{Q}(x)+\bar{R}(x), \quad \text{con} \quad \text{grado}(R),\text{grado}(\bar{R})<\text{grado}(P')$$

Se per assurdo $R(x)\neq\bar{R}(x)$ allora

$$P'(x)(Q(x)-\bar{Q}(x))=\bar{R}(x)-R(x)\neq 0$$

da cui $Q(x)-\bar{Q}(x)\neq 0$. Segue, utilizzando l'Esercizio 14.2, che

$$\text{grado}(\bar{R}-R)=\text{grado}(Q-\bar{Q})+\text{grado}(P')\geq\text{grado}(P')$$

contro l'ipotesi che $\text{grado}(\bar{R}-R)<\text{grado}(P')$. ■

Il Teorema 14.3 ci permette di definire per due polinomi $P(x),P'(x)\in\mathbb{K}[x]$ il M.C.D., cioè un polinomio $M(x)$ tale che $M(x)$ divide $P(x)$, $M(x)$ divide $P'(x)$ e se un altro polinomio divide entrambi allora divide $M(x)$. Infatti tale polinomio $M(x)$ si ottiene utilizzando lo stesso algoritmo utilizzato per determinare il M.C.D. di due interi come mostrato nell'Osservazione 12.3. Inoltre, sempre da tale procedimento, si ottiene che $M(x)=P(x)Q(x)+P'(x)Q'(x)$ per due opportuni, non unici, polinomi $Q(x)$ e $Q'(x)$. Si osservi che, essendo in un campo gli elementi diversi da zero invertibili, il M.C.D. è unico a meno di una costante moltiplicativa diversa da zero.

▪ **Esempio 14.3** Si considerino in $\mathbb{R}[x]$ i polinomi

$$P(x)=x^3-x^2+x-1, \quad P'(x)=x^2-1$$

allora

$$P(x)=P'(x)(x-1)+2x-2$$

e

$$P'(x)=(2x-2)(x/2+1/2)+0$$

quindi il M.C.D (l'ultimo resto diverso da 0) è $M(x)=2x-2$ il quale, risalendo nelle divisioni, si può scrivere come

$$2x-2=P(x)+P'(x)(-x+1).$$

Come osservato in precedenza, si noti che si poteva prendere come M.C.D. anche $(x-1)$. ▪

Siamo nella giusta posizione per enunciare un importante risultato sulla teoria dei polinomi in una variabile.

Teorema 14.4 Sia $\mathbb{K}$ un campo. Allora l'anello dei polinomi $\mathbb{K}[x]$ è UFD. In particolare, ogni polinomio non costante $P(x)\in\mathbb{K}[x]$ si scrive in modo unico come

$$P(x)=uQ_1(x)^{r_1}\cdots Q_s(x)^{r_s}, \quad r_i\in\mathbb{N}^* \tag{14.1}$$

con $Q_i(x)$ polinomi irriducibili distinti e $u\in\mathbb{K},u\neq 0$.

Dimostrazione. Osserviamo subito che la funzione $d:\mathbb{K}[x]\to\mathbb{N}$, $d(P)=\text{grado}(P)$, è una funzione grado (si veda l'Esercizio 14.2). In virtù del Teorema 14.1 basta mostrare che ogni polinomio irriducibile è primo. Sia quindi $P(x)$ un polinomio irriducibile e dimostriamo che se $P(x)|Q(x)H(x)$ allora $P(x)|Q(x)$ o $P(x)|H(x)$. Sia $M(x)$ il M.C.D. di $P(x)$ e $Q(x)$. Si presentano due casi

(i) $M(x)$ non è costante. Allora $M(x)|P(x)$, cioè $P(x)=M(x)P'(x)$. Ma essendo $P(x)$ irriducibile ed essendo le uniche unità di $\mathbb{K}[x]$ gli elementi di $\mathbb{K}$ diversi da zero, segue che $P(x)=M(x)\lambda$ con $\lambda\in\mathbb{K}$, $\lambda\neq 0$. Ma $M(x)|Q(x)$ da cui $P(x)=M(x)\lambda|Q(x)$.

(i) $M(x)$ è costante. Possiamo assumere che $M(x) = 1 \in \mathbb{K}[x]$. Quindi esistono $A(x), B(x) \in \mathbb{K}[x]$ tali che

$$1 = A(x)P(x) + B(x)Q(x)$$

che moltiplicata per $H(x)$ restituisce

$$H(x) = A(x)P(x)H(x) + B(x)Q(x)H(x)$$

da cui segue che $P(x)|H(x)$.

■

Il Teorema 14.4 garantisce che un polinomio $P(x) \in \mathbb{K}[x]$ si possa decomporre come prodotto di polinomi irriducibili. Per esempio il polinomio $P(x) = x^3 - x^2 + x - 1 \in \mathbb{R}[x]$ si scrive come $P(x) = (x^2+1)(x-1)$. Il problema a questo punto è però capire quando un polinomio è irriducibile. I polinomi di grado 1 sono sempre irriducibili. Per i polinomi di grado 2 o 3 vale la seguente proposizione.

Proposizione 14.7 Sia $\mathbb{K}$ un campo e sia $P(x) \in \mathbb{K}[x]$ un polinomio con grado$(P) \in \{2,3\}$. Allora $P(x)$ è irriducibile se e solo se non ha radici in $\mathbb{K}$.

Dimostrazione. Se $P(x)$ è irriducibile allora non esiste un polinomio di grado 1 che lo divide, altrimenti si avrebbe $P(x) = (ax+b)Q(x)$ con $Q(x)$ polinomio di grado 1 o 2 e $P(x)$ sarebbe riducibile, quindi per la Proposizione 14.6 non esistono radici di $P(x)$. Viceversa, supponiamo che $P(x)$ non abbia radici ma che per assurdo sia riducibile, cioè $P(x) = A(x)B(x)$ con $A(x)$ e $B(x)$ polinomi non costanti. Allora grado(P) = grado(A) + grado(B). Segue, da grado$(P) \in \{2,3\}$, che almeno uno tra $A(x)$ e $B(x)$ ha grado 1 e sempre dalla Proposizione 14.6 il polinomio $P(x)$ avrebbe una radice contro l'ipotesi. ■

! Se il polinomio ha grado 4 la proposizione precedente non si applica. Per esempio il polinomio $x^4 + 3x^2 + 2 \in \mathbb{R}[x]$ non ha radici reali ma $x^4 + 3x^2 + 2 = (x^2+1)(x^2+2)$, quindi è riducibile. Un altro esempio è dato dal polinomio $P(x) = x^4 - 4$ visto come polinomio in $\mathbb{Q}[x]$. In questo caso $P(x)$ non ha radici in $\mathbb{Q}$ ma $x^4 - 4 = (x^2-2)(x^2+2)$.

La Proposizione 14.5 pone un limite superiore al numero di radici di un polinomio ma non dice nulla sull'esistenza delle stesse. Per esempio, il polinomio $P(x) = 2x - 1 \in \mathbb{Z}[x]$ non ammette alcuna radice. Anche quando D è un campo l'esistenza delle radici non è garantita. Per esempio, il polinomio $P(x) = x^2 + 1 \in \mathbb{R}[x]$ non ammette radici. Infatti una tale radice sarebbe un numero reale il cui quadrato è -1, assurdo. Vi è un caso in cui invece l'esistenza delle radici è assicurata. Tale risultato è così importante da meritare il nome di *Teorema Fondamentale dell'Algebra* il cui enunciato è il seguente.

Teorema 14.5 — Teorema Fondamentale dell'Algebra. Ogni polinomio $P(x) \in \mathbb{C}[x]$ ammette almeno una radice.

Dimostrazione. La dimostrazione non sarà data durante il corso di Algebra 1 poiché tecnicamente difficile con argomenti puramente algebrici. È bene osservare che esistono numerosissime dimostrazioni di tale risultato molte delle quali provenienti da branche differenti della matematica. La prima dimostrazione corretta fu data da Gauss nella sua tesi di laurea. ■

Sia $P(x)$ un polinomio in $\mathbb{C}[x]$ di grado d. Applicando il Teorema Fondamentale d volte si può scrivere

$$P(x) = c(x-c_1)(x-c_2)\cdots(x-c_d) = c(x-\gamma_1)^{r_1}\cdots(x-\gamma_s)^{r_s}, \quad c \in \mathbb{C} \tag{14.2}$$

dove $\gamma_1, \ldots, \gamma_s$ sono le radici distinte del polinomio $P(x)$ e $r_1, \ldots, r_s$ le corrispondenti molteplicità, quindi $r_1 + \cdots + r_s = d$.

Per quanto riguarda i polinomi in $\mathbb{R}[x]$ abbiamo visto che ci sono polinomi di grado 2 irriducibili. Ci si può chiedere se tutti i polinomi di grado maggiore di 2 siano riducibili. Per rispondere osserviamo subito che se un polinomio a coefficienti reali ammette una radice complessa α, cioè se per un polinomio $P(x) \in \mathbb{R}[x]$ esiste un $\alpha \in \mathbb{C}$ con $P(\alpha) = 0$, allora $P(\bar{\alpha}) = 0$ dove con $\bar{\alpha}$ abbiamo indicato il coniugato di α. Infatti $P(\bar{\alpha}) = \overline{P(\alpha)} = 0$. Sia adesso $P(x) \in \mathbb{R}[x]$ un polinomio con grado$(P) > 2$. Sia α una radice complessa di $P(x)$, allora

$$(x-\alpha)|P(x)\,, \quad (x-\bar{\alpha})|P(x)$$

Segue che, essendo i polinomi di primo grado irriducibili (primi),

$$(x-\alpha)(x-\bar{\alpha})|P(x)$$

cioè

$$(x^2-(\alpha+\bar{\alpha})x+|\alpha|^2)|P(x)$$

Ma $x^2-(\alpha+\bar{\alpha})x+|\alpha|^2$ è un polinomio a coefficienti reali, quindi in $\mathbb{R}[x]$ vale la scomposizione

$$P(x) = (x^2-(\alpha+\bar{\alpha})x+|\alpha|^2)Q(x)\,, \tag{14.3}$$

con $Q(x) \in \mathbb{R}[x]$ polinomio con grado$(Q) =$ grado$(P) - 2 > 1$, quindi non costante. Conseguentemente vale la seguente

Proposizione 14.8 Sia $P(x)$ un polinomio di grado maggiore di 2 a coefficienti reali, allora $P(x)$ è riducibile.

Se $P(x) \in \mathbb{R}[x]$ ha grado 3 si ottiene dalla (14.3)

$$P(x) = (x^2-(\alpha+\bar{\alpha})x+|\alpha|^2)(ax+b)\,, \quad a,b \in \mathbb{R}$$

Segue che $(ax+b)|P(x)$ da cui $-(b/a)$ è una radice di $P(x)$. In altri termini vale la seguente

Proposizione 14.9 Sia $P(x)$ un polinomio di grado 3 a coefficienti reali, allora esiste almeno una radice reale di $P(x)$.

Il ragionamento si può estendere facilmente ad un polinomio $P(x) \in \mathbb{R}[x]$ di qualsiasi grado dispari maggiore di 3 e concludere che tutti i polinomi a coefficienti reali di grado dispari hanno una radice reale.

! Per i polinomi in un campo che non sia $\mathbb{R}$ la proprietà sul grado dei polinomi irriducibili non è necessariamente vera. A titolo di esempio, il polinomio $P(x) = x^4 - 2 \in \mathbb{Q}[x]$ ha grado 4 ma non è riducibile in $\mathbb{Q}[x]$. Infatti, $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$ in $\mathbb{R}[x]$ ma i due fattori non sono polinomi di $\mathbb{Q}[x]$.

■ **Esempio 14.4** Sia $P(x) = x^4 + 1 \in \mathbb{R}[x]$. Il polinomio $P(x)$ non ha radici reali ma, dal Teorema Fondamentale dell'Algebra, ha radici complesse, infatti esistono, in $\mathbb{C}$, 4 radici quarte del numero -1:

$$\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\,, \qquad \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\,, \qquad -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\,, \qquad -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

dalle quali, seguendo la (14.3), si ottiene

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

■

14.5 Problemi proposti

Problema 14.3 Un polinomio complesso $P(x)$ si dice reale quando esiste un polinomio $Q(x)$ con coefficienti reali e uno scalare complesso α per il quale $P(x) = \alpha Q(x)$. In particolare, qualsiasi polinomio $P(x)$ con coefficienti reali è reale. Attenzione: secondo questa definizione il polinomio complesso ix è reale. Una condizione equivalente procede attraverso l'idea di *coniugazione complessa*. Il complesso coniugato di $P(x)$ è definito come il polinomio $\bar{P}(x)$ ottenuto da $P(x)$ sostituendo tutti i suoi coefficienti con i loro complessi coniugati. Per esempio, il complesso coniugato di $x+iy$ è $x-iy$.

- Verificare che $P(x)$ è reale se e solo se esiste un numero complesso α tale che $P(x) = \alpha\bar{P}(x)$
- Dimostrare che $P(x)$ è irriducibile se e solo se $\bar{P}(x)$ è irriducibile; dedurre che se $P(x)$ ha componenti irriducibili $P_1(x), \ldots, P_s(x)$ allora $\bar{P}(x)$ ha componenti $\bar{P}_1(x), \ldots, \bar{P}_s(x)$ con le stesse molteplicità.

Problema 14.4 Trova gli zeri del polinomio complesso $P(x) = x^4 + 81$. Quindi scrivere $P(x)$ come prodotto di fattori lineari complessi e come prodotto di fattori quadratici reali.

Problema 14.5 Mostra che $x = i - 1$ è uno zero del polinomio complesso dato da $P(x) = x^4 + 2x^3 + 3x^2 + 2x + 2$. Quindi fattorizzare $P(x)$ in $\mathbb{C}$.

14.6 Polinomi in più variabili

In questa sezione diamo una breve introduzione ai polinomi in più variabili senza dimostrare proprietà generali.

Definizione 14.7 Sia D un dominio. Un *polinomio* a coefficienti in D in due variabili è una funzione

$$\begin{array}{rccl} P: & D\times D & \to & D \\ & (x,y) & \mapsto & \displaystyle\sum_{i,j} a_{ij}x^i y^j, \quad a_{ij}\in D \end{array}$$

Indichiamo un polinomio in due variabili con $P(x,y) = \sum_{i,j} a_{ij}x^i y^j$ e denotiamo l'insieme dei polinomi in due variabili in un dominio D con $D[x,y]$.

■ **Esempio 14.5** La funzione $(x,y) \mapsto x^2y + xy - y^2$ definisce il polinomio a coefficienti in $\mathbb{Z}$ $P(x,y) = x^2y + xy - y^2$. ■

La somma e il prodotto di polinomi in due variabili si definisce in analogia con quanto visto per i polinomi in una variabile. Anche in questo caso $(D[x,y], \cdot, +)$ è un dominio di integrità le cui unità sono le unità del dominio D.

Dato un polinomio $P(x,y) = \sum_{i,j} a_{ij}x^i y^j$ ciascun addendo costituisce un monomio e il grado del monomio è dato dalla somma dei corrispondenti esponenti di x e di y. Per esempio x^3y^2 è un monomio di grado 5. Il grado del polinomio è definito come il massimo dei gradi dei singoli monomi. Quindi per il polinomio $P(x,y) = x^2 - x^3y - x^3y^2 + 3x^2x^2$ il grado è 5.

Esercizio 14.3 Dimostrare che il grado gode della proprietà additiva, cioè se $P(x,y) \neq 0$ e $Q(x,y) \neq 0$ allora

$$\text{grado}(P(x,y)Q(x,y)) = \text{grado}(P(x,y)) + \text{grado}(Q(x,y)).$$

Generalizzando si può dare la seguente

Definizione 14.8 Sia D un dominio. Un *polinomio* a coefficienti in D in n variabili è una funzione

$$\begin{array}{rccl} P: & D^n & \to & D \\ & (x_1,\ldots,x_n) & \mapsto & \displaystyle\sum_{i_1\ldots i_n} a_{i_1\ldots i_n} {x_1}^{i_1}\cdots {x_n}^{i_n}, \quad a_{i_1\ldots i_n}\in D \end{array}$$

Si possono estendere anche in questo caso le operazioni e la nozione di grado in modo del tutto analogo. Costruendo in tal modo il dominio $D[x_1,\dots,x_n]$.

■ **Esempio 14.6** Il polinomio $P(x,y,z) = xy^2 - xyz + xy^2z^3 - x^2 + 2xy - x$ è un polinomio in tre variabili. ■

Se $\mathbb{K}$ è un campo anche per il dominio $\mathbb{K}[x_1,\dots,x_n]$ dei polinomi in più variabili a coefficienti in un campo vale il Teorema 14.4, cioè il dominio $\mathbb{K}[x_1,\dots,x_n]$ è UFD. La dimostrazione è sulla stessa linea di quella per i polinomi in una variabile ma in questo caso la dimostrazione che ogni polinomio irriducibile è primo risulta più complessa e si opera per induzione sul numero di variabili. In particolare, ogni polinomio non costante $P(x_1,\dots,x_n) \in \mathbb{K}[x_1,\dots,x_n]$ si scrive in modo unico come

$$P(x_1,\dots,x_n) = uQ_1(x_1,\dots,x_n)^{r_1}\cdots Q_s(x_1,\dots,x_n)^{r_s}, \quad r_i \in \mathbb{N}^* \tag{14.4}$$

con $Q_i(x_1,\dots,x_n)$ polinomi irriducibili distinti e $u \in \mathbb{K}, u \neq 0$.

14.7 Polinomi omogenei

Un ruolo importante tra i polinomi in più variabili è occupato dai polinomi *omogenei* la cui definizione è la seguente.

Definizione 14.9 Un polinomio $F \in D[x_1,\dots,x_n]$ è *omogeneo* (*forma*) se tutti i monomi che lo compongono hanno lo stesso grado d.

■ **Esempio 14.7** Se $d = 1$ si ottengono le *forme lineari* che sono del tipo $a_1x_1 + a_2x_2 + \cdots + a_nx_n$. Se $d = 2$ le *forme quadratiche* le quali hanno l'espressione, se $n = 2$,

$$a_{11}x^2 + a_{12}xy + a_{22}y^2.$$

Se $d = 3$ si chiamano *forme cubiche* la cui espressione, sempre per $n = 2$, è

$$a_{11}x^3 + a_{12}x^2y + a_{21}xy^2 + a_{22}y^3.$$

■

Si osservi che un polinomio $P(x_1,\dots,x_n)$ di grado d che non sia necessariamente una forma si scrive comunque come somma di forme

$$P(x_1,\dots,x_n) = F_\ell(x_1,\dots,x_n) + \cdots + F_d(x_1,\dots,x_n), \quad \ell \leq d$$

dove $F_\ell,\dots,F_d$ sono forme di grado $\ell,\dots,d$ rispettivamente.

■ **Esempio 14.8** Il polinomio $P(x,y,z) = xy^2 - xyz + xy^2z^3 - x^2 + 2xy - x$ si scrive come

$$P(x,y,z) = (-x) + (2xy - x^2) + (xy^2 - xyz) + (xy^2z^3) = F_1(x,y,z) + F_2(x,y,z) + F_3(x,y,z) + F_6(x,y,z).$$

■

Vi è un utile caratterizzazione delle forme

Proposizione 14.10 Sia $F(x_1,\dots,x_n)$ un polinomio in $D[x_1,\dots,x_n]$, con D dominio infinito. Allora F è una forma di grado d se e solo se per ogni $t \in D$

$$F(tx_1,\dots,tx_n) = t^dF(x_1,\dots,x_n).$$

Dimostrazione. Se F è omogeneo allora

$$F(x_1,\dots,x_n) = \sum_{i_1\dots i_n} a_{i_1\dots i_n} x_1{}^{i_1}\cdots x_n{}^{i_n}, \quad i_1 + \cdots + i_n = d$$

Segue che, se $t \in D$,

$$F(tx_1,\ldots,tx_n) = \sum_{i_1\ldots i_n} a_{i_1\ldots i_n}(tx_1)^{i_1}\cdots(tx_n)^{i_n} = t^d \sum_{i_1\ldots i_n} a_{i_1\ldots i_n} {x_1}^{i_1}\cdots {x_n}^{i_n} = t^d F(x_1,\ldots,x_n)\,.$$

Viceversa, sia $F(x_1,\ldots,x_n)$ un polinomio in n variabili di grado d in $D[x_1,\ldots,x_n]$ con la proprietà che

$$F(tx_1,\ldots,tx_n) = t^d F(x_1,\ldots,x_n)\,, \quad \forall t \in D$$

Vogliamo mostrare che F è una forma di grado d. Scriviamo il polinomio F come somma di polinomi omogenei di grado minore o uguale a d, cioè

$$F = F_0 + F_1 + F_2 + \cdots + F_d$$

dove gli F_i sono polinomi omogenei di grado i. Si trova

$$\begin{aligned} t^d F(x_1,\ldots,x_n) &= F(tx_1,\ldots,tx_n) \\ &= F_0(tx_1,\ldots,tx_n) + F_1(tx_1,\ldots,tx_n) + \cdots + F_d(tx_1,\ldots,tx_n) \\ &= F_0(x_1,\ldots,x_n) + tF_1(x_1,\ldots,x_n) + \cdots + t^d F_d(x_1,\ldots,x_n) \end{aligned}$$

Dall'ultima identità si ricava che

$$F_0(x_1,\ldots,x_n) + tF_1(x_1,\ldots,x_n) + \cdots + t^d(F_d(x_1,\ldots,x_n) - F(x_1,\ldots,x_n)) = 0\,, \quad \forall t \in D$$

L'ultima rappresenta un equazione di grado d con coefficienti nel dominio $D[x_1,\ldots,x_n]$ la quale risulta avere infinite soluzioni, tutti gli elementi di D. Dalla Proposizione 14.5 segue che l'unica possibilità è che tutti i coefficienti siano identicamente nulli, cioè

$$F_0 = 0, F_1 = 0, \ldots, F_{d-1} = 0, F_d - F = 0\,.$$

Segue che $F = F_d$. ■

Vale la seguente proprietà

Proposizione 14.11 Un divisore di una forma è una forma.

Dimostrazione. Sia $F(x_1,\ldots,x_n) \in D(x_1,\ldots,x_n)$ una forma e supponiamo che

$$F(x_1,\ldots,x_n) = P(x_1,\ldots,x_n)Q(x_1,\ldots,x_n)\,.$$

Vogliamo dimostrare che $P(x_1,\ldots,x_n)$ e $Q(x_1,\ldots,x_n)$ sono forme. Supponiamo per assurdo che $P(x_1,\ldots,x_n)$ non sia una forma. Decomponendo $P(x_1,\ldots,x_n)$ e $Q(x_1,\ldots,x_n)$ in somme di forme si ottiene (omettiamo di scrivere il nome delle variabili per semplificare le notazioni):

$$P = F_a + \cdots + F_b\,, \quad F_a \neq 0, F_b \neq 0$$

$$Q = G_p + \cdots + G_q\,, \quad G_p \neq 0, G_q \neq 0$$

Se P non è una forma si deve avere $a < b$. Allora

$$\text{grado}(F_a G_p) = a + p < b + q = \text{grado}(F_b G_q)$$

da cui l'assurdo che F non è una forma. ■

Se D è un campo $\mathbb{K}$ allora, utilizzando la (14.4) e la Proposizione 14.11, si perviene alla

Proposizione 14.12 Sia $\mathbb{K}$ è un campo e sia $F(x_1,\ldots,x_n) \in \mathbb{K}[x_1,\ldots,x_n]$ una forma non costante di grado d. Allora $F(x_1,\ldots,x_n)$ si scrive in modo unico come

$$F(x_1,\ldots,x_n) = uF_1(x_1,\ldots,x_n)^{r_1}\cdots F_s(x_1,\ldots,x_n)^{r_s}, \quad r_i \in \mathbb{N}^* \tag{14.5}$$

con $F_i(x_1,\ldots,x_n)$ forme irriducibili distinte e $u \in \mathbb{K}, u \neq 0$.

Un caso particolare della Proposizione 14.12 si ottiene quando $\mathbb{K} = \mathbb{C}$ e le variabili sono 2.

Proposizione 14.13 Sia $F(x,y)$ una forma di grado d in $\mathbb{C}[x,y]$. Allora

$$F(x,y) = (\alpha_1 x + \beta_1 y)^{r_1}\cdots(\alpha_s x + \beta_s y)^{r_s}, \quad r_i \in \mathbb{N}^*$$

dove $\alpha_i, \beta_j \in \mathbb{C}$ e $r_1 + \cdots + r_s = d$.

Dimostrazione. La forma $F(x,y)$ può essere scritta come

$$F(x,y) = \sum_{i=0}^{d} a_i x^i y^{d-i}$$

Sia $c = \max\{i\colon a_i \neq 0\}$. Allora

$$F(x,y) = \sum_{i=0}^{c} a_i x^i y^{d-i} = y^d \sum_{i=0}^{c} a_i \left(\frac{x}{y}\right)^i.$$

Adesso

$$\sum_{i=0}^{c} a_i \left(\frac{x}{y}\right)^i$$

è un polinomio di grado c nella variabile $t = x/y$ e per la (14.2) si avrà

$$\sum_{i=0}^{c} a_i \left(\frac{x}{y}\right)^i = a_c \left(\frac{x}{y} - \gamma_1\right)^{v_1} \cdots \left(\frac{x}{y} - \gamma_s\right)^{v_p}, \quad v_i \in \mathbb{N}^*, a_c \in \mathbb{C}, a_c \neq 0, \gamma_i \in \mathbb{C}$$

con $v_1 + \cdots + v_p = c$. Infine,

$$\begin{aligned} F(x,y) &= y^d a_c \left(\frac{x}{y} - \gamma_1\right)^{v_1} \cdots \left(\frac{x}{y} - \gamma_s\right)^{v_p} \\ &= a_c \frac{y^d}{y^c} (x - \gamma_1 y)^{v_1} \cdots (x - \gamma_s y)^{v_p} \\ &= a_c y^{d-c} (x - \gamma_1 y)^{v_1} \cdots (x - \gamma_s y)^{v_p}. \end{aligned}$$

■

Infine, ecco una piccola utile proposizione, che ci fornisce una condizione sufficiente per l'irriducibilità di alcuni polinomi.

Proposizione 14.14 Siano F e G due forme non nulle di grado d e $d+1$ rispettivamente. Se F e G non hanno fattori comuni allora il polinomio $P = F + G$ è irriducibile.

Dimostrazione. Supponiamo che $F + G = PQ$ con P e Q polinomi non costanti. Scriviamo

$$P = A_p + \cdots + A_{p'}, \quad Q = B_q + \cdots + B_{q'}$$

dove A_i sono forme di grado i e B_j sono forme di grado j, $p \leq p'$, $q \leq q'$, $A_p, A_{p'}, B_q, B_{q'} \neq 0$. Supponiamo che $p < p'$ e che $q < q'$. Raggrupando monomi di pari grado in $F+G=PQ$ e ricordando che f ha grado d e G ha grado $d+1$ otteniamo

$$F = A_p B_q\,, \quad G = A_p B_{q+1} + A_{p+1} B_q\,, \quad 0 = A_{p+1} B_{q+1} + A_{p+2} B_q + A_p B_{q+2}\,, \ldots, 0 = A_{p'} B_{q'}$$

Ma l'ultima uguaglianza, $0 = A_{p'} B_{q'}$, è assurda poiché $A_{p'}$ e $B_{q'}$ sono polinomi non nulli. Si deve quindi avere che $p = p'$ o $q = q'$. Se $p = p'$ si avrebbe

$$F = A_p B_q\,, \quad G = A_p B_{q+1}$$

da cui A_p sarebbe un fattore comune per F e G contro l'ipotesi. Alla stessa conclusione si perviene se $q = q'$. In conclusione $F+G$ è irriducibile. ■

14.8 Problemi proposti

Problema 14.6 Dimostrare che il criterio di omogeneità dato nella Proposizione 14.10 può fallire su un dominio finito considerando i polinomi sul campo $\mathbb{Z}_2$.

Problema 14.7 Determinare le componenti lineari delle seguenti forme quadratiche in $\mathbb{C}$:

1. $F(x,y) = x^2 + xy + y^2$
2. $F(x,y) = x^3 - y^3$
3. $F(x,y) = x^3 + y^3$
4. $F(x,y) = x^3 + x^2 y + xy^2 + y^3$

Problema 14.8 Dimostrare che i seguenti polinomi sono irriducibili

1. $F(x,y) = xy^2 - xy^2 - x^2 - x^3$
2. $F(x,y) = x^6 - x^2 y^3 - y^5$
3. $F(x,y) = (x^2 + y^2)^2 - y(3x^2 - y^2)$