Matematica di Base (Algebra)

Silvio Valentini
Dipartimento di Matematica Pura ed Applicata
Università di Padova
via G. Belzoni n.7, I–35131 Padova, Italy
carnoval,silvio@math.unipd.it

October 16, 2003

Contents

1 Premessa

In questo corso non ci occuperemo di argomenti di matematica che vi sono estranei ma cercheremo piuttosto di ripensare ad alcuni tra gli argomenti di matematica che a livello di scuola superiore sono di solito trattati con poca precisione. In generale saremo più interessati a sollevare problemi piuttosto che a risolverli; infatti risolverli sarà lo scopo dei prossimi corsi di carattere matematico che incontrerete durante i vostri studi. Insomma, quel che vogliamo è che alla fine del corso il vostro modo di affrontare le questioni matematiche sia più maturo e che smettiate di pensare alla matematica come ad una collezione di tecniche da applicare.

Tanto per cominciare, consideriamo ad esempio un insieme numerico che probabilmente supponete di conoscere abbastanza bene, se non altro per averlo usato per anni: l'insieme dei numeri reali.

Sicuramente ricorderete che i numeri reali si possono suddividere in *numeri razionali* e *numeri irrazionali*. I numeri razionali sono di solito associati alle frazioni, anche se non si tratta di una corrispondenza perfetta visto che possiamo trovare un numero razionale in corrispondenza ad ogni frazione mentre lo stesso numero razionale corrisponde in generale a molte frazioni diverse.

Un po' più difficile è forse ricordare che i numeri razionali sono quei numeri la cui espansione decimale è finita o periodica mentre i restanti numeri sono gli irrazionali. È quindi elementare fornire esempi concreti di numeri razionale in quanto basta fare il quoziente di due numeri interi e non troppo difficile neppure fornire qualche esempio concreto di numero irrazionale. Si può ad esempio considerare $0,101101110111101111110\ldots$ che non ha uno sviluppo decimale finito o periodico visto che il numero di 1 dopo uno 0 aumenta sempre. Naturalmente, voi conoscete dalla scuola altri numeri irrazionali (sicuramente ricorderete $\sqrt{2}$, $\sqrt{3}$, π, $\ldots$) ma come si fa a essere sicuri che il loro sviluppo decimale non è finito o periodico? La domanda è interessante perché pone le prime basi per la necessità dello sviluppo di una accurata formalizzazione e quindi di fare della matematica. Infatti, mentre per fare vedere che un certo numero q è un numero razionale basta trovare una coppia di numeri interi a e b tali che dividendo a per b si ottenga q, per far vedere che un certo numero r *non* è un numero razionale bisogna far vedere che qualsiasi tentativo si faccia di dividere un numero intero per un altro numero intero non si ottiene mai r; naturalmente questo compito non si può fare per tentativi, visto che c'è il rischio di non arrivare mai alla fine dei tentativi, e bisogna quindi elaborare qualche altra maniera di convincersi che tali numeri interi non esistono. Sorge quindi la necessità di introdurre un'idea completamente nuova, quella di *dimostrazione*. La prova della irrazionalità di alcuni dei numeri precedenti non è troppo difficile ma per altri la dimostrazione non è affatto banale.

Proviamo adesso a porci alcune semplici domande.

Il numero $q = 0,999999\ldots$ è senza dubbio un numero razionale visto che è chiaramente periodico. Si tratta di un numero minore, uguale o maggiore di 1?

Mentre si fa presto a decidere che q non è maggiore di 1 forse qualche dubbio rimane rispetto alla decisione se si tratta di un numero minore o di un numero uguale ad 1. Per fortuna la risposta in questo caso non è troppo difficile. Infatti c'è una regoletta che ci dice come associare una frazione ad ogni numero periodico e con tale regoletta non è difficile scoprire che $q = \frac{9}{9}$ e quindi che q e 1 coincidono; si tratta di un risultato forse inaspettato visto che q sembra essere sempre minore di 1 sia pure per quantità che diventano via via minori man mano che si considerano più cifre nella sua espasione decimale.

Questo esempio ci fornisce comunque almeno un paio di considerazioni: un numero razionale (e ancora di più un numero reale) può avere più di una espressione in notazione decimale e inoltre decidere quando due espansioni decimali indicano lo stesso numero non è una operazione che in generale sia banale. Infatti nel caso dei numeri razionali, le cui espansioni decimali sono finite o periodiche, sappiamo cosa fare visto che c'è una regola adatta, ma che fare se ci troviamo di fronte a due numeri irrazionali? Siamo ancora capaci di decidere se due espansioni decimali indicano lo stesso numero reale o due numeri reali diversi?

È evidente che la presenza o meno di una regoletta cambia completamente la situazione: alcune questioni si possono decidere mentre per rispondere ad altre domande non si sa come fare, vale a dire che non c'è un programma che fornisca la risposta.

Consideriamo ora una nuova questione che forse avete dato sempre per scontata: le operazioni.

È chiaro che sappiamo fare le usuali operazioni di somma, sottrazione, prodotto e divisione tra i numeri razionali, ma cosa i può dire delle stesse operazioni tra i numeri reali?

Quel che sappiamo è che un numero reale è irrazionale quando si tratta di una espansione decimale infinita e non periodica, ma allora come si fa ad applicare il metodo che conosciamo per fare la somma al caso di un numero irrazionale con se stesso? Si consideri ad esempio il numero irrazionale $x = 0,10110111011110\ldots$ che abbiamo già visto in precedenza. Come si fa a *calcolare* $x + x$ o $x \times x$? Sicuramente non possiamo usare il solito metodo che prevede di cominciare a sommare o moltiplicare dalla cifra più a destra visto che in questo caso tale cifra più a destra non c'è. D'altra parte non possiamo neppure trasformare tale numero in una frazione, ed usare poi il metodo per sommare due frazioni che già conoscete, visto che non c'è nessuna frazione che equivalga ad x.

Sembra quindi che non esista un *metodo* per fare le operazioni tra i numeri reali (nessun programma per un calcolatore permette di fare la somma tra due numeri reali), ma allora cosa vogliono dire queste operazioni?

Naturalmente il problema di non sapere bene cosa vogliano dire le operazioni tra i numeri reali porta ad altre conseguenze. Ad esempio, $\sqrt{2}$ è *definito* come quel numero reale x tale che $x \times x = 2$, ma abbiamo già detto che se qualcosa come $\sqrt{2}$ esiste esso non è sicuramente un numero razionale e quindi non abbiamo un'idea precisa di cosa voglia dire $x \times x$. Ma allora cosa significa la definizione che abbiamo dato di $\sqrt{2}$?

Naturalmente a partire da quelle che abbiamo proposto nascono altre domande ma sembra chiaro che esiste una forte necessità di ripensare, a partire dai concetti più elementari, la matematica che avete studiato fino ad oggi.

Esercizi

1. Determinare la regola che associa una frazione ad un numero razionale e dimostrare che essa è corretta.
2. Dimostrare che $\sqrt{2}$ non è un numero razionale.
3. Dimostrare che, per ogni numero primo p, $\sqrt{p}$ non è un numero razionale.
4. Dimostrare che esistono due numeri irrazionali x e y tali che x^y è un numero razionale. (*Suggerimento.* Si consideri $\sqrt{2}^{\sqrt{2}}$; se tale numero è razionale abbiamo trovato i due numeri irrazionali cercati; altrimenti si consideri $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$)

2 Collezioni e insiemi

L'operazione mentale di pensare insieme, come un'unica entità, più cose è tra le più naturali e si riflette infatti costantemente nel linguaggio naturale: chiamiamo gregge, un unico concetto, una collezione di pecore, chiamiamo classe una collezione di studenti e chiamiamo squadra una collezione di giocatori.

Questa operazione è forse la più semplice tra le operazioni di astrazione che si possono operare sulla realtà. La sua utilità è evidente in quanto rende possibile ridurre la complessità di un mondo in cui il numero di oggetti in gioco cresce facilmente al di là delle nostre possibilità di controllo: ad esempio le classi di una scuola possono essere una ventina mentre il numero degli studenti può essere di cinquecento e, per chi deve fare l'orario delle lezioni, è ben diverso pensare di organizzare venti oggetti piuttosto che cinquecento.

Naturalmente il pensare assieme le cose non è una operazione che viene effettuata in modo completamente casuale ma piuttosto secondo certi criteri che, di volta in volta, possono essere i più diversi: gli studenti di una scuola possono essere raggruppati in classi in relazione alla loro età, ma, quando si tratta di usare la pelestra, possono anche essere divisi in due grandi gruppi a seconda del loro sesso. In entrambi i casi i gruppi vengono formati seguendo un certo concetto.

In matematica un simile approccio ha avuto un tale successo che buona parte della matematica si è potuta ridurre alla sola nozione di collezione e alle operazioni che forniscono nuove collezioni a partire da altre collezioni. Nei prossimi paragrafi cominceremo appunto a vedere come tale riduzione possa essere effettuata. Tuttavia prima ancora di cominciare con questo programma di lavoro conviene vedere fino a che punto l'operazione di costruire delle collezioni si possa effettuare in modo sicuro ed esente da paradossi, almeno nel caso in cui si voglia parlare di oggetti matematici. Vogliamo perciò analizzare in modo astratto l'idea del *mettere le cose insieme*: con un facile gioco di parole potremo dire che vogliamo analizzare il *concetto di concetto*.

2.1 Il concetto di concetto

Per partire con la nostra analisi, la prima idea che viene in mente, ispirata dalla vita di tutti i giorni, è quella di confondere un concetto con una proprietà: il concetto di gregge è basato sulla proprietà di essere una pecora appartenente ad un certo pastore, quello di classe scolastica sulla proprietà di avere la stessa età, quello di numero naturale pari sulla proprietà di essere divisibile per 2. L'idea sembra quindi buona. Tanto per cominciare, è fuori di dubbio che ogni collezione finita, che possiamo indicare con $\{a_1, \ldots, a_n\}$ se essa è formata dagli elementi a_1, $\ldots a_n$, può essere comunque descritta tramite la proprietà di "essere uno dei suoi elementi uguale ad a_1 oppure di essere uguale ad a_2 oppure $\ldots$ oppure di essere uguale ad a_n" (notazione $\{x \mid x = a_1 \text{ o } \ldots \text{ o } x = a_n\}$ che si legge "la collezione degli elementi x tali che $x = a_1$ o $\ldots$ o $x = a_n$"). Inoltre l'idea funziona bene anche per indicare collezioni che contengono un numero non finito di elementi: in questo caso infatti la notazione precedente, vale a dire $\{a_1, \ldots, a_n\}$, non può proprio funzionare e passare attraverso la descrizione tramite una proprietà sembra essere l'unica strada percorribile. In questo modo possiamo ad esempio indicare la collezione dei numeri pari tramite la notazione $\{x \mid x \text{ si divide per } 2\}$ o la collezione dei numeri primi positivi con la notazione $\{x \mid \text{gli unici divisori interi di } x \text{ sono } 1 \text{ e } x \text{ stesso}\}$.

Bisogna tuttavia notare che considerare una collezione di oggetti come un unico ente la rende a sua volta un possibile soggetto di proprietà: ad esempio potrò dire "il gregge è del pastore Silvio" o "la collezione dei numeri pari contiene un numero non finito di elementi". È quindi possibile che il confondere un concetto con una proprietà possa portare a qualche situazione paradossale. Il primo esempio di tali paradossi si deve a Bertrand Russell. Egli si è posto il problema di analizzare la collezione R i cui elementi sono le collezioni che non sono elementi di se stesse. Osserviamo prima di tutto che se le collezioni possono essere soggetto di una proprietà la frase "le collezioni che non sono elementi di se stesse" è dotata di significato. Ora, è facile riconoscere che, ad esempio, la collezione di tutti i gatti è un elemento di R, poiché essa è un concetto e non è perciò certamente un gatto e non può quindi essere un elemento di se stessa. D'altra parte la collezione di tutte le collezioni con un numero non finito di elementi non è un elemento di R, poiché essa è un elemento di se stessa; infatti, tale collezione ha sicuramente un numero non finito di elementi distinti: ad esempio, essa contiene la collezione dei numeri naturali, quella dei numeri naturali escluso il numero 1, quella dei numeri naturali escluso il numero 2 e così via. Sorge ora, abbastanza naturale, il problema di scoprire se R è oppure no un elemento di se stesso. Ma questa domanda ci conduce direttamente ad una situazione paradossale: se R fosse un elemento di R allora, visto che R

è costituito esattamente dalle collezioni che non sono elemento di se stesse, dedurremmo che R non è un elemento di se stesso; d'altra parte se R non è un elemento di se stesso per la definizione stessa di R ci troveremo forzati ad ammettere che R deve essere un elemento di se stesso. Trascrivendo le considerazioni precedenti in simboli utilizzando la notazione $X \in Y$ per indicare che X è un elemento di Y, abbiamo

$$R \in R \text{ se e solo se } R \in \{X \mid X \notin X\} \text{ se e solo se } R \notin R$$

Poiché non sono previste altre possibilità, vale a dire che o R è un elemento della collezione R o non lo è, ci troviamo in un paradosso senza via d'uscita.

2.2 Insiemi

Il paradosso di Russell che abbiamo visto alla fine della sezione precedente ci obbliga a riflettere sul tipo di collezioni che potranno esserci utilizzate per fare matematica visto che è chiaro che pensare di ammettere tutte le possibili collezioni è una strada troppo pericolosa. Tuttavia analizzando la struttura del paradosso possiamo cercare di capire quali collezioni possiamo ammettere senza correre troppi rischi. Il paradosso sembra nascere da una situazione di autoriferimento in quanto la collezione R è fatta con collezioni tra le quali R stessa può trovarsi. Una via per sfuggire al paradosso è allora quella di abbandonare l'idea di usare tutte le collezioni e di limitarsi ad usare solo quelle formate da elementi che sono giá stati riconosciuti come collezioni "sicure". Diremo che se seguiamo questo approccio accetteremo per le collezioni il principio di *buona fondatezza*.

Per evitare di fare confusione, d'ora in avanti chiameremo collezione il risultato di una qualunque operazione mentale consistente nel pensare alle cose assieme (e per le collezioni accetteremo i rischi connessi!) mentre riserveremo il nome di *insieme* per quelle particolari collezioni che possono essere soggetto di proprietà senza dare luogo a paradossi. Naturalmente la nostra speranza è che la collezione degli insiemi si riesca a descrivere per bene e che sia sufficiente per fare tutta la matematica cui siamo interessati. Notate, tanto per cominciare, che il principio di buona fondatezza richiede che la collezione di tutti gli insiemi non sia un insieme.

Esercizi.

1. Dimostrare che la collezione di tutti gli insiemi non è un insieme.

2. Dimostrare che la collezione di tutti gli insiemi infiniti non è un insieme.

2.2.1 Gli assiomi di base

Se vogliamo seguire il principio di buona fondatezza ci ritroviamo all'inizio a non possedere alcun insieme per cui l'unico insieme che possiamo costruire è quello che non ha nessun elemento (si ricordi che le uniche collezioni che ammettiamo come elementi di un insieme sono quelle che sono già state riconosciute come insiemi). Cominciamo perciò con il seguente assioma.

Definizione 2.1 (Assioma dell'insieme vuoto) *La collezione che non contiene alcun elemento è un insieme che chiameremo* insieme vuoto *e indicheremo con* $\emptyset$.

Non è difficile rendersi conto che usando solo l'insieme vuoto di matematica se ne fa veramente poca, per cui è bene cercare di costruire nuovi insiemi. Iniziamo dunque introducendo un po' di notazioni che ci saranno utili nel seguito della trattazione.

La più importante relazione tra insiemi è naturalmente la *relazione di appartenenza*, indicata con $X \in Y$, cui abbiamo già accennato nella sezione precedente. La useremo per indicare che X è un elemento dell'insieme Y. La sua negazione verrà denotata con $X \notin Y$ e verrà usata per indicare che l'elemento X non appartiene all'insieme Y. Ad essa segue per importanza la *relazione di sottoinsieme* che può essere definita utilizzando la relazione di appartenenza.

Definizione 2.2 (Sottoinsieme) *Siano* X *e* Y *due insiemi. Scriveremo allora* $X \subseteq Y$ *come abbreviazione per dire che, per ogni insieme* z*, se* $z \in X$ *allora* $z \in Y$.

È interessante notare che se X è un insieme e Y è una collezione i cui elementi appartengono tutti a X allora il principio di buona fondatezza ci spinge a considerare anche Y come un insieme.

Definizione 2.3 (Assioma del sottoinsieme) *Sia* X *un insieme e* Y *una collezione tale che per ogni elemento di* Y *è anche un elemento di* X*. Allora* Y *è un insieme.*

Visto che tutto quello che ci interessa analizzare degli insiemi sono i loro elementi non è difficile accordarsi su fatto che possiamo considerare uguali due insiemi se questi hanno esattamente gli stessi elementi.

Definizione 2.4 (Estensionalità) *Siano* X *ed* Y *due insiemi. Diremo allora che* X *è uguale a* Y *se e solo se* X *e* Y *hanno gli stessi elementi.*

Usando la definizione di sottoinsieme è immediato verificare che l'insieme X è uguale all'insieme Y se e solo se $X \subseteq Y$ e $Y \subseteq X$.

Possiamo ora tornare alla situazione cui eravamo arrivati prima delle disavventure dovute al paradosso di Russell per vedere come si può, almeno in parte, recuperare l'idea di definire un insieme tramite una proprietà pur rispettando il principio di buona fondatezza. Come abbiamo detto l'idea che ci deve guidare è che possono essere elementi di un insieme solo quelle collezioni che abbiamo già riconosciuto come insiemi. Questo ci porta immediatamente al seguente assioma.

Definizione 2.5 (Assioma di separazione) *La collezione di tutti gli elementi di* X *che soddisfano la proprietà* $P(-)$ *è un insieme che indicheremo con* $\{x \in X \mid P(x)\}$.

Infatti, la collezione $\{x \in X \mid P(x)\}$, essendo composta solamente di elementi di un insieme, e quindi già riconosciuti come insiemi, è una collezione che il principio di buona fondatezza ci assicura essere "non pericolosa".

Possiamo immediatamente utilizzare l'assioma di *separazione* per definire una prima operazione tra insiemi.

Definizione 2.6 (Intersezione binaria di insiemi) *Siano X e Y due insiemi. Diremo* intersezione *tra l'insieme X e l'insieme Y l'insieme così definito*

$$X \cap Y \equiv \{x \in X \mid x \in Y\}$$

È ovvio che se X e Y sono due insiemi allora, come conseguenza dell'assioma di *separazione*, anche $X \cap Y$ è un insieme.

Tuttavia, l'assioma di separazione ci permette di ottenere solamente insiemi che sono sottoinsiemi di altri insiemi e avendo noi, per ora, a disposizione solo l'insieme vuoto tutto ciò che possiamo ottenere è solo l'insieme vuoto. Introduciamo quindi il più semplice dei modi per costruire nuovi insiemi.

Definizione 2.7 (Assioma della coppia) *Siano X e Y due insiemi. Allora la collezione i cui elementi sono gli insiemi X e Y è un insieme che indicheremo con $\{X, Y\}$.*

Il principio di buona fondatezza ci assicura che questo assioma non è pericoloso e possiamo quindi usarlo per produrre nuovi insiemi. Tramite l'assioma della coppia possiamo produrre insiemi con uno (perché?) o due elementi quale ad esempio $\{\emptyset, \{\emptyset\}\}$. Tuttavia, se il nostro scopo è quello di rifare la matematica usando solo gli insiemi, conviene sforzarci un po' per ottenere almeno insiemi con un numero qualsiasi di elementi (vorremmo pur ottenere i numeri naturali!). Introduciamo quindi il seguente assioma.

Definizione 2.8 (Assioma dell'unione binaria) *Siano X e Y due insiemi. Allora la collezione i cui elementi sono elementi di X o elementi di Y è un insieme che indicheremo con $X \cup Y$.*

Per giustificare il fatto che l'assioma dell'unione binaria ci permette di definire un insieme "sicuro" dobbiamo di nuovo rifarci al principio di buona fondatezza (perché?).

Usando l'assioma dell'unione è possibile finalmente costruire insiemi con un numero qualsiasi, purché finito, di elementi.

Esercizi

1. Dimostrare che due insiemi X e Y sono uguali se e solo se $X \subseteq Y$ e $Y \subseteq X$.

2. Dimostrare che esiste un unico insieme vuoto.

3. Dimostrare che l'unico sottoinsieme dell'insieme vuoto è l'insieme vuoto.

4. Definire, utilizzando gli assiomi fin qui introdotti, un insieme con un unico elemento.
5. Dimostrare che $X \cap Y = X$ se e solo se $X \subseteq Y$
6. Dimostrare che $W \subseteq X$ e $W \subseteq Y$ se e solo se $W \subseteq X \cap Y$.
7. Dimostrare che $X \cup Y = Y$ se e solo se $X \subseteq Y$
8. Dimostrare che $X \subseteq W$ e $Y \subseteq W$ se e solo se $X \cup Y \subseteq W$.
9. Dimostrare che con gli assiomi fin qui considerati possiamo costruire insiemi finiti con un numero arbitrario di elementi.
10. Dimostrare che se X è un insieme con n elementi e Y è un insieme con m elementi allora l'insieme $X \cap Y$ è vuoto se e solo se l'insieme $X \cup Y$ ha $n + m$ elementi.

2.2.2 I numeri naturali

Naturalmente gli insiemi finiti non sono sufficienti per fare la matematica. Il prossimo passo è quindi quello di definire una collezione i cui elementi siano una ragionevole ricostruzione dei numeri naturali: l'idea di fondo è che dobbiamo costruire, per ogni numero naturale n, un insieme che abbia esattamente n elementi. Sappiamo quindi subito come partire, visto che di insiemi con 0 elementi ce n'è uno solo:

$$0 \equiv \emptyset$$

Il prossimo passo è quello di capire come trovare un insieme che abbia un unico elemento. Anche questo è facile e il problema è piuttosto quello di scegliere un insieme particolare tra tutti gli infiniti insiemi con un unico elemento. Una scelta standard, che risulterà vantaggiosa, è la seguente:

$$1 \equiv \{\emptyset\}$$

cioé $1 \equiv \{0\}$.

A questo punto abbiamo già costruito due insiemi diversi e quindi ottenere un insieme che rappresenti il numero 2 è facile. Infatti basta porre:

$$2 \equiv \{0, 1\}$$

che ci dà anche l'idea generale su come procedere:

$$n \equiv \{0, 1, \dots, n-1\}$$

Possiamo esprimere questa definizione di infiniti oggetti in modo più compatto tramite una definizione *induttiva* dei numeri naturali:

$$\begin{array}{ll} \text{(Base)} & 0 \equiv \emptyset \\ \text{(Passo)} & n+1 \equiv n \cup \{n\} \end{array}$$

che ci dice (base) come partire e (passo) come ottenere un nuovo elemento, il successivo numero naturale, a partire da un elemento già costruito.

Definizione 2.9 (Assioma dei numeri naturali) *La collezione i cui elementi sono gli insiemi costruiti tramite la precedente definizione induttiva è un insieme che indicheremo con ω.*

Anche in questo caso il principio di buona fondatezza ci assicura che questa collezione non è pericolosa perché costituita solamente con elementi che sono insiemi. Tuttavia, l'averla riconosciuta come insieme è un grande passo avanti: possediamo infatti il nostro primo insieme infinito! Vale la pena di sottolineare che questa definizione dei numeri naturali si fonda pesantemente sull'intuizione che già si possiede dei numeri naturali; non sarebbe infatti possibile, in mancanza di questa intuizione, afferrare l'idea fondamentale che sostiene che la definizione induttiva dei numeri naturali produce ad ogni passo un nuovo insieme ma soprattutto che il processo di produzione di nuovi insiemi è discreto (cioé ha senso parlare di "step") e non ha termine.

Prima di concludere questo capitolo, visto che adesso possediamo insiemi con infiniti elementi, è utile rafforzare l'assioma dell'unione binaria a questa nuova situazione.

Definizione 2.10 (Assioma dell'unione arbitraria) *Sia I un insieme di insiemi. Allora la collezione i cui elementi sono gli elementi di un qualche $X \in I$ è un insieme che indicheremo con $\bigcup_{X \in I} X$.*

È facile rendersi conto che l'assioma dell'unione binaria altro non è che un'istanza di questo assioma nel caso in cui l'insieme I abbia due elementi. Possiamo giustificare questo nuovo assioma facendo appello al principio di buona fondatezza visto che anche in questo caso gli elementi della collezione $\bigcup_{X \in I} X$ sono già stati riconosciuti come elementi di un qualche insieme.

Esercizi

1. Dimostrare che sistono infiniti insiemi con un unico elemento.
2. Dimostrare che i numeri naturali sono uno diverso dall'altro.
3. Trovare una diversa rappresentazione insiemistica per i numeri interi.
4. Dimostrare che $X \subseteq W$ per ogni $X \in I$ se e solo se $\bigcup_{X \in I} X \subseteq W$.

2.2.3 Induzione

La definizione induttiva dei numeri naturali ci mette immediatamente a disposizione una potente tecnica per dimostrare le proprietà dei numeri naturali. Basta infatti notare che ogni numero naturale è *raggiungibile*, a partire dallo 0, applicando un numero sufficiente di volte l'operazione di "passare al successivo" per rendersi conto che ogni proprietà che vale per lo 0 e che vale per $n + 1$ qualora valga per n deve inevitabilmente valere per tutti i numeri naturali.

Definizione 2.11 (Principio di induzione) *Sia $P(-)$ una proprietà sui numeri naturali. Allora, se vale $P(0)$ e, per ogni numero naturale n, $P(n)$ implica $P(n+1)$ allora P vale per ogni numero naturale.*

Vedremo più avanti alcune applicazioni del principio di induzione. Illustriamone comunque immediatamente una applicazione che permette di ottenerne una (apparente) generalizzazione che risulterà molto utile.

Definizione 2.12 (Principio di induzione completa) *Sia $P(-)$ una proprietà sui numeri naturali. Allora, se, per ogni numero naturale n, $P(n)$ è conseguenza di $P(0)$, ..., $P(n-1)$, allora $P(-)$ vale per ogni numero naturale.*

Dimostrazione. Introduciamo la seguente nuova proposizione

$$Q(n) \equiv \text{per ogni numero } m \text{ tale che } 0 \leq m \leq n,\ P(m) \text{ vale}$$

È allora ovvio che se vale $Q(n)$ allora vale anche $P(n)$ visto che se $P(m)$ vale per ogni numero tale che $0 \leq m \leq n$ allora $P(-)$ vale in particolare per n.

Vediamo allora di dimostrare che $Q(-)$ vale per ogni n utilizzando il principio di induzione.

- (Base) Dobbiamo dimostrare che vale $Q(0)$, cioé che per ogni numero m tale che $0 \leq m \leq 0$ vale $P(m)$, cioé che vale $P(0)$. Ora, per ipotesi, noi sappiamo che, per ogni numero naturale n, $P(n)$ è conseguenza di $P(0)$, ..., $P(n-1)$ che in particolare nel caso $n = 0$ dice che $P(0)$ è vero in quanto conseguenza di un insieme vuoto di ipotesi.

- (Passo) Dobbiamo dimostrare che se assumiamo che $Q(n)$ valga allora anche $Q(n+1)$ vale. Ora, dire che $Q(n)$ vale significa che, per ogni numero m tale che $0 \leq m \leq n$, vale $P(m)$ ma, per ipotesi, questo implica che $P(n+1)$ vale e quindi, per ogni $0 \leq m \leq n+1$, vale $P(m)$, cioé vale $Q(n+1)$.

Esercizi

1. Dimostrare per induzione che, per ogni numero naturale n, $2^n \geq n+1$.

2. Dimostrare per induzione che per ogni numero naturale n

$$1 + 2 + 3 + \ldots + n = \frac{n \times (n+1)}{2}$$

3. Trovare una dimostrazione della precedente uguaglianza che *non* utilizzi il principio di induzione.

4. Dimostrare per induzione che n rette dividono il piano in un numero di regioni minore o uguale a 2^n.

5. Trovare l'errore nella seguente prova per induzione che "dimostra" che tutti i bambini hanno gli occhi dello stesso colore. Sia $P(n)$ la proprietà che afferma che tutti i bambini in un gruppo di n bambini hanno gli occhi dello stesso colore. Allora

   - (Base) Ovvio, infatti bisogna andare a verificare che tutti i bambini in un gruppo di 0 bambini hanno gli occhi dello stesso colore.
   - (Passo) Supponiamo che tutti i bambini in un gruppo di n bambini abbiano gli occhi dello stesso colore e dimostriamo che lo stesso vale per tutti i bambini di un gruppo di $n+1$ bambini. Consideriamo quindi un gruppo di $n+1$ bambini e togliamone uno; otteniamo in tal modo un gruppo di n bambini e quindi, per ipotesi induttiva, tutti hanno gli occhi dello stesso colore. Togliamone ora un altro ottenendo di nuovo un gruppo di n bambini che, per ipotesi induttiva, hanno nuovamente gli occhi dello stesso colore. Ma allora anche i bambini che evevamo tolto hanno gli occhi dello stesso colore.

6. (algoritmo veloce di moltiplicazione) Dimostrare, utilizzando il principio di induzione completa, che il seguente algoritmo per moltiplicare due numeri naturali è corretto. Dati due numeri n e m se $n = 0$ allora rispondiamo 0. Altrimenti, se n è pari calcoliamo il prodotto di $\frac{n}{2}$ con $2 * m$ mentre se n è dispari calcoliamo il prodotto di $\frac{n-1}{2}$ con $2 * m$ e aggiungiamo m al risultato. Possiamo scrivere il precedente algoritmo nel modo seguente

$$\begin{cases} 0 \times m & = & 0 \\ (n+1) \times m & = & \text{if } \mathsf{Pari}(n+1) \\ & & \text{then } \frac{n+1}{2} \times (2 * m) \\ & & \text{else } (\frac{n}{2} \times (2 * m)) + m \end{cases}$$

   L'nteresse in questo algoritmo sta nel fatto che in un calcolatore la divisione e la moltiplicazione per 2 sono operazioni primitive estremamente veloci.

7. (Torre di Hanoi) Il gioco della torre di Hanoi consiste nello spostare n dischi di diverso diametro, infilati ordinatamente in un piolo l'uno sull'altro, verso un secondo piolo utilizzando un terzo piolo e con il vincolo che un disco non deve mai essere posto sopra un disco di diametro maggiore. La leggenda narra che ad Hanoi ci sono dei monaci che stanno spostando dall'inizio dell'universo 64 dischi e che l'universo finirà quando anche l'ultimo disco sarà spostato.

   Trovare una funzione f che fornisca il minimo numero di mosse necessarie per spostare n dischi e dimostrare per induzione che, per ogni $n \in \omega$, $f(n) \geq 2^{n-1}$ (e possiamo quindi stare tranquilli sulla durata dell'universo!).

8. Sia $\leq$ l'usuale relazione d'ordine tra i numeri naturali ω. Un sottoinsieme S di ω possiede un elemento minimo se esiste un elemento $m \in S$ tale che,

per ogni $x \in S$, $m \leq x$. Dimostrare, utilizzando il principio di induzione completa, che ogni sottoinsieme non vuoto S di ω ha elemento minimo. (Sugg.: porre $P(n) \equiv n \notin S$ e dimostrare che se S non ha elemento minimo allora $S = \emptyset$)

9. Dimostrare che se ogni sottoinsieme non vuoto di ω ha minimo allora vale il principio di induzione. (Sugg.: se $P(-)$ è la proprietà in esame si consideri il sottoinsieme $S \equiv \{x \in \omega \mid \text{non vale } P(x)\}$; ora, se $P(-)$ non valesse per ogni n allora S sarebbe non vuoto e quindi dovrebbe avere minimo, ma allora ...)

2.2.4 Somma e prodotto

Naturalmente i numeri naturali non ci interessano solo in quanto essi sono il nostro primo esempio di insieme infinito ma anche perché sono il nostro primo esempio di insieme numerico, un insieme cioé su cui possiamo definire le *solite* operazioni. Una operazione infatti altro non è che una funzione totale (per una definizione formale di cosa è una funzione si veda il prossimo capitolo, per ora ci accontentiamo di quel che avete imparato alle scuole superiori). Nel nostro caso le operazioni che vogliamo definire sui numeri naturali sono la somma ed il prodotto (attenzione: sottrazione e divisione non sono operazioni sui numeri naturali visto che non si tratta di funzioni totali).

Per definire tali operazioni useremo in modo essenziale il fatto che i numeri naturali sono un insieme induttivo: visto che ogni numero naturale si può raggiunere applicando un numero sufficiente di volte l'operazione di successore per definire una operazione o una proprietà sui numeri naturali è sufficiente definirla per lo zero e per il successore di un qualsiasi numero naturale.

Cominciamo quindi ricordando l'operazione di successore di un numero naturale ponedo

$$\mathsf{S}(n) \equiv n + 1 (\equiv n \cup \{n\})$$

Possiamo allora definire la somma tra due numeri naturali come segue

$$\begin{cases} m + 0 & = & m \\ m + \mathsf{S}(n) & = & \mathsf{S}(m + n) \end{cases}$$

e, una volta che sappiamo come fare la somma, possiamo definire il prodotto ponendo

$$\begin{cases} m \times 0 & = & 0 \\ m \times \mathsf{S}(n) & = & m + (m \times n) \end{cases}$$

È interessante notare che queste definizioni si possono facilmente programmare in un qualsiasi linguaggio di programmazione che permetta l'uso della ricorsione.

Naturalmente quelle che abbiamo definito altro non sono che le solite operazioni di somma e prodotto. Si potrebbe ora dimostrare che esse godono delle usuali proprietà cui siete abituati che ricordiamo qui sotto.

Definizione 2.13 (Proprietà della somma) *La somma tra numeri naturali è una operazione che gode delle seguenti proprietà:*

$$\begin{array}{ll} \textit{(commutativa)} & m+n=n+m \\ \textit{(associativa)} & m+(n+k)=(m+n)+k \\ \textit{(elemento neutro)} & m+0=m=0+m \end{array}$$

Definizione 2.14 (Proprietà del prodotto) *Il prodotto tra numeri naturali è una operazione che gode delle seguenti proprietà:*

$$\begin{array}{ll} \textit{(commutativa)} & m\times n=n\times m \\ \textit{(associativa)} & m\times(n\times k)=(m\times n)\times k \\ \textit{(elemento neutro)} & m\times 1=m=1\times m \\ \textit{(distributiva)} & m\times(n+k)=(m\times n)+(m\times k) \end{array}$$

Esercizi

1. Sulla falsariga della somma, del prodotto e delle seguenti definizioni, definire per ricorsione altre operazioni sui numeri naturali:
   - (predecessore)
   $$\begin{cases} \mathsf{pred}(0) & = & 0 \\ \mathsf{pred}(n+1) & = & n \end{cases}$$
   - (esponente)
   $$\begin{cases} x^0 & = & 1 \\ x^{n+1} & = & x\times x^n \end{cases}$$
   - (fattoriale)
   $$\begin{cases} 0! & = & 1 \\ n+1! & = & (n+1)\times n! \end{cases}$$

3 Relazioni e funzioni

Adesso che abbiamo ricostruito i numeri naturali all'interno di un ambiente insiemistico il prossimo passo è recuperare il concetto di funzione.

Naturalmente nel linguaggio comune, e anche nella matematica che avete già visto, avrete già sentito parlare di funzioni (esempio: la temperatura è *funzione* dell'ora del giorno, prendere l'ombrello è *funzione* delle previsioni del tempo, $\sin(x)$ è una *funzione* trigonomtrica, ...).

Quel che vogliamo fare qui è analizzare in modo astratto il concetto di funzione.

3.1 Relazioni

Il primo passo per ottenere tale definizione è quello di formalizzare il concetto di relazione all'interno della teoria degli insiemi.

Definizione 3.1 (Coppia ordinata) *Siano x e y due insiemi. Diremo* coppia ordinata *di x e y l'insieme $\langle x, y\rangle \equiv \{x, \{x, y\}\}$.*

Si verifica immediatamente che, per ogni coppia di insiemi x e y, la collezione $\langle x, y\rangle$ è un insieme.

Tramite la definizione di coppia ordinata abbiamo voluto introdurre un meccanismo che ci permetta di distinguere il primo e il secondo elemento all'interno di una coppia di elementi; infatti l'*estensionalità* ci costringe a riconoscere come uguali i due insiemi $\{x, y\}$ e $\{y, x\}$ e quindi se vogliamo distinguere un primo elemento nella coppia dobbiamo, in qualche modo, dichiararlo tale. Questo è esattamente ciò che si ottiene tramite la definizione di coppia ordinata; infatti, si specifica appunto che, nella coppia ordinata $\langle x, y\rangle$, x è il primo elemento di una coppia di elementi costituita da $\{x, y\}$.

Dal punto di visto tecnico, lo scopo della definizione è quello di poter dimostrare che $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$ se e solo se $x_1 = x_2$ e $y_1 = y_2$ (vedi esercizi).

Ora, una relazione tra gli elementi dei due insiemi X e Y può essere specificata dicendo quali elementi dell'insieme X sono in relazione con quali elementi dell'insieme Y. Possiamo esprimere questa situazione all'interno della teoria degli insiemi dicendo che una relazione si identifica con la collezione delle coppie ordinate $\langle x, y\rangle$ il cui primo elemento $x \in X$ è in relazione con il secondo elemento $y \in Y$. Come primo passo, questo ci spinge verso la seguente definizione.

Definizione 3.2 (Assioma del prodotto cartesiano) *Siano X e Y due insiemi. Allora la collezione i cui elementi sono coppie ordinate il cui primo elemento sta in X e il cui secondo elemento sta in Y è un insieme che chiameremo* prodotto cartesiano *di X e Y e indicheremo con $X \times Y$.*

Come al solito, possiamo fare ricorso al principio di buona fondatezza per assicurarci della non pericolosità di questa definizione.

È ora evidente che ogni relazione R tra due insiemi X e Y è un sottoinsieme di $X \times Y$ e quindi è a sua volta un insieme.

Esercizi

1. Siano x e y due insiemi. Verificare, utilizzando gli assiomi introdotti nei paragrafi precedenti, che la coppia ordinata $\langle x, y\rangle$ è un insieme.

2. Siano x_1, x_2, y_1 e y_2 degli insiemi. Dimostrare che $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$ se e solo se $x_1 = x_2$ e $y_1 = y_2$.

3. Supponiamo che X sia un insieme con n elementi e Y sia un insieme con m elementi. Quanti sono gli elementi di $X \times Y$?

3.1.1 Proprietà delle relazioni

Esiste per le relazioni tutto un catalogo di nomi in funzione delle particolari proprietà cui una relazione può soddisfare. Ad esempio, dato un insieme X, una relazione $R \subseteq X \times X$ si dice

- (identità) se $R \equiv \{\langle x, x\rangle \in X \times X \mid x \in X\}$;
- (totale) se $R \equiv X \times X$;
- (riflessiva) se, per ogni $x \in X$, $\langle x, x\rangle \in R$;
- (transitiva) se, per ogni $x, y, z \in X$, se $\langle x, y\rangle \in R$ e $\langle y, z\rangle \in R$ allora $\langle x, z\rangle \in R$;
- (simmetrica) se, per ogni $x, y \in X$, se $\langle x, y\rangle \in R$ allora $\langle y, x\rangle \in R$;
- (antisimmetrica) se, per ogni $x, y \in X$, se $\langle x, y\rangle \in R$ e $\langle y, x\rangle \in R$ allora $x = y$;
- (tricotomica) se, per ogni $x, y \in X$, $\langle x, y\rangle \in R$ o $\langle y, x\rangle \in R$ o $x = y$;
- (preordine) se R è *riflessiva* e *transitiva*;
- (di equivalenza) se R è *riflessiva*, *transitiva* e *simmetrica*;
- (ordine parziale) se R è *riflessiva*, *transitiva* e *antisimmetrica*;
- (ordine totale) se R è un *ordine parziale tricotomico*

È utile ricordare anche la seguente operazione sulle relazioni.

Definizione 3.3 (Relazione inversa) *Sia R una relazione tra l'insieme X e l'insieme Y. Allora chiameremo relazione inversa di R la relazione definita ponendo*

$$R^{-} \equiv \{\langle y, x\rangle \in Y \times X \mid \langle x, y\rangle \in R\}$$

Esercizi

1. Sia U un insieme e sia R la relazione tra sottoinsiemi di U definita ponendo $\langle X, Y\rangle \in R$ se e solo se $X \subseteq Y$. Dimostrare che R è una relazione d'ordine parziale.
2. Sia $\leq$ la relazione tra elementi di ω definita ponendo $\langle x, y\rangle \in\leq$ se e solo se $x = y$ oppure $x \in y$. Dimostrare che $\leq$ è una relazione d'ordine totale.
3. Sia X un insieme. Dimostrare che la relazione totale è una relazione di equivalenza.
4. Sia X un insieme e R una relazione su X. Dimostrare che se R è simmetrica allora $R = R^{-}$.

3.1.2 Rappresentazione cartesiana di una relazione

Data una relazione R tra gli insiemi X e Y, risulta molto conveniente la possibilità di darne una rappresentazione grafica che rende a volte esplicite proprietà che non sono evidenti quando la relazione è rappresentata come insieme di coppie.

Possiamo infatti supporre di rappresentare ciascuno degli insiemi X e Y su una retta e di porre le due rette in posizione l'una ortogonale all'altra. Allora l'insieme dei punti del piano individuato dalle rette X e Y rappresenta il prodotto cartesiano $X \times Y$ tra X e Y e una relazione R tra X e Y si può quindi rappresentare come un particolare sottoinsieme di punti di tale piano.

Esercizi

1. Rappresentare sul piano cartesiano una relazione identica. Di quale punti del piano si tratta?

2. Rapresentare nel piano cartesiano una relazione simmetrica. Cosa si nota?

3. Rappresentare sul piano cartesiano $\omega \times \omega$ le relazioni $\leq$ e $\leq^-$.

3.1.3 Relazioni di equivalenza e partizioni

Le relazioni di equivalenza saranno particolarmente rilevanti negli sviluppi futuri. Una relazione di equivalenza gode infatti delle tre principali proprietà che uno si aspetta dalla relazione Id_X di identità tra elementi dell'insieme X, vale a dire la relazione tra gli elementi di un insieme X definita dall'insieme di coppie i cui elementi sono identici:

$$\mathsf{Id}_X \equiv \{\langle x, x\rangle \in X \times X \mid x \in X\}$$

È infatti immediato verificare che la relazione Id_X è in realtà una relazione di equivalenza, vale a dire è una relazione *riflessiva*, *simmetrica* e *transitiva*, ma la cosa più interessante è il fatto che queste proprietà sono caratteristiche di una relazione di identità nel senso che data una qualsiasi relazione di equivalenza noi possiamo sempre costruire un opportuno insieme su cui tale relazione di equivalenza permette di definire una relazione di identità.

Per mostrare questo importante risultato introduciamo prima di tutto la nozione di *partizione* di un insieme.

Definizione 3.4 (Partizione) *Sia X un insieme. Allora una partizione su X è un insieme I di sottoinsiemi di X tali che*

- *per ogni $Y \in I$, $Y \neq \emptyset$*
- $X = \bigcup_{Y \in I} Y$
- *se Y e Z sono due elementi di I tali che $Y \neq Z$ allora $Y \cap Z = \emptyset$*

Intuitivamente, una partizione di un insieme X è quindi una maniera di dividere X in pezzi separati non vuoti. Infatti la terza condizione sostiene che o due pezzi sono uguali o sono disgiunti. Per di più, dato un qualsiasi elemento $x \in X$, in virtù della seconda e della terza condizione, possiamo sempre individuare quell'unico elemento $Y_x \in I$ tale che $x \in Y_x$.

Ora è immediato verificare che una partizione I su un insieme X determina sempre una relazione di equivalenza R_I tra gli elementi di X definita ponendo, per ogni $x, y \in X$:

$$x\ R_I\ y \equiv y \in Y_x$$

vale a dire che $x\ R_I\ y$ vale se e solo se x e y appartengono allo stesso elemento della partizione I (verificare per esercizio che R è una relazione di equivalenza).

La cosa più interessante è però che anche una relazione di equivalenza determina una partizione, vale a dire che partizioni e relazioni di equivalenza sono due modi diversi di parlare della stessa cosa.

Definizione 3.5 (Classe di equivalenza) *Sia R una relazione di equivalenza su un insieme X e sia x un elemento di X. Allora la* classe di equivalenza *di x è il sottoinsieme di X definito da*

$$[x]_R \equiv \{y \in X \mid x\ R\ y\}$$

Possiamo allora dimostrare il seguente teorema.

Teorema 3.6 *Sia R una relazione di equivalenza sull'insieme X. Allora l'insieme*

$$X/R \equiv \{[x]_R \mid x \in X\}$$

delle classi di equivalenza di R è una partizione su X.

Dimostrazione. La prima cosa da osservare è che $\{[x]_R \mid x \in X\}$ è un insieme in quanto, per ogni $x \in X$, $[x]_R$ è un insieme, in quanto sottoinsieme di X, e quindi il principio di buona fondazione ci assicura che non corriamo nessun rischio (si veda comunque il prossimo paragrafo dove vedremo che la collezione $\mathcal{P}(X)$ di tutti i sottoinsiemi di un dato insieme X è un insieme; in virtù dell'assioma del sottoinsieme, questo fatto chiaramente significa che $\{[x]_R \mid x \in X\}$ è un insieme in quanto sottoinsieme di $\mathcal{P}(X)$).

Osserviamo ora che, in virtù della *riflessività* di R, nessuna classe di equivalenza è vuota in quanto, per ogni $x \in X$, $x \in [x]_R$.

Come conseguenza di quanto appena detto si vede subito che ogni elemento di X appartiene ad una qualche classe di equivalenza, vale a dire la *sua* classe di equivalenza, e quindi l'unione di tutte le classi di equivalenza è sicuramente uguale ad X.

Consideriamo ora due classi di equivalenza $[x]_R$ e $[y]_R$. Dobbiamo allora fare vedere che o $[x]_R = [y]_R$ o $[x]_R \cap [y]_R = \emptyset$. Supponiamo allora che $[x]_R \cap [y]_R \neq \emptyset$. Allora esiste un elemento $z \in X$ tale che $z \in [x]_R$ e $z \in [y]_R$, vale a dire che $x\ R\ z$ e $y\ R\ z$. Ma allora $z\ R\ y$ segue per *simmetria* e quindi si ottiene $x\ R\ y$ per *transitività*.

A conferma che partizioni e relazioni di equivalenza sono due modi alternativi di presentare lo stesso concetto, non è difficile vedere che le due costruzioni che abbiamo proposto sono una l'inversa dell'altra. Infatti se R è una relazione di equivalenza, I_R è la partizione associata ad R e R_{I_R} la relazione di equivalenza associata alla partizione I_R, allora, per ogni $x, y \in X$,

$$\begin{array}{rll} x\ R_{I_R}\ y & \text{sse} & y \in [x]_R \\ & \text{sse} & x\ R\ y \end{array}$$

D'altra parte, per ogni partizione I, la partizione I_{R_I} associata alla relazione di equivalenza R_I associata ad I coincide con la partizione I stessa. Infatti, per ogni $Y \subseteq X$,

$$\begin{array}{rll} Y \in I_{R_I} & \text{sse} & (\exists x \in X)\ Y = [x]_{R_I} \\ & \text{sse} & (\exists x \in X)\ Y = \{z \in X \mid x\ R_I\ z\} \\ & \text{sse} & (\exists x \in X)\ Y = \{z \in X \mid z \in Y_x\} \\ & \text{sse} & (\exists x \in X)\ Y = Y_x \\ & \text{sse} & Y \in I \end{array}$$

È ora possibile vedere che data una relazione di equivalenza R su un insieme X essa induce una relazione identica sull'insieme X/R. Infatti possiamo porre, per ogni coppia di elementi $[x]_R, [y]_R \in X/R$,

$$[x]_R\ \mathsf{Id}_{X/R}\ [y]_R \equiv x\ R\ y$$

Dobbiamo ora verificare che questa è una *buona definizione*, cioé una definizione corretta che non dipende dai particolari rappresentanti usati nelle classi di equivalenze. Supponiamo quindi che $[x_1]_R = [x_2]_R$ e $[y_1]_R = [y_2]_R$. Allora ricaviamo subito che $x_1\ R\ x_2$ e $y_1\ R\ y_2$. Se ora supponiamo che $[x_1]_R\ \mathsf{Id}_{X/R}\ [y_1]_R$ otteniamo subito che $x_1\ R\ y_1$ e quindi, utilizzando le proprietà *simmetrica* e *transitiva* della relazione R, si vede immediatamente che $x_2\ R\ y_2$ e naturalmente questo implica che $[x_2]_R\ \mathsf{Id}_{X/R}\ [y_2]_R$. Adesso è immediato verificare che $\mathsf{Id}_{X/R}$ è una relazione di identità, vale a dire che se $[x]_R\ \mathsf{Id}_{X/R}\ [y]_R$ allora $[x]_R = [y]_R$. Infatti $[x]_R\ \mathsf{Id}_{X/R}\ [y]_R$ significa che $x\ R\ y$ che vuol dire appunto che $[x]_R = [y]_R$.

Esercizi

1. Sia X un insieme e I sia una sua partizione. Verificare che la relazione R_I definita ponendo
$$x\, R_I\, y \equiv (Y_x = Y_y)$$
è una relazione di equivalenza.

2. Considerate l'insieme dei numeri interi. Possiamo farne una partizione considerando il sottoinsieme di tutti i numeri positivi, il sottoinsieme costituito dal solo numero 0 e il sottoinsieme costituito da tutti i numeri negativi. Trovare la relazione di equivalenza che corrisponde a tale partizione.

3. Considerate la relazione di equivalenza che considera uguali due ore x e y quando esse differiscono per un multiplo di 12 ore, vale a dire quando esiste un numero intero k tale che $x - y = 12 * k$. Quali e quante sono le classi di equivalenza associate a tale relazione?

4. (Costruzione dei numeri interi) Si supponga di voler costruire un insieme che possa essere identificato come l'insieme dei numeri interi pur avendo a disposizione, come nel nostro caso, solamente i numeri naturali. Possiamo allora indicare l'intero i tramite una coppia (m, n) di numeri naturali tali che, *se fossimo in grado di fare sempre la sottrazione tra due numeri naturali*, $i = m-n$. Naturalmente questo approccio soffre di due problemi: senza gli interi *non* possiamo fare sempre la sottrazione tra due numeri naturali e, inoltre, lo stesso intero viene ad essere rappresentato da infinite coppie di numeri naturali.

   Per risolvere entrambi questi problemi possiamo considerare sull'insieme $\omega \times \omega$ delle coppie ordinate di numeri naturali consideriamo la seguente relazione
   $$\langle m, n\rangle \cong \langle p, q\rangle \equiv (m + q) = (p + n)$$
   Dimostrare che $\cong$ è una relazione di equivalenza sull'insieme $\omega \times \omega$.

   Possiamo ora considerare l'insieme delle classi di equivalenza $\omega \times \omega/ \cong$ come l'insieme Z degli interi.

   Infatti all'interno di Z possiamo facilmente ritrovare una copia dei numeri naturali se al numero naturale n associamo la classe di equivalenza determinata dalla coppia $\langle n, 0\rangle$, ma possiamo anche trovare i *numeri negativi* visto che possiamo rappresentare il *vecchio* numero intero $-n$ tramite la classe di equivalenza il cui rappresentante è $\langle 0, n\rangle$.

   Inoltre possiamo definire su Z la usuale operazione di somma ponendo
   $$[\langle m, n\rangle]_{\cong} + [\langle p, q\rangle]_{\cong} \equiv [\langle m + p, n + q\rangle]_{\cong}$$
   Verificare che si tratta di una *buona definizione* che non dipende dai rappresentanti usati.

   La novità rispetto al caso dei numeri naturali è che su Z possiamo finalmente definire anche la sottrazione ponendo
   $$[\langle m, n\rangle]_{\cong} - [\langle p, q\rangle]_{\cong} \equiv [\langle m + q, n + p\rangle]_{\cong}$$
   Si verifichi anche in questo caso che si tratta di una buona definizione e che
   $$[\langle m, 0\rangle]_{\cong} - [\langle n, 0\rangle]_{\cong} \equiv [\langle m, n\rangle]_{\cong}$$

5. Sulla falsariga dell'esercizio precedente fornire una costruzione per l'insieme Q dei numeri razionali. (sugg.: non scordatevi delle frazioni!)

3.2 Funzioni

Lo scopo principale di questa sezione è la definizione del concetto di funzione. Dopo aver introdotto nella sezione precedente le relazioni possiamo utilizzarle per scegliere al loro interno le particolari relazioni che sono funzioni.

Definizione 3.7 *Siano X e Y due insiemi. Allora una relazione $R \subseteq X \times Y$ è una funzione se e solo se, per ogni $x \in X$, se $\langle x, y\rangle \in R$ e $\langle x, z\rangle \in R$ allora $y = z$.*

Un'attenta lettura della precedente definizione rivela che le funzioni sono quelle relazioni da X ad Y tali che un elemento x dell'insieme X di partenza (nel seguito X sarà chiamato anche *dominio della funzione*) è in relazione con al più con un solo elemento y dell'insieme Y di arrivo (nel seguito Y sarà chiamato anche *codominio della funzione*). Questo fatto si può anche esprimere sostenendo che la scelta di x *determina* la scelta di y, vale a dire che il valore di y è *funzione* di x. Il fatto che ci sia al più un solo elemento $y \in Y$ che è in relazione con $x \in X$ ci permette di semplificare un po' la notazione per le funzioni rispetto a quella per le relazioni. Infatti, potremo scrivere $R(x) = y$ al posto di $\langle x, y\rangle \in R$ e dire che y è l'*immagine* di x tramite la funzione R.

3.2.1 Proprietà delle funzioni

Così come nel caso delle relazioni abbiamo individuato delle proprietà particolari di cui una relazione può godere, e abbiamo deciso una volta per tutte i nomi di tali proprietà, conviene fare qualcosa di analogo anche nel caso delle funzioni.

Definizione 3.8 (Funzione totale) *Siano X e Y due insiemi e sia f una funzione da X a Y. Allora diremo che f è una funzione* totale *se, per ogni $x \in X$, esiste un $y \in Y$, e quindi uno solo, tale che la coppia ordinata $\langle x, y\rangle$ appartiene ad f, vale a dire se la funzione f è definita per ogni elemento del dominio.*

Definizione 3.9 (Funzione iniettiva) *Siano X e Y due insiemi e sia f una funzione da X a Y. Allora diremo che f è una funzione* iniettiva *se accade che elementi distinti di X hanno immagini distinte, vale a dire se ogni volta che un elemento $y \in Y$ è immagine di un qualche elemento $x \in X$ tale x è unico, vale a dire che se $\langle x_1, y\rangle \in f$ e $\langle x_2, y\rangle \in f$ allora $x_1 = x_2$.*

Definizione 3.10 (Funzione suriettiva) *Siano X e Y due insiemi e sia f una funzione da X a Y. Allora diremo che f è una funzione* suriettiva *se accade che ogni elemento di Y è immagine di un qualche elemento di X.*

Definizione 3.11 (Funzione biettiva) *Siano X e Y due insiemi e sia f una funzione da X a Y. Allora diremo che f è una funzione* biettiva *se f è sia iniettiva che suriettiva.*

Definizione 3.12 (Immagine diretta) *Siano X e Y due insiemi e sia f una funzione da X a Y. Allora chiameremo* immagine diretta

$$f(U) \equiv \{y \in Y \mid esiste\ x \in U\ tale\ che\ y = f(x)\}$$

Definizione 3.13 (Immagine inversa) *Siano X e Y due insiemi e sia f una funzione da X ad Y. Allora chiameremo* immagine inversa

$$f^{-1}(V) \equiv \{x \in X \mid esiste\ y \in V\ tale\ che\ y = f(x)\}$$

Definizione 3.14 (Funzione inversa) *Siano X e Y due insiemi e sia f una funzione iniettiva da X ad Y. Allora chiameremo* funzione inversa *di f la relazione opposta f^-.*

Definizione 3.15 (Composizione di relazioni e di funzioni) *Siano X, Y e Z tre insiemi e R sia una relazione tra X e Y e S sia una relazione tra Y e Z. Allora possiamo definire la composizione di R ed S ponendo*

$$S \circ R \equiv \{\langle x, z\rangle \in X \times Z \mid esiste\ y \in Y\ tale\ che\ \langle x, y\rangle \in R\ e\ \langle y, z\rangle \in S\}$$

(si legge S dopo *R).*

Vale la pena di notare che la funzione inversa di una funzione totale può essere non totale. Tuttavia nel caso in cui la funzione f sia non solo iniettiva ma anche suriettiva abbiamo che la funzione f^{-1} è pure una funzione biettiva e $f \circ f^{-1} = \mathsf{id}_X$ e $f^{-1} \circ f = \mathsf{id}_Y$

Esercizi

1. Fornire un esempio di una funzione totale, di una funzione iniettiva, di una funzione suriettiva e di una funzione biettiva.

2. Dimostrare che la composizione di relazioni è una operazione associativa, vale a dire dimostrare che se f è una funzione da X verso Y, g è una funzione da Y verso W e h è una funzione da W verso Z allora

$$(h \circ g) \circ f = h \circ (g \circ f)$$

3. Dimostrare che la relazione identica è l'identità per l'operazione di composizione.

4. Siano X e Y due insiemi e sia f una funzione da X verso Y. Dimostrare che

   - $f(U_1 \cup U_2) = f(U_1) \cup f(U_2)$
   - $f(U_1 \cap U_2) \subseteq f(U_1) \cap f(U_2)$
     Trovare un controesempio alla inclusione mancante.
   - $f^-(V_1 \cup V_2) = f^-(V_1) \cup f^-(V_2)$
   - $f^-(V_1 \cap V_2) = f^-(V_1) \cap f^-(V_2)$

3.2.2 Costruzione dei numeri reali

A differenza dei numeri interi e dei numeri razionali che si possono sempre presentare utilizzando una quantità finita di informazione, vale a dire una coppia di numeri naturali, ogni numero reale richiede di specificare una quantità infinita di informazione, vale a dire, ad esempio, tutte le infinite cifre di una sua espansione decimale. I primi oggetti che possono racchiudere tutta questa informazione in un solo insieme sono le relazioni e le funzione; questo è il motivo per cui useremo particolari insiemi di funzioni per rappresentare i numeri reali all'interno della teoria degli insiemi.

L'intuizione che sta alla base della particolare scelta che faremo è che possiamo specificare un numero reale r se specifichiamo tutte le sue approssimazioni decimali, vale a dire, supponendo che

$$r \equiv n, n_0 n_1 n_2 n_3 \dots$$

dove n è la parte intera di r e n_0, n_1, n_2 sono le varie cifre decimali, noi possiamo specificare la seguente *successione* di numeri razionali

$$\begin{array}{rcl} q_0 & \equiv & n, n_0 \\ q_1 & \equiv & n, n_0 n_1 \\ q_2 & \equiv & n, n_0 n_1 n_2 \\ \dots & & \end{array}$$

Ora, una successione di numeri naturali altro non è che una funzione

$$r : \omega \to Q$$

Naturalmente, il problema è che non tutte le funzioni da ω in Q possono rappresentare un numero reale ma vanno bene solo le successioni che *convergono.* Tra tutte le funzioni da ω in Q dobbiamo quindi scegliere solo quelle i cui valori, da un certo punto in poi, siano tra loro tanto vicini di una qualsiasi distanza decisa a priori (formalmente possiamo esprimere questa condizione dicendo che una funzione $r : \omega \to Q$ è un numero reale se accade che, fissato un qualsiasi $\epsilon \in Q$ esiste un $M \in \omega$ tale che, per ogni $n_1, n_2 \in \omega$ che siano maggiori di M accade che $|q_{n_1} - q_{n_2}| \leq \epsilon$).

Purtroppo non siamo ancora arrivati in fondo con la nostra costruzione. Considerate infatti le due successioni seguenti:

$$\begin{array}{rcl} r_1 & \equiv & 0 \; \frac{1}{2} \; \frac{3}{4} \; \frac{7}{8} \; \dots \\ r_2 & \equiv & 0 \; \frac{3}{2} \; \frac{3}{4} \; \frac{9}{8} \; \dots \end{array}$$

Si tratta chiaramente di due successioni diverse ma non è difficile convincersi che sono entrambi convergenti a 1. Siamo cioé nella solita situazione in cui abbiamo più modi diversi per denotare lo stesso oggetto (ad esempio avevamo molte coppie di numeri naturali che denotavano lo stesso numero intero o molte coppie di frazioni che denotavano lo stesso numero razionale). La soluzione è quindi la solita: i numeri reali non saranno semplicemente l'insieme delle funzioni dai naturali ai razionali che convergono ma piuttosto le classi di equivalenza su tale insieme di funzioni determinate dalla relazione di equivalenza che pone equivalenti due funzioni convergenti quando convergono allo stesso valore (formalmente, le funzioni convergenti r_1 e r_2 da ω verso Q sono in relazione se accade che, fissato un qualsiasi $\epsilon \in Q$ esiste un $M \in \omega$ tale che, per ogni $n \in \omega$ maggiore di M accade che $|q_n^{r_1} - q_n^{r_2}| \leq \epsilon$).

Esercizi

1. Dimostrare che la relazione sopra definita tra funzioni convergenti è una relazione di equivalenza
2. Definire le usuali operazioni tra numeri reali.
3. Definire la relazione d'ordine sui numeri reali.
4. Definire la radice quadrata di un numero reale

3.2.3 Grafico di una funzione

Visto che una funzione altro non è che una speciale relazione il grafico di una funzione è semplicemente un caso speciale del grafico di una relazione. Tuttavia, visto l'ampio spettro di applicazioni, lo studio dei grafici delle funzioni costituirà tuttavia un grosso capitolo dei vostri studi futuri per cui non si ritiene necessario insistere fin da ora sull'argomento.

Esercizi

1. Si consideri la seguente funzione f dall'insieme Q dei numeri razionali verso l'insieme Z dei numeri interi

   $$f \equiv \{\langle x, y\rangle \in Q \times Z \mid \begin{array}{l} y \text{ è uguale ad } x \text{ o è il numero} \\ \text{intero immediatamente minore a } x\} \end{array}$$

   (f si chiama la funzione *parte intera*)

   Se ne tracci il grafico.

2. Si tracci il grafico della seguente funzione f dall'insieme Q verso se stesso

   $$f \equiv \{\langle x, y\rangle \in Q \times Q \mid y = x + 1\}$$

4 Insiemi induttivi non numerici

Nei precedenti paragrafi abbiamo visto come costruire i naturali e, a partire da essi, tutti gli altri insiemi numerici. I naturali non sono tuttavia l'unico esempio di insieme che riusciamo a costruire tramite una definizione induttiva. Infatti, in questo capitolo vogliamo introdurre altri esempi di insiemi definiti tramite un processo induttivo. Essi saranno utili nel seguito dei vostri studi anche se non si tratta di insieme numerici.

4.1 Liste

Il prossimo esempio di insieme induttivo che vogliamo introdurre è una semplice generalizzazione dell'insieme dei numeri naturali. Se analizziamo la definizione induttiva dei numeri naturali ci possiamo infatti rendere conto che possiamo darne una rappresentazione della seguente forma

$$0, 0I, 0II, 0III, \ldots$$

vale a dire che, a partire da 0, possiamo ottenere un generico numero naturale aggiungendo un nuovo I alla destra di qualcosa che sia stato già costruito come numero naturale. Possiamo allora generalizzare questa costruzione se invece che aggiungere sempre lo stesso simbolo I aggiungiamo un simbolo preso da un insieme fissato di simboli. Ad esempio se consideriamo l'insieme delle lettere dell'alfabeto e sostituiamo lo 0 con un simbolo bianco, che indicheremo con nil, otteniamo l'insieme delle *parole*, vale a dire le liste finite di lettere. I numeri naturali sono quindi le parole che si possono scrivere usando un unica lettera.

Definizione 4.1 (Liste su un insieme) *Sia A un insieme. Allora indicheremo con $\mathsf{List}(A)$ l'insieme i cui elementi sono le* parole *ottenute utilizzando gli elementi di A come* lettere*, vale a dire che gli elementi di $\mathsf{List}(A)$ sono i seguenti:*

- *(Base) nil è un elemento di $\mathsf{List}(A)$;*
- *(Passo) Se l è un elemento di $\mathsf{List}(A)$ e a è un elemento di A allora $l \cdot a$ è un elemento di $\mathsf{List}(A)$.*

Visto che l'insieme delle liste nasce tramite una definizione induttiva è immediato pensare ad una generalizzazione della proprietà di induzione per dimostrare proprietà sui suoi elementi.

Definizione 4.2 (Induzione sulle liste) *Sia A un insieme e sia $\mathsf{List}(A)$ l'insieme delle liste sull'insieme A. Sia inoltre $P(-)$ una proprietà sugli elementi dell'insieme $\mathsf{List}(A)$. Allora per dimostrare che $P(-)$ vale per ogni lista l basta dimostrare che vale $P(\mathsf{nil})$ e che se vale $P(l)$ allora vale anche $P(l \cdot a)$ per ogni elemento $a \in A$.*

Esercizi

1. Sia A un insieme. Si definisca la funzione length che data una lista l di $\mathsf{List}(A)$ ne fornisce la lunghezza (si noti che $\mathsf{length}(\mathsf{nil}) = 0$).

2. Si consideri la segunte definizione di una funzione sulle coppie di liste l_1 e l_2 di $\mathsf{List}(A)$ il cui intento è quello di fornire la lista ottenuta concatenando l_1 e l_2

$$\begin{cases} \mathsf{append}(m, \mathsf{nil}) & = & m \\ \mathsf{append}(m, l \cdot a) & = & \mathsf{append}(m, l) \cdot a \end{cases}$$

Dimostrare per induzione che, per ogni coppia di liste l_1 e l_2,

$$\mathsf{lenght}(\mathsf{append}(l_1, l_2)) = \mathsf{lenght}(l_1) + \mathsf{lenght}(l_2)$$

3. Si consideri la seguente funzione sugli elementi di $\mathsf{List}(A)$ che presa una lista l fornisce la lista opposta di l.

$$\begin{cases} \mathsf{reverse}(\mathsf{nil}) & = & \mathsf{nil} \\ \mathsf{reverse}(l \cdot a) & = & \mathsf{append}(a \cdot \mathsf{nil}, \mathsf{reverse}(l)) \end{cases}$$

   Dimostrare che, per ogni lista l,

$$\mathsf{length}(l) = \mathsf{lenght}(\mathsf{reverse}(l))$$

4. Definire una funzione norep che data una lista l di $\mathsf{List}(A)$ fornisce una nuova lista in cui nessuna *lettera* appare due volte.

5. Verificare che la seguente funzione $\mathsf{ord}(-) : \mathsf{List}(\omega) \rightarrow \mathsf{List}(\omega)$ quando applicata ad una lista di numeri naturali fornisce una lista ordinata che contiene gli stessi elementi:

$$\begin{cases} \mathsf{ord}(\mathsf{nil}) & = & \mathsf{nil} \\ \mathsf{ord}(l \cdot a) & = & \mathsf{insert}(a, \mathsf{ord}(l)) \end{cases}$$

$$\begin{cases} \mathsf{insert}(a, \mathsf{nil}) & = & \mathsf{nil} \cdot a \\ \mathsf{insert}(a, l \cdot b) & = & \mathsf{if}\ b \leq a\ \mathsf{then}\ l \cdot b \cdot a\ \mathsf{else}\ \mathsf{insert}(a, l) \cdot b \end{cases}$$

4.2 Alberi

Un altro esempio di insieme induttivo, notevolmente più complesso del precedente, sono gli alberi. In queste note ci limiteremo a considerare gli *alberi binari* che risultano comunque notevoli per la ricchezza delle loro applicazioni. Come al solito dobbiamo cominciare con una definizione induttiva degli elementi dell'insieme degli alberi binari.

Definizione 4.3 (Alberi binari) *Sia A un insieme. Allora gli elementi di* $\mathsf{BinTree}(A)$ *sono i seguenti:*

- *(Base) se a è un elemento di A allora* $\mathsf{leaf}(a)$ *è un elemento di* $\mathsf{BinTree}(A)$*;*
- *(Passo) se t_1 e t_2 sono due elementi di* $\mathsf{BinTree}(A)$ *allora (t_1, t_2) è un elemento di* $\mathsf{BinTree}(A)$

Può essere utile osservare che in letteratura si incontrano molte altre definizioni sostanzialmente analoghe del concetto di albero binario.

Esercizi

1. Definire la funzione $\mathsf{depth}(-)$ che dato un albero binario b ne fornisce la profondità, vale a dire la lunghezza del ramo più lungo.

5 Cardinalità

È immediato rendersi conto che il principio di buona fondatezza ci assicura che possiamo riconoscere come insieme anche la collezione di tutti i sottoinsiemi di un qualunque insieme.

Definizione 5.1 (Assioma delle parti) *Sia X un insieme. Allora la collezione di tutti i sottoinsiemi di X è un insieme che chiameremo* potenza *dell'insieme X e indicheremo con $\mathcal{P}(X)$.*

Infatti, per l'assioma del sottoinsieme, ogni sottoinsieme Y di X è a sua volta un insieme e quindi la collezione $\mathcal{P}(X)$ è formata solo da elementi che abbiamo già riconosciuto come insiemi nel momento in cui essa viene formata. Bisogna tuttavia ammettere che se l'insieme X è infinito, come ad esempio ω, il processo di riconoscimento di tutti i sottoinsiemi sembra proprio essere tutto meno che effettivo!

Ora, supponiamo che X sia un insieme finito e indichiamo con $|X|$ il numero di elementi di X, che chiameremo *cardinalità* dell'insieme X. È allora facile dimostrare, usando ad esempio il principio di induzione, che se $|X| = n$ allora $|\mathcal{P}(X)| = 2^n$. Ma cosa succede nel caso X non sia un insieme con un numero finito di elementi? È facile convincersi che anche $\mathcal{P}(X)$ conterrà un insieme non finito di elementi, ma quanti sono? Sono tanti quanti gli elementi in X? Sono di più come accade nel caso in cui X sia un insieme finito? Per rispondere a queste domande è necessario prima di tutto chiarire cosa si deva intendere in generale con l'operazione di contare il numero di elementi di un insieme.

L'idea generale è quella di rifarsi al modo di contare dei bambini che contano sulle dita, ricordandosi però che noi abbiamo mani con infinite dita! Quello che faremo per contare non sarà cioè, in prima istanza, lo scoprire quanti elementi compaiono in un insieme ma cercheremo piuttosto di capire quando due insiemi abbiano lo stesso numero di elementi. Poi, nello stesso modo di un bambino, diremo che ci sono cinque oggetti quando ci sono tanti oggetti quante sono le dita di una sola mano.

In realtà, abbiamo già predisposto tutto quello che ci serve per risolvere questo primo problema almeno nel caso degli insiemi con un numero finito di elementi. In questo caso infatti due insiemi hanno lo stesso numero di elementi esattamente quando esiste una funzione totale e biettiva dal primo insieme verso il secondo. Infatti, supponiamo di avere due insiemi finiti X e Y e supponiamo che Y abbia meno elementi di X; allora è impossibile definire una funzione tra X e Y che sia totale e iniettiva. D'altra parte se supponiamo che X abbia meno elementi di Y è impossibile definire tra X e Y una funzione che sia suriettiva. Quindi, nel caso stiamo considerando due insiemi finiti per vedere se essi hanno lo stesso numero di elementi possiamo provare a trovare una funzione totale e biettiva dal primo al secondo. Il trucco consiste ora nell'usare lo stesso test come definizione del fatto che due insiemi, anche non finiti, hanno lo stesso numero di elementi.

Definizione 5.2 (Equinumerosità) *Siano X e Y due insiemi. Allora diremo* *che X e Y sono* equinumerosi *se e solo se esiste una funzione totale e biettiva da X verso Y.*

In questo modo siamo riusciti ad avere una nozione di equinumerosità tra due insiemi che non richiede di parlare del numero di elementi di un insieme che è una nozione chiaramente problematica, almeno per quanto riguarda gli insiemi con un numero non finito di elementi.

5.1 Insiemi numerabili

Bisogna però notare subito che questa nozione di equinumerosità produce talvolta risultati inaspettati. Ad esempio, una sua conseguenza immediata è il fatto che l'insieme P dei numeri pari risulta equinumeroso con l'insieme ω dei numeri naturali visto che possiamo definire la seguente mappa double da ω verso P

$$\mathsf{double}(n) \equiv 2n$$

che è chiaramente totale e biettiva. Abbiamo cioé ottenuto che l'insieme dei numeri naturale è equinumeroso con un suo sottoinsieme proprio! Naturalmente questo non dovrebbe stupirci più che tanto visto che nessuno può garantire che una nozione di equinumerosità tra due insiemi, che nel caso tali insiemi siano finiti significa che essi hanno lo stesso numero di elementi e quindi esclude che un insieme finito possa avere lo stesso numero di elementi di un suo sottoinsieme proprio, preservi per intero il suo significato quando essa viene utilizzata su insiemi che finiti non sono. Potremo invece approfittare di questa mancanza di uniformità della nozione di equinumeroso per distinguere gli insiemi finiti da quelli che finiti non sono.

Definizione 5.3 (Insiemi finiti e infiniti) *Sia X un insieme. Allora diremo che X è in* insieme infinito *se esso è equinumeroso con una sua parte propria. Diremo invece che X è un* insieme finito *quando esso non è infinito.*

Non è difficile accorgersi che anche l'insieme dei numeri interi è equinumeroso con l'insieme dei numeri naturali. Infatti possiamo utilizzare la seguente mappa $\mathsf{Nat2Int}$

$$\mathsf{Nat2Int}(n) = (-1)^n \lfloor \frac{n+1}{2} \rfloor$$

dove $\lfloor q \rfloor$ rappresenta la parte intera del numero razionale q, che risulta evidentemente totale e biettiva.

Un po' più sorprendente è forse il fatto che anche l'insieme delle frazioni, tramite le quali è possibile dare un nome a tutti numeri razionali (in realtà infiniti nomi per ciascun numero razionale!), è equinumeroso con l'insieme dei numeri naturali. In generale, se trascuriamo il problema delle frazioni con denominatore nullo, possiamo pensare ad una frazione come ad una coppia ordinata di numeri naturali. Dobbiamo quindi trovare una mappa totale e biettiva dall'insieme dei numeri naturali all'insieme delle coppie ordinate di numeri naturali. In pratica è più facile risolvere il problema nell'altra direzione, vale a dire definire una mappa totale è biettiva dall'insieme delle coppie ordinate di numeri naturali verso l'insieme dei numeri naturali. È facile rendersi conto che vale il seguente lemma e quindi trovare questa mappa è completamente equivalente a trovarne una dall'insieme dei numeri naturali all'insieme delle coppie.

Lemma 5.4 *Siano X e Y due insiemi e sia f una mappa totale e biettiva da X a Y. Allora è possibile definire una mappa totale e biettiva da Y a X.*

Dimostrazione. Si definisca la mappa g da Y a X nel modo seguente:

$$\langle y, x\rangle \in g \equiv \langle x, y\rangle \in f$$

L'idea è naturalmente che la mappa g associa ad $y \in Y$ quell'unico elemento $x \in X$ tale che $f(x) = y$. Dobbiamo allora dimostrare tre cose: prima di tutto bisogna far vedere che g è davvero una funzione, poi che si tratta di una funzione totale e infine che è una funzione biettiva.

- (buona definizione) Supponiamo che sia $\langle y, x_1\rangle$ che $\langle y, x_2\rangle$ siano elementi di g. Allora dobbiamo dimostrare che $x_1 = x_2$. Ma noi sappiamo che se $\langle y, x_1\rangle \in g$ allora $\langle x_1, y\rangle \in f$ e che se $\langle y, x_2\rangle \in g$ allora $\langle x_2, y\rangle \in f$. Ma allora, visto che f è iniettiva in quanto biettiva, $x_1 = x_2$.

- (totalità) Bisogna dimostrare che, per ogni elemento $y \in Y$ esiste un $x \in X$ tale che $\langle y, x\rangle \in g$. Ma noi sappiamo che affinché questo accada basta che, per ogni elemento $y \in Y$ esiste un $x \in X$ tale che $\langle x, y\rangle \in f$ che vale visto che f è suriettiva in quanto biettiva.

- (biettività) Dobbiamo dimostrare che g è sia iniettiva che suriettiva. Dimostrare l'iniettività significa far vedere che se $\langle y_1, x\rangle$ e $\langle y_2, x\rangle$ sono elementi di g allora $y_1 = y_2$. Ora $\langle y_1, x\rangle \in g$ implica che $\langle x, y_1\rangle \in f$ e $\langle y_2, x\rangle \in g$ implica che $\langle x, y_2\rangle \in f$. Ma allora otteniamo immediatamente che $y_1 = y_2$ visto che f è una funzione. Per quanto riguarda la suriettività di g, dobbiamo dimostrare che per ogni $x \in X$ esiste un $y \in Y$ tale che $\langle y, x\rangle \in g$. Ora per dimostrare questo risultato basta far vedere che per ogni $x \in X$ esiste un $y \in Y$ tale che $\langle x, y\rangle \in f$ che è una immediata conseguenza della totalità di f.

Possiamo ora risolvere il nostro problema originale esibendo una mappa totale e biettiva che fornisce un numero naturale in corrispondenza di ogni coppia ordinata di numeri naturali:

$$\mathsf{Pair2Nat}(\langle x, y\rangle) \equiv \frac{1}{2}(x + y)(x + y + 1) + x$$

Sebbene il risultato non sia immediato si può dimostrare che $\mathsf{Pair2Nat}(-)$ gode delle proprietà richieste.

5.2 Insiemi più che numerabili

Dopo aver visto che i numeri razionali non sono di più che i numeri naturali può forse risultare sorprendente il fatto che non tutti gli insiemi infiniti sono equinumerosi. Infatti con un argomento dovuto a Cantor, e che useremo spesso nel seguito, possiamo far vedere che l'insieme dei sottoinsiemi dei numeri naturali non è equinumeroso con l'insieme dei numeri naturali. È ovvio che per dimostrare questo risultato basta far vedere che ogni funzione dall'insieme ω verso l'insieme $\mathcal{P}(\omega)$ non è suriettiva.

Teorema 5.5 (Teorema di Cantor) *Ogni funzione f da ω a $\mathcal{P}(\omega)$ non è suriettiva.*

Dimostrazione. Basta far vedere che esiste un sottoinsieme di numeri naturali che non è immagine secondo f di nessun numero naturale. È ovvio che tale sottoinsieme dipende dalla funzione f che stiamo considerando. Una possibile scelta è la seguente

$$U_f \equiv \{n \in \omega \mid n \notin f(n)\}$$

Non dovrebbe essere difficile riconoscere nella definizione del sottoinsieme U_f una forte analogia con il paradosso di Russell, ma questa volta la stessa idea, la *diagonalizzazione*, viene utilizzata per definire il sottoinsieme che goda della proprietà richiesta invece che per trovare una contraddizione. Tuttavia il metodo è analogo: faremo infatti vedere che l'ipotesi che U_f sia nell'immagine di f porta a contraddizione e quindi la funzione f non può essere suriettiva. Supponiamo infatti che esista un numero naturale n tale che $U_f = f(n)$. Allora, $n \in f(n)$ se e solo se $n \in U_f$ e quindi, per definizione di U_f, se e solo se $n \notin f(n)$, cioè abbiamo ottenuto una contraddizione.

Esercizi

1. Siano X e Y due insiemi tali che $|X| = n$ e $|Y| = m$. Determinare il numero degli elementi di $X \times Y$. Quante sono le relazioni tra X e Y? Quante sono le funzioni iniettive da X a Y? (Difficile) Quante sono le funzioni tra X e Y?

2. Sia X un insieme con n elementi. Allora l'insieme $\mathcal{P}(X)$ ha 2^n elementi.

3. Dimostrare che la funzione

$$\mathsf{Nat2Int}(n) = (-1)^n \lfloor \frac{n+1}{2} \rfloor$$

che manda un numero naturale in un numero intero è totale e biettiva.

4. (Difficile) Dimostrare che la funzione

$$\mathsf{Pair2Nat}(\langle x, y\rangle) \equiv \frac{1}{2}(x+y)(x+y+1) + x$$

che mappa una coppia ordinata di numeri naturali in un numero naturale è totale e biettiva.

5. Dimostrare che l'insieme F delle funzioni totali da ω a ω è un insieme più che numerabile. (sugg.: supponete che $\phi(-)$ sia una funzione da ω verso F e dimostrate che $\phi(-)$ non può essere suriettiva; infatti, basta definire una funzione $f_\phi(-)$ da ω a ω ponendo $f_\phi(n) = \phi(n)(n) + 1$ per ottenere una funzione totale da ω a ω tale che ...)

6. Dimostrare che l'insieme dei numeri reali compresi tra 0 e 1 è più che numerabile. (sugg.: supponete che $\phi(-)$ sia una funzione da ω verso $[0,1]$ e dimostrate che $\phi(-)$ non può essere suriettiva; infatti, basta definire una funzione $f_\phi(-)$ da ω a ω che fornisce le varie cifre decimali di un numero reale r ponendo $f_\phi(n) = (\phi(n)[n]+1) \mathsf{mod}\ 10$, dove con $\phi(n)[n]$ intendiamo la n-ma cifra decimale del numero reale $\phi(n)$ e dimostrare che r non può essere nell'immagine di $\phi(-)$)

6 Contare

Per *calcolo combinatorio* si intende quella branca della Matematica che studia i modi di raggruppare ed ordinare oggetti presi da un insieme assegnato, con l'obiettivo finale di contare il numero dei possibili raggruppamenti od ordinamenti.

6.1 Il principio generale del calcolo combinatorio

Cominciamo con un semplice problema: quante *parole* di tre lettere si possono scrivere utilizzando solo le cinque vocali?

Per rispondere a questa domanda, e soprattutto per acquisire un metodo di ragionamento che ci servirà in molti altri problemi di questo tipo, possiamo pensare di scrivere effettivamente tutte queste parole di tre lettere.

Evidentemente, per la prima lettera possiamo scegliere tra 5 possibilità, vale a dire, una qualsiasi tra le lettere a, e, i, o, u. Poi, ad ognuna di queste 5 possibilità si possono abbinare 5 possibilità per la seconda lettera della parola. In totale, per le prime due lettere, abbiamo $5 \times 5 = 25$ possibilità: *aa*, *ae*, *ai*, *ao*, *au*, *ea*, ... E ad ognuna di queste 5×5 possibilità per le prime due lettere, potremo abbinare 5 possibilità per la terza lettera, per cui in definitiva avremo $5 \times 5 \times 5 = 125$ possibilità: *aaa*, *aae*, *aai*, ...

È chiaro che siamo in presenza di un principio generale.

Definizione 6.1 (Primo principio del calcolo combinatorio) *Se una certa scelta può essere effettuata in r modi diversi, per ciascuno dei quali una seconda scelta può essere effettuata in s modi diversi, e, per ciascuno dei modi in cui si sono compiute le prime due scelte, una terza scelta può essere effettuata in t modi diversi, ecc., allora la successione di tutte le scelte può essere compiuta in $r \times s \times t \ldots$ modi diversi.*

Come caso speciale di tale principio possiamo ottenere il seguente teorema che fornisce in generale il metodo per risolvere i problemi come quello sopra considerato.

Teorema 6.2 (Disposizioni con ripetizione) *Supponiamo di avere n oggetti e di volerli ordinare in gruppi di k oggetti con la possibilità di scegliere più volte lo stesso oggetto. Allora avremo n^k modi diversi di ottenere tali ragruppamenti.*

Un problema simile al precedente è il seguente: quante sono le parole di 7 lettere costruibili utilizzando tutte le 21 lettere dell'alfabeto italiano, ma senza ripetizione, cioé col vincolo di non utilizzare una lettera più di una volta in una stessa parola?

Questa volta le scelte per la prima lettera sono evidentemente 21 ma ora le scelte si riducono via via che procediamo. Per la seconda lettera possiamo infatti scegliere tra 20 possibilità visto che non possiamo utilizzare la lettera già usata, per la terza lettera siamo ridotti a 19 scelta possibili, e così via. La risposta a questo problema è quindi che le parole di 7 lettere costruibili utilizzando senza ripetizione tutte le 21 lettere dell'alfabeto italiano sono $21 \times 20 \times 19 \times 18 \times 17 \times 16 \times 15$.

È chiaro che il precedente è solamente un esempio particolare del problema generale di *pescare* da un insieme avente un certo numero n di elementi, per costruire tutte le possibili sequenze di k elementi con l'obiettivo finale di contare il numero di tali k-uple. Le k-uple andavano pensate *ordinate*, nel senso che occorreva tenere conto dell'ordine con cui gli elementi di una data k-upla si succedevano, in quanto due k-uple costituite dagli stessi elementi, ma posti in ordine diverso, andavano considerate distinte.

Teorema 6.3 (Disposizioni senza ripetizione) *Supponiamo di avere n oggetti e di volerli ordinare in gruppi di k oggetti in modo che lo stesso oggetto non compaia mai più di una volta. Allora avremo $n \times (n-1) \times \ldots \times (n-k+1)$ modi diversi di ottenere tali ragruppamenti.*

Consideriamo infine il seguente problema: se 6 persone si vogliono mettere in fila da sinistra a destra (rispetto al fotografo) per una foto di gruppo, in quanti modi diversi possono farlo? Non è difficile trovare la risposta: per scegliere il primo elemento della fila, abbiamo 6 possibilità; in corrispondenza di ciascuna di queste 6 possibilità, abbiamo 5 possibilità per il secondo elemento; abbinate a queste 6×5 possibilità abbiamo 4 possibilità per il terzo elemento; per ciascuna di queste $6 \times 5 \times 4$ possibilitàabbiamo 3 possibilità per il quarto elemento, ecc. Quindi la risposta è che le 6 persone possono mettersi in fila in $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 6!$ modi diversi.

Dovrebbe essere evidente che questo problema altro non è che un caso speciale, quando $k = n$, di quello prima considerato.

Corollario 6.4 (Permutazioni) *Supponiamo di avere n og-getti e di volerli ordinare in modo che lo stesso oggetto non compaia mai più di una volta. Allora avremo $n!$ modi diversi di ottenere tali ragruppamenti.*

Esercizi

1. In una compagnia di quattro amici (Roberto, Paolo, Enzo, Walter) bisogna scegliere un capo e un vice. In quanti modi può essere effettuata la scelta?

2. Per andare da una città A ad una cittàB ci sono quattro strade diverse. In quanti modi possibile "fare un giro" da A fino a B e ritorno? E se al ritorno non si vuole ripercorrere la stessa strada dell'andata?

3. In un plotone di 25 militari bisogna scegliere un addetto alle pulizie, un addetto alle cucine e un soldato che monti di sentinella. In quanti modi è possibile effettuare la scelta?

4. Quante parole di 5 lettere si possono scrivere utilizzando liberamente le 21 lettere dell'alfabeto italiano, con possibilitàdi ripetizione di una lettera ma col vincolo di evitare le 'doppie', cioé due (o più) lettere uguali consecutive? (ad esempio sono parole ammissibili: atoim, qtatq, eoeoe... mentre non sono ammissibili: aggfe, pppio...)

5. Per giocare al totocalcio, come è noto, bisogna scegliere un pronostico (che può essere 1, X o 2) per ciascuna delle 13 partite sulla schedina. Quante schedine diverse è possibile compilare?

6. Sappiamo che in ogni computer, la memoria è costituita da tanti *bit*, essendo un bit un dispositivo fisico che può assumere due stati differenti. Indicati convenzionalmente con 0 e 1 tali due stati fisici, diremo, in sostanza, che un bit è una 'cella' di memoria che può assumere, di volta in volta, o il valore 0 o il valore 1. Una sequenza di 8 bit forma il cosiddetto *byte*. Quante diverse "informazioni" può contenere un byte? Quante informazioni diverse si potranno memorizzare in una sequenza di 10 bytes?

7. Sia X un insieme di n elementi. Quante sono le funzioni iniettive di X in se?

6.2 Le combinazioni

Introduciamo ora, tramite un nuovo problema un caso un po' diverso dai precedenti: una compagnia di 5 ragazzi (Aldo (A), Bruno (B), Carlo (C), Dario (D) ed Ernesto (E)), deve passare una notte in una stanza in cui ci sono solo 2 letti. In quanti modi è possibile scegliere i due ragazzi che dormiranno nei letti? (gli altri tre si arrangeranno sul pavimento ...)

È chiaro che in questo caso si tratta di contare il numero di coppie *non* ordinate che è possibile costruire *pescando* dall'insieme A, B, C, D, E. Infatti, si tratta di coppie non ordinate, perché evidentemente la scelta C, E e la scelta E, C andranno considerate equivalenti e andranno quindi contate come una scelta sola.

Per risolvere questo problema procediamo nel modo che segue. Facciamo (o immaginiamo di fare) un grafo che porti a costruire tutte le possibili coppie ordinate di ragazzi; poi, prese due coppie ordinate equivalenti in quanto formate dagli stessi due ragazzi, ma in ordine scambiato, le consideriamo come se fossero una sola.

È chiaro che il numero di scelte possibili sarà $\frac{5\times4}{2}=10$ dove si deve dividere per 2 a causa della presenza di coppie equivalenti.

Proviamo adesso con un caso un po' più complicato: cosa succede se i ragazzi sono 7 (A, B, C, D, E, F, G) e i letti 3?

Evidentemente, basterà pensare a tutte le terne ordinate di ragazzi, poi raggruppare le terne equivalenti, vale a dire contenenti gli stessi elementi, perché se più terne contengono gli stessi elementi, noi le vogliamo contare una volta sola.

Ma, presa una terna ordinata (ad esempio: la terna (A, D, E)) quante sono le terne equivalenti ad essa? Naturalmente, sono tante quate sono i modi di mettere in fila 3 oggetti fissati, ossia sono $3! = 6$ (nel nostro esempio si tratta delle terne (A, D, E), (A, E, D), (D, A, E), (D, E, A), (E, A, D), (E, D, A)). Pertanto la risposta al problema è il numero $\frac{7\times6\times5}{3\times2\times1}=35$.

Possiamo quindi enunciare un nuovo principio generale.

Definizione 6.5 (Secondo principio del calcolo combinatorio) *Se in un certo problema noi abbiamo considerato inizialmente le n-uple ordinate, ma in realtà ci interessano le n-uple non ordinate, dobbiamo pensare il nostro elenco di n-uple ordinate ripartito in tanti gruppi, avendo noi posto in ciascun gruppo tutte le n-uple equivalenti (cioé tutte le n-ple contenenti gli stessi elementi, se pure in ordine diverso). Abbiamo così tanti gruppi, ciascuno formato da $n!$ n-uple, e ciascun gruppo va contato una sola volta. E' chiaro allora che il numero totale delle n-uple ordinate andrà diviso per $n!$.*

Anche in questo caso possiamo esprimere il principio appena enunciato in forma di teorema.

Teorema 6.6 (Combinazioni) *Consideriamo un insieme di n oggetti. Allora i modi in cui possiamo scegliere k elementi tra questi n sono*

$$\left(\begin{array}{c} n \\ k \end{array}\right) \equiv \frac{n\times(n-1)\times\ldots\times(n-k+1)}{k!}$$

Può essere utile osservare che

$$\frac{n\times(n-1)\times\ldots\times(n-k+1)}{k!}=\frac{n!}{k!(n-k)!}$$

6.2.1 Binomio di Newton

Mostriamo ora una immediata applicazione dell'idea delle combinazioni. Supponiamo di voler dimostrare che

$$(a+b)^n = \sum_{k=1\ldots n} \left(\begin{array}{c} n \\ k \end{array}\right) a^k b^{n-k}$$

dove a secondo membro intendiamo la somma n addendi della forma

$$\left(\begin{array}{c} n \\ k \end{array} \right) a^k b^{n-k}$$

Per dimostrare tale identità si può pensare di effettuare la moltiplicazione con n fattori

$$(a+b) \times \ldots \times (a+b)$$

scegliendo, da ciascun fattore $(a+b)$, o il termine a, o il termine b, in tutti i modi possibili, per poi sommare algebricamente i prodotti così ottenuti. Ora, se io scelgo, ad esempio, k volte il fattore b e $n-k$ volte il fattore a, allora avrò il monomio$a^{n-k}b^k$. Quante volte comparirà questo monomio nella somma finale? Tante volte quanti sono i modi in cui, fra gli n fattori, posso selezionare quei k dai quali scegliere b, vale a dire proprio $\left(\begin{array}{c} n \\ k \end{array} \right)$.

Esercizi

1. Un mazzo da poker è formato da 32 carte. A ciascun giocatore se ne distribuiscono 5. Quanti giochi diversi può avere in mano un giocatore?

2. In una compagnia di 20 ragazzi, per Carnevale 18 si vestiranno da "zombi". In quanti modi è possibili scegliere quei 18?

3. Quanti sottoinsiemi di 5 elementi contiene un insieme di 10 elementi?

4. Dal mio guardaroba di 10 magliette e 8 paia di pantaloni voglio scegliere 5 magliette e altrettante paia di pantaloni per andare in ferie. In quanti modi diversi posso effettuare la scelta?

5. Devo distribuire a 10 bambini 5 mele, 2 banane e 3 pesche. In quanti modi diversi posso effettuare la distribuzione?

6. Dimostrare che due persone di Padova hanno le stesse iniziali.

7. Nella mia libreria ho: 10 libri di Storia, 6 libri sugli animali e 7 libri di matematica. Voglio allinearli su di uno scaffale, in modo tale che i libri di una medesima materia siano tutti vicini fra loro. In quanti modi diversi posso ordinare i miei 23 libri?

8. Dimostrare che, per ogni n e ogni k,

$$\left(\begin{array}{c} n \\ k \end{array} \right) \equiv \left(\begin{array}{c} n \\ n-k \end{array} \right)$$

9. Calcolare il coefficiente del del monomio di sesto grado di $(a+b)^{10}$.