Algebra di Base
S.I.S.S. Firenze - 2006

Carlo Casolo
Dipartimento di Matematica "Ulisse Dini",
Università di Firenze,
casolo@math.unifi.it

Indice

Capitolo 1

Insiemi

1.1 Introduzione.

I fondamenti della teoria degli insiemi (anche nel curriculum di un corso di laurea in matematica) sono in genere oggetto di studio nei corsi superiori di logica. Dal punto di vista della didattica di base, il concetto di insieme viene di solito assunto in forma 'ingenua', e la relativa teoria descritta prescindendo da una formulazione assiomatica della stessa. Si tratta, essenzialmente, di fissare un linguaggio, ma non bisogna ignorare che la teoria degli insiemi è anch'essa una teoria matematica, e che non è del tutto "naturale" come potrebbe sembrare (o come sarebbe bello). Per quanto questi non si presentino al livello degli strumenti e dei concetti relativi ad una istruzione matematica non specialistica, la teeoria degli insiemi affronta questioni e problemi molto sottili, la cui portata, non può tuttavia venire intesa se non dopo aver compiuto un certo percorso nella matematica, alla base della quale è la teoria stessa degli insiemi.
Dunque assumeremo come primitivi i concetti di *oggetto* (o *ente*), *insieme, elemento, appartenenza*. Parlando senza pretendere di essere rigorosi, un insieme è "qualcosa" a cui altri "qualcosa" (i suoi elementi) appartengono. Questa relazione di appartenenza è soggetta ad assiomi ben precisi che, come detto, non è il caso di descrivere, e che delimitano con precisione che cosa può o non può essere un insieme (si veda più avanti il Paradosso di Russel).

In genere si utilizzano lettere maiuscole, come $A, X, S, ...$ per indicare gli insiemi, e lettere minuscole, come $a, a', x, y, \alpha, \dots$ per gli elementi di un insieme. Alcuni insiemi particolarmente importanti hanno un simbolo in esclusiva. Ad esempio $\mathbb{N}$ indicherà sempre e solo l'insieme di tutti i numeri *naturali*, cioé dei numeri $0, 1, 2, 3, 4 \dots$.

Altri insiemi per i quali riserviamo un simbolo speciale sono:

- l'insieme $\mathbb{Z}$ dei numeri **interi**; cioè l'insieme dei numeri $0, 1, -1, 2, -2, 3, -3, \ldots$

- l'insieme $\mathbb{Q}$ dei numeri **razionali**; cioè l'insieme dei numeri $\frac{m}{n}$, dove $m, n \in Z$ e $n \neq 0$;

- l'insieme $\mathbb{R}$ dei numeri **reali**;

- l'insieme $\mathbb{C}$ dei numeri **complessi**.

La costruzione rigorosa di questi insiemi a partire dall'insieme $\mathbb{N}$ è argomento che per ora non tratteremo..

Il simbolo $\in$ indica l'*appartenenza* di un elemento ad un certo insieme; $a \in X$ significa cioè che a è un elemento dell'insieme X. Con $\notin$ si intende la non appartenenza: $a \notin X$ significa che a **non** è un elemento dell'insieme X. Ad esempio, $2 \in \mathbb{N}$ mentre $\pi \notin \mathbb{N}$.
Un specifico insieme verrà di solito descritto mediante informazioni delimitate da parentesi graffe $\{....\}$. L'informazione può essere costituita dall'indicazione diretta degli elementi dell'insieme, oppure dalle proprietà che individuano gli elementi stessi. Ad esempio, l'insieme i cui elementi sono i numeri naturali 2, 3, 4 può essere descritto nelle seguenti maniere (e, naturalmente, in molte altre):

$$\{2, 3, 4\}, \quad \{x \mid x \in \mathbb{N} \text{ e } 2 \leq x \leq 4\}.$$

Nella seconda modalità, la barra verticale $|$ segnala che ciò che segue è la proprietà che serve ad individuare gli elementi. A volte, invece della barra, si usano i 'due punti'. Ad esempio $\{2x : x \in \mathbb{N}\}$ è l'insieme dei numeri interi pari.
È opportuno osservare che né l'ordine con cui sono descritti, o elencati, gli elementi di un insieme, né eventuali ripetizioni, modificano l'insieme. Ad esempio, le scritture:

$$\{1, 2\}, \quad \{1, 2, 1\}, \quad \{2, 1\}$$

individuano tutte il medesimo insieme.
Inoltre, è bene sapere che gli elementi di un insieme possono anche essere di 'natura' diversa; ad esempio, gli *elementi* dell'insieme $X = \{1, \{1\}\}$, sono il *numero intero* 1 e *l'insieme* $\{1\}$ (X contiene quindi due elementi distinti).

insieme vuoto

È conveniente contemplare anche la possibilità che un insieme sia privo di elementi. In matematica è frequente la possibilità di considerare proprietà che non sono soddisfatte da alcun oggetto. Tali proprietà definiscono quindi insiemi privi di elementi. Ad esempio, l'insieme dei numeri interi pari che sono potenza di tre non contiene alcun elemento.
L'insieme privo di elementi si denota con $\emptyset$ e si chiama **insieme vuoto**. Ad

esempio, è vuoto l'insieme delle soluzioni reali del sistema di equazioni

$$\begin{cases} 2x + 3y = 3 \\ xy = 1 \end{cases}$$

Questo si puó scrivere così: $\{(x, y) \mid x, y \in \mathbb{R},\ 2x + 3y = 3 \text{ e } xy = 1\} = \emptyset$.

L'insieme vuoto è "uno solo". Così, ad esempio l'insieme dei numeri pari che sono potenze di 3 (che è vuoto) è uguale all'insieme degli elefanti verdi che fumano la pipa (che, per quanto mi consta, è anch'esso vuoto).

Assumeremo, almeno per il momento, come primitivo anche il concetto di numero di elementi di un insieme (anche se, nel seguito, accenneremo alla teoria - dovuta a Cantor - che descrive rigorosamente tale concetto). Diremo che un insieme X è **finito** se X contiene un numero finito di elementi, e in tal caso, se il numero di elementi di X è n, scriviamo $|X| = n$. Ad esempio, $|\{1, 2, 6, 8\}| = 4$, e $|\emptyset| = 0$. Se invece X contiene un numero infinito di elementi, diremo che X è un insieme **infinito** e scriveremo $|X| = \infty$. Ad esempio $|\mathbb{N}| = \infty$. Il simbolo $|X|$ (che quindi, per quanto riguarda un approccio introduttivo, sarà ∞ oppure un numero naturale), lo chiameremo **ordine** (o *cardinalità*) dell'insieme X.

Paradosso di Russell

il paradosso di Russsel

Anche se si tratta di una insidia che non si presenta nell'ambito della nostra utilizzazione del linguaggio della teoria degli insiemi, può essere interessante riportare che non tutto ciò che ci si presenta intuitivamente come una **proprietà** può essere utilizzato per definire un insieme. L'esempio più famoso ed importante per la nascita di quella che sarà poi la teoria assiomatica degli insiemi è il cosiddetto *Paradosso di Russell*.
Per illustrare il paradosso, diciamo che un insieme è *normale* se non contiene se stesso come elemento (si può pensare ad esempio all'insieme di tutti i concetti astratti: questo è, direi, un concetto astratto esso stesso, quindi contiene se stesso come elemento, non è dunque un insieme normale). Intutivamente, l'essere normale ci appare senz'altro come una proprietà 'sensata'; ma cosa accade quando la utilizziamo per definire un insieme ?
Definiamo cioè l'insieme N i cui elementi sono tutti gli insiemi normali. Quindi

$$N = \{X \mid X \text{ è un insieme e } X \notin X\}.$$

A questo punto, se N è un insieme, esso è o non è normale. Analizzate le due possibilità: entrambe conducono ad una contraddizione. Quindi N non è un insieme; non ogni proprietà costituisce una definizione.

Il paradosso di Russel mostra che qualche cosa non si può fare. Il concetto di insieme va quindi specificato in modo più accurato. Il punto del paradosso non è tanto l'immaginarsi come possa avvenire che un insieme contenga se stesso (generando un processo all'infinito), quanto il fatto che una certa relazione tra enti (quella di appartenenza) venga usata in modo autoreferenziale. Questo è alla base di molti altri 'paradossi logici', come quello del mentitore, del barbiere, etc. che alcuni già conosceranno e nei quali non si fa riferimento a processi all'infinito. Per essere assolutamente moderni vediamo un esempio riferito alla rete Internet.
Come si sa, le varie pagine Internet accessibili in rete contengono diverse connessioni (links) ad altre pagine; tali connessioni sono di norma segnalate da una o più parole sottolineate. Ora, vi sono pagine che contengono un link a se stesse (tipicamente le cosiddette home pages), altre (la maggioranza) che non contengono un link a se stesse. Il numero totale di pagine (nel mondo, o possiamo limitarci ad ambiti più ristretti - non cambia nulla) è comunque finito. Supponiamo che io (il Grande Fratello) chieda al mio capo tecnico di allestire una pagina Internet che contenga un link a tutte e sole le pagine che non hanno link a se stesse... Se ci pensate un attimo, vedete che una tale pagina non si può fare, e che tale paradosso è molto simile al paradosso di Russell.

1.2 Sottoinsiemi.

sottoinsiemi

Un insieme S si dice **sottoinsieme** dell'insieme A, e si scrive $S \subseteq A$, se ogni elemento di S appartiene ad A. Se $S \subseteq A$ si dice anche che S è *incluso* in A.
Viceversa, $S \not\subseteq A$ significa che S non è sottoinsieme di A, ovvero che *esiste almeno un elemento x tale che $x \in S$ ma $x \notin A$.*

Ad esempio $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$, $\{1,6\} \subseteq \{6,3,2,1\}$, mentre $\{1,6\} \not\subseteq \{x \,|x \in \mathbb{N} \text{ e } 2 \text{ divide } x\}$, dove chiaramente

In particolare, ogni insieme è un sottoinsieme di se stesso, così come l'insieme vuoto è un sottoinsieme di qualunque insieme. Quindi:

$$\textit{per ogni insieme } A, \quad \emptyset \subseteq A \quad e \quad A \subseteq A. \tag{1.1}$$

È anche chiaro che l'inclusione tra insiemi è una proprietà *transitiva*; ovvero, se A, B, C sono insiemi con $A \subseteq B$ e $B \subseteq C$, allora $A \subseteq C$. Un sottoinsieme S dell'insieme A si dice **proprio** se non coincide con A, ovvero $S \subseteq A$ e $S \neq A$. Per indicare che S è un sottoinsieme proprio di A si scrive $S \subsetneq A$ (o, talvolta, $S \subset A$).

ugualglianza

Due insiemi A e B sono **uguali** (si scrive $A = B$) se ogni elemento di A è elemento

di B e viceversa. Quindi $A = B$ se e soltanto se è soddisfatta la *doppia inclusione*

$$A \subseteq B \quad \text{e} \quad B \subseteq A. \tag{1.2}$$

Spesso, per provare l'uguaglianza di due insiemi si dimostra appunto la doppia inclusione; vedremo esempi di questo metodo nelle pagine seguenti. Chiaramente, per provare invece che due insiemi **non sono** uguali è sufficiente trovare un elemento di uno dei due insiemi che non appartiene all'altro.

Esempi:

$$\{1,2,3\} = \{x \mid x \in \mathbb{Z}, \frac{1}{2} \leq x \leq \sqrt{10}\ \} \qquad \{1,\{1\}\} \neq \{1\}$$

$$\{1\} \not\subseteq \{\{1\},\{2\}\} \qquad \{\emptyset,\{\emptyset\},\emptyset\} = \{\emptyset,\{\emptyset\}\}.$$

insieme delle parti

Dato un insieme A, allora la collezione di tutti i sottoinsiemi di A costituisce un insieme, detto **insieme della parti** (o *insieme potenza*) dell'insieme A, che si denota con $\mathcal{P}(A)$. Quindi

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

Osserviamo che l'osservazione 1.1 si traduce quindi nel fatto che, per ogni insieme A,

$$\emptyset \in \mathcal{P}(A) \quad \text{e} \quad A \in \mathcal{P}(A). \tag{1.3}$$

Esempi: Se $X = \{1,2,3\}$, allora $\mathcal{P}(X) = \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,2\},\{1,2\},\{1,2,3\}\}$.

$$\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset \qquad \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset,\{\emptyset\}\}$$

Osserviamo gli ultimi due esempi: nel primo caso l'insieme ha 3 elementi e l'insieme delle sue parti ha $8 = 2^3$ elementi; nel secondo caso l'insieme (vuoto) ha 0 elementi, e l'insieme delle sue parti ne ha $1 = 2^0$; nel terzo caso l'insieme ha 1 elemento e l'insieme delle sue parti ne ha 2. Per esercizio di descriva l'insieme delle parti di un insieme con due elementi (ad esempio $\{1,2\}$) e quello di un insieme con 4 elementi: si scoprirà che l'insieme delle parti ha rispettivamente, $4 = 2^2$ e $16 = 2^4$ elementi. In effetti, come vedremo più avanti, non è difficile provare dimostrare il seguente fatto:

Se A è un insieme finito e $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$.

1.3 Operazioni tra insiemi.

Siano A e B due insiemi. Si chiama **unione** degli insiemi A e B, e si denota con $A \cup B$, l'insieme i cui elementi sono gli oggetti che appartengono ad almeno uno tra A e B. *unione*

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

Si chiama **intersezione** degli insiemi A e B, e si denota con $A \cap B$, l'insieme i cui elementi sono gli oggetti che appartengono sia ad A che a B. *intersezione*

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

Insiemi A e B si dicono *disgiunti* se non hanno elementi in comune, cioè se $A \cap B = \emptyset$.

Esempi. 1) Siano $A = \{-1, 0, 1\}$, $B = \{2x \mid x \in \mathbb{N} \text{ e } 0 \leq x \leq 3\}$, allora

$$A \cup B = \{-1, 0, 1, 2, 4, 6\} \quad \text{e} \quad A \cap B = \{0\};$$

2) Siano $P = \{x \mid x \in \mathbb{N} \text{ e 2 divide } x\}$ e $D = \{x \mid x \in \mathbb{N} \text{ e 2 non divide } x\}$ (cioè, rispettivamente, l'insieme dei numeri naturali pari, e quello dei numeri naturali dispari), allora

$$P \cup D = \mathbb{N} \quad \text{e} \quad P \cap D = \emptyset.$$

Le seguenti osservazioni, che è utile formulare, sono immediate:

Siano A, B insiemi; allora

$$\begin{aligned} A = A \cup \emptyset; \quad \emptyset \cap A = \emptyset; \\ A \subseteq A \cup B; \quad A \cap B \subseteq A; \\ A = A \cup B \quad \text{se e solo se} \quad B \subseteq A; \\ A = A \cap B \quad \text{se e solo se} \quad A \subseteq B. \end{aligned}$$

Inoltre, le operazioni di unione e intersezione di insiemi soddisfano ad alcune importanti proprietà che sono di facile verifica.

Proposizione 1.3.1. *Siano A, B e C insiemi. Allora*

(1) $A \cup A = A \quad e \quad A \cap A = A;$

(2) $A \cup B = B \cup A \quad e \quad A \cap B = B \cap A;$

(3) $A \cup (B \cup C) = (A \cup B) \cup C \quad e \quad A \cap (B \cap C) = (A \cap B) \cap C.$

La proprietà (2) è la proprietá **commutativa**; mentre la (3) è la proprietà **associativa**. La prossima proposizione descrive le importanti proprietà **distributive** tra l'unione e l'intersezione di insiemi

Proposizione 1.3.2. *Siano A, B e C insiemi. Allora* *distributività*

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

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

Diamo, per chi è interessato, e per una volta, la
Dimostrazione. (1). Sia $x \in A \cap (B \cup C)$. Allora $x \in A$ e $x \in B \cup C$; possiamo scrivere (la parentesi graffa indica, come avviene per i sistemi di equazioni, che entrambe le condizioni devono essere verificate):

$$\begin{cases} x \in A \\ x \in B \ \text{ o } \ x \in C \end{cases}$$

Abbiamo quindi due possibilità:

$$\begin{cases} x \in A \\ x \in B \end{cases}; \quad \text{oppure} \quad \begin{cases} x \in A \\ x \in C \end{cases}$$

Dunque $x \in A \cap B$ o $x \in A \cap C$; cioè $x \in (A \cap B) \cup (A \cap C)$. Abbiamo provato quindi che

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$

Viceversa, sia $x \in (A \cap B) \cup (A \cap C)$. Allora

$$\begin{cases} x \in A \\ x \in B \end{cases} \quad \text{oppure} \quad \begin{cases} x \in A \\ x \in C \end{cases}$$

Nel primo caso $x \in A$ e $x \in B$, allora $x \in A$ e $x \in B \cup C$, e quindi $x \in A \cap (B \cup C)$; allo stesso modo, se $x \in A$ e $x \in C$, allora $x \in A \cap (B \cup C)$. Dunque

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

La doppia inclusione è verificata e l'uguaglianza (1) é provata. ∎

Siano A e B due insiemi. Si chiama **differenza** di A e B, e si denota con $A \setminus B$, l'insieme i cui elementi sono gli oggetti che appartengono ad A ma non appartengono a B: *differenza*

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

Si chiama **differenza simmetrica** di A e B, e si denota con $A \Delta B$, l'insieme i cui elementi sono quelli che appartengono ad uno e un solo degli insiemi A e B: *diff.simmetrica*

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

Esempi. 1) Siano $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$; allora

$$A \setminus B = \{1, 2\}; \qquad B \setminus A = \{4, 5\}; \qquad A\Delta B = \{1, 2, 4, 5\}.$$

2) Siano $A = \{1, 2, 3\}$ e $B = \{2x \mid x \in \mathbb{N}\}$; allora

$$A \setminus B = \{1, 3\}; \qquad B \setminus A = \{2x \mid x \in \mathbb{N} \text{ e } x \neq 1\}; \qquad A\Delta B = \{1, 3, 4, 6, 8, 10, \ldots\}.$$

Gli 'esempi mostrano che la differenza tra insiemi non è commutativa; sussistono invece le seguenti proprietà: $A \setminus B \subseteq A$; $A \setminus A = \emptyset$; $A \setminus \emptyset = A$.

Esercizio. Siano A, B e C insiemi; si provi che $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

Soluzione. Sia $x \in (A \cup B) \setminus C$. Allora $x \in (A \cup B)$ e $x \notin C$; quindi $x \in A$ (e $x \notin C$) o $x \in B$ (e $x \notin C$). Dunque $x \in (A \setminus C) \cup (B \setminus C)$, il che prova la prima inclusione $(A \cup B) \setminus C \subseteq (A \setminus C) \cup (B \setminus C)$.
Sia ora $y \in (A \setminus C) \cup (B \setminus C)$. Allora $y \in A \setminus C$ oppure $y \in B \setminus C$. In ogni caso $y \notin C$ e $y \in A$ o $y \in B$. Quindi $y \in (A \cup B) \setminus C$, provando così l'altra inclusione $(A \setminus C) \cup (B \setminus C) \subseteq (A \cup B) \setminus C$. Per il principio della doppia inclusione si ricava pertanto l'uguaglianza cercata.

Seguendo il tipo di ragionamenti impiegati nella soluzione del precedente esercizio, dovreste essere in grado di dimostrare da voi le seguenti rilevanti proprietà.

Proposizione 1.3.3. (leggi di De Morgan) *Siano A, B e C insiemi. Allora*

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \quad \text{e} \quad A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C).$$

Nota. Per quanto piuttosto interessante da un punto di vista algebrico, la differenza simmetrica è un'operazione che capita di incontrare un po' più raramente a livello elementare. Mi limito quindi ad elencarne le principali proprietà. Si osservino in particolare le proprietà (4), (5), e (6) che, rispettivamente, dicono che la differenza simmetrica è commutativa, che è associativa, e che l'intersezione è distributiva rispetto alla differenza simmetrica.

Proposizione 1.3.4. *Siano A, B e C insiemi. Allora*

(1) $A\Delta A = \emptyset$;

(2) $A\Delta\emptyset = A$;

(3) $A\Delta B = (A \cup B) \setminus (A \cap B)$;

(4) $A\Delta B = B\Delta A$;

(5) $(A\Delta B)\Delta C = A\Delta(B\Delta C)$;

(6) $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.

Esercizio. Siano A, B, C insiemi. Si dimostri che:
(a) $A\triangle(B\cup C)\subseteq(A\triangle B)\cup C$.
(b) $A\triangle(B\cup C)=(A\triangle B)\cup C$ se e solo se $A\cap C=\emptyset$.

Soluzione. (a) $(B\cup C)\setminus A\subseteq(B\setminus A)\cup(C\setminus A)\subseteq(B\setminus A)\cup C\subseteq(A\triangle B)\cup C$. Inoltre, poichè $B\subseteq B\cup C$ si ha $A\setminus(B\cup C)\subseteq A\setminus B\subseteq(A\triangle B)$.
Dunque: $A\triangle(B\cup C)=(A\setminus(B\cup C))\cup(B\cup C)\setminus A)\subseteq(A\triangle B)\cup C$.

(b) Sia $A\cap C=\emptyset$; per il punto (a) è sufficiente provare l'inclusione $(A\triangle B)\cup C\subseteq A\triangle(B\cup C)$. Sia quindi $x\in(A\triangle B)\cup C=(A\setminus B)\cup(B\setminus A)\cup C$; se $x\in A$, allora $x\notin B$ e (per ipotesi) $x\notin C$, quindi $x\in A\setminus(B\cup C)\subseteq A\triangle(B\cup C)$; se invece $x\in(B\setminus A)\cup C$ allora $x\notin A$ (sempre perchè $A\cap C=\emptyset$), e quindi $x\in(B\cup C)\setminus A\subseteq A\triangle(B\cup C)$.
Dunque $(A\triangle B)\cup C\subseteq A\triangle(B\cup C)$.
Viceversa, sia $A\cap C\neq\emptyset$, e sia $x\in A\cap C$. Allora, poichè $x\in C$ si ha $x\in(A\triangle B)\cup C$; ma $x\notin A\setminus(B\cup C)$ (perchè $x\in C$) e $x\notin(B\cup C)\setminus A$ (perchè $x\in A$); quindi $x\notin(A\setminus(B\cup C))\cup((B\cup C)\setminus A)=A\triangle(B\cup C)$. Dunque $(A\triangle B)\cup C\not\subseteq A\triangle(B\cup C)$.

Spesso, per aiutare la nostra intuizione, si ricorre nella rappresentazione di generici insiemi ai cosiddetti *diagrammi di Wenn*: in essi un insieme viene rappresentato come la porzione di piano delimitata da una curva chiusa semplice (cioè priva di incroci). Ad esempio, il segunete disegno illustra la differenza simmetrica $A\Delta B$: *diagr.di Wenn*

L'affermazione (a) dell'esercizio di sopra è illustrata dai seguenti diagrammi:

Va però tenuto ben presente che l'utilizzo dei diagrammi di Wenn può essere molto conveniente per farci un'idea di quello che sta accadendo, ma non fornisce in nessun modo dimostrazioni rigorose (ed a volte può risultare anchhe fuorviante).

Prima di proseguire, diciamo qualcosa a proposito dell'uso degli *indici* nella nota- *indici*

zione matematica. Il lettore sarà già familiare con il loro impiego nelle definizioni di successioni: i termini di una successione si denotano in generale con a_n dove n (l'indice) è un numero intero positivo (che per lo più parte da 0 o da 1). Lo stesso principio, ovvero quello di assegnare ad un enete appartenente ad una famiglia - finita o infinita - un'etichetta che consenta di richiamarlo con una notazione più economica e compatta, viene utilizzato anche in molti altri contesti. Ad esempio, se n è un certo intero positivo, e A è un insieme con n elementi (che è possibile non siano noti con precisione), si possono designare gli elementi di A come

$$A = \{a_1, a_2, a_3, \ldots, a_n\}.$$

Più in generale, data una famiglia - anche infinita - di oggetti (i quali possono a loro volta essere insiemi), può essere spesso opportuno indicizzarli. In generale gli indici sono presi in un altro insieme noto, come $\mathbb{N}$ o $\mathbb{Z}$, ma a volta si può essere generici fino in fondo e assegnare gli indici in un non specificato insieme (che allora viene in genere chiamato I - l'insieme degli indici). Spesso poi, l'indice ha strettamente a che fare con la definizione del particolare ente che esso etichetta; questo normalmente accade nelle successioni. Come altro esempio, l'insieme dei numeri naturali maggiori di un certo numero n può essere indicizzato proprio da tale n

$$A_n = \{a \in \mathbb{N} \mid a \geq n\},$$

che è una notazione conveniente se abbiamo intenzione di considerare tutta la famiglia di insiemi di questo tipo; si dice allora

$$\text{la famiglia degli insiemi } A_n \text{ al variare di } n \in \mathbb{N}.$$

---

unioni e intersezioni generalizzate

Unioni e intersezioni generalizzate. (questa parte è più tecnica, e può essere omessa se sembra troppo specialistica).

Se A, B e C sono insiemi, allora la proprietà associativa dell'intersezione consente di poter scrivere senza ambiguità $A \cap B \cap C$, intendendo, indifferentemente, $(A \cap B) \cap C$ o $A \cap (B \cap C)$. Chiaramente si ha l'uguaglianza:

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

Similmente, per quanto concerne l'unione; avremo:

$$A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C) = \{\ x \mid x \in A \ \text{ o } \ x \in B \ \text{ o } \ x \in C\ \}.$$

Questo si estende ad un numero qualunque di insiemi; se $A_1, A_2, \ldots, A_n$ sono insiemi; allora

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{\ x \mid x \in A_i \ \text{ per qualche } \ i = 1, 2, \ldots, n\ \}.$$

e

$$A_1 \cap A_2 \cap \cdots \cap A_n = \{\ x \mid x \in A_i \ \text{ per ogni } \ i = 1, 2, \ldots, n\ \}.$$

Ora, il passo naturale è passare ad una famiglia infinita di insiemi. Sia F una famiglia di insiemi. Si definisce, rispettivamente, l'unione e l'intersezione degli insiemi della famiglia F nel modo seguente:

$$\bigcup_{A \in F} A = \{x \mid x \in A \ \text{ per qualche } \ A \in F\ \}.$$

$$\bigcap_{A \in F} A = \{x \mid x \in A \ \text{ per ogni } \ A \in F\ \}.$$

Nella pratica, gli insiemi di una famiglia sono in genere *indicizzati*; cioè è dato un insieme I, detto di *indici*, ed una corrispondenza tra gli insiemi della famiglia F e gli elementi di I, per cui all'elemento $i \in I$ corrisponde l'insieme $A_i \in F$. Si scrive che F è la famiglia degli insiemi $(A_i)_{i \in I}$ e quindi per unione e intersezione si usa la notazione:

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

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

Forse la cosa risulterà più chiara dopo alcuni esempi.

Esempi. 1) Per ogni $i \in \mathbb{N}$ sia $M_i = \{x \mid x \in \mathbb{N}\ ,\ x \leq i\ \}$. In questo caso, l'insieme degli indici è l'insieme dei numeri naturali e, ad esempio, $M_4 = \{0, 1, 2, 3, 4\}$. Allora:

$$\bigcup_{i \in \mathbb{N}} M_i = \mathbb{N} \qquad \text{e} \qquad \bigcap_{i \in \mathbb{N}} M_i = \{0\}.$$

Infatti, sia $X = \bigcup_{i \in \mathbb{N}} M_i$; allora chiaramente $X \subseteq \mathbb{N}$ (dato che, per ogni $i \in \mathbb{N}\ :\ M_i \subseteq \mathbb{N}$); viceversa, se $n \in \mathbb{N}$ allora $n \in M_n$ e quindi $n \in X$, dunque $\mathbb{N} \subseteq X$.
L'intersezione è chiara, dato che, per ogni $i \in \mathbb{N} : \{0\} \subseteq M_i$ e $\bigcap_{i \in \mathbb{N}} M_i \subseteq M_0 = \{0\}$.

2) Per ogni $i \in \mathbb{N}$ sia $N_i = \{x \mid x \in \mathbb{N}\ ,\ x \geq i\ \}$. Allora:

$$\bigcup_{i \in \mathbb{N}} N_i = \mathbb{N} \qquad \text{e} \qquad \bigcap_{i \in \mathbb{N}} N_i = \emptyset.$$

Infatti, l'unione è chiara, dato che $N_0 = \mathbb{N}$; per quanto riguarda l'intersezione, essa è chiaramente contenuta nell'insieme $\mathbb{N}$, ma, per ogni $x \in \mathbb{N}$ abbiamo che $x \notin N_{x+1}$, quindi, a maggior ragione, $x \notin \bigcap_{i \in \mathbb{N}} N_i$.

1.4 Prodotto cartesiano.

coppie ordinate

Siano A e B insiemi; siano $a \in A$ e $b \in B$; il simbolo (a, b) è la **coppia ordinata** la cui prima coordinata (o componente) è l'elemento a e la seconda è l'elemento b. Per definizione, due coppie ordinate (a, b) e (a', b') (con $a, a' \in A,\ b, b' \in B$) sono uguali se e solo se $a = a'$ e $b = b'$.

prod.cartesiano

La collezione di tutte le coppie ordinate la cui prima componente appartiene all'insieme A e la seconda componente appartiene all'insieme B è un insieme, che si denota con $A \times B$, e si chiama **prodotto cartesiano** di A per B. Quindi:

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

Ad esempio, se $A = \{1, 2\}$ e $B = \{0, 1, \pi\}$; allora

$$A \times B = \{(1, 0), (1, 1), (1, \pi), (2, 0), (2, 1), (2, \pi)\}.$$

$\mathbb{R} \times \mathbb{R}$, che si denota anche con $\mathbb{R}^2$ è l'insieme di tutte le coppie ordinate di numeri reali.

Osservazioni. Siano A e B insiemi. Allora

- $A \times \emptyset = \emptyset = \emptyset \times A$;
- se $A \neq \emptyset \neq B$, allora $A \times B = B \times A$ se e solo se $A = B$;
- se $A' \subseteq A$ e $B' \subseteq B$, allora $A' \times B' \subseteq A \times B$.

cardinalità di un prodotto

Facciamo anche una semplice ma basilare osservazione riguardo al numero di elementi di un prodotto cartesiano, nel caso di insiemi finiti. Supponiamo quindi che A e B siano insiemi finiti, con $|A| = n$ e $|B| = m$ (ricordo che ciò significa che A contiene n elementi e B ne contiene m). Possiamo elencare gli elementi di A e quelli di B, ovvero scrivere

$$A = \{a_1, a_2, \ldots, a_n\} \qquad \text{e} \qquad B = \{b_1, b_2, \ldots, b_n\}.$$

Allora il prodotto cartesiano $A \times B$ avrà come elementi tutte le coppie del tipo (a_i, b_j), con l'indice i che va da 1 a n, e l'indice j che va da 1 a m. Possiamo quindi mentalmente "costruire" gli elementi del prodotto $A \times B$ figurandoci di fissare di volta in volta la prima componente a_i della coppia (per la quale quindi abbiamo n scelte diverse), e quindi sistemare come seconda componente tutte le possibili scelte per b_j (che sono n). È chiaro dunque che in totale otterremo $n \times m = nm$ coppie distinte, le quali costituiscono la totalità degli elementi di $A \times B$ Pertanto $|A \times B| = nm$, ed abbiamo dunque provato che

se A e B sono insiemi finiti, allora $|A \times B| = |A||B|$.

n-uple

La definizione di prodotto cartesiano puó essere estesa da due ad un numero finito arbitrario n di insiemi. Siano $A_1, A_2, \ldots, A_n$ insiemi. L'insieme

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

è l'insieme delle n-uple ordinate la cui i-esima componenete appartiene all'insieme A_i.
Se tutti gli insiemi A_i coincidono con l'insieme A, allora si parla di insieme delle n-uple ordinate di A, e si denota tale insieme con A^n. Ad esempio, $\mathbb{R}^n$ è l'insieme di tutte le n-uple ordinate di numeri reali. Chiaramente due n-uple sono uguali se e solo se tutte le componenti sono corrispondentemente uguali; inoltre valgono osservazioni simili a quelle fatte sopra per le coppie, la cui esplicita formulazione lasciamo per esercizio.

---

cardinalità di una unione

Nota. Avendo, poco sopra, stabilito la cardinalità (numero di elementi) di un prodotto diretto di insiemi finiti, può essere a questo punto utile fare una osservazione (anch'essa semplice ma utilissima) intorno alla cardinalità di una *unione* di insiemi finiti. Siano dunque A e B insiemi finiti, con $|A| = n$ e $|B| = m$. È chiaro che se A e B sono disgiunti (cioè non hanno elementi in cumune, o in altri termini $A \cap B = \emptyset$), allora il numero di elementi della loro unione $A \cup B$ è la somma $n + m$. In generale, però, non possiamo assumere in partenza che A e B siani disgiunti, tuttavia possiamo osservare che se contiamo separatamente gli elementi di A e poi quelli di B, arriviamo al numero $n + m$ avendo contato due volte gli elementi in comune tra A e B (cioè gli elementi dell'intersezione $A \cap B$). Quindi, per ottenere il umero effettivo di elementi di $A \cup B$ dobbiamo togliere dal valore $n + m$ il numero di elementi contati due volte, e questo numero è $|A \cap B|$. Pertanto

se A e B sono insiemi finiti, allora $|A \cup B| = |A| + |B| - |A \cap B|$.

1.5 Cenni di calcolo proposizionale

proposizioni

La logica proposizionale descrive come trattare le connessioni logiche elementari tra oggetti base di un ragionamento, detti *proposizioni*. Una **proposizione** è una affermazione (una 'frase', un espressione nel linguaggio) a cui è possibile associare in modo univoco un valore di verità: Vero [V] o Falso [F]. Ad esempio sono proposizioni le seguenti:

- 24 è un numero pari;
- 24 è un numero primo;
- 24 è somma di due numeri primi;
- ogni numero intero pari è somma di due numeri primi;

delle quali, la prima è vera, la seconda falsa, la terza vera [$24 = 13 + 11 = 17 + 7$], la quarta è vera o falsa, si presume che sia vera (si tratta della famosa *Congettura di Goldbach*), ma ancora nessuno ne ha stabilito la correttezza. Non sono invece proposizioni le seguenti:

- qual è il massimo comun divisore tra 24 e 30 ?
- sia p un numero primo;
- ogni proposizione che appare in questa riga di testo è falsa.

connettivi logici

Vero e Falso si dicono *valori di verità*; ad ogni proposizione viene quindi associato uno ed un solo valore di verità, e corrispondentemente diremo che una certa proposizione "è vera" o "è falsa". I **connettivi logici**, che tra breve descriveremo, traducono in modo formale le principali connessioni tra proposizioni, che usualmente (magari in maniera ingenua) utilizziamo nello sviluppo di un argomentazione, e consentono di formare nuove proposizioni a partire da altre proposizioni date.

congiunzione

Il primo dei connettivi logici che descriviamo è la *congiunzione* $\wedge$. Esso traduce il concetto espresso nel discorso dalla congiunzione "e": se P e Q sono due proposizioni, allora $P \wedge Q$ (da leggersi, appunto, "P e Q") è quella proposizione che è vera *se e soltanto se entrambe P e Q sono vere*. Questo può essere convenientemente esplicato mediante la sua *tavola di verità*:

tavole di verità

P	Q	P $\wedge$ Q
V	V	V
V	F	F
F	V	F
F	F	F

dove, ovviamente, V significa che la proposizione è vera, F che è falsa. La tavola fornisce il valore di verita di $P \wedge Q$ in funzione di tutte le possibili e separate attribuzioni di valori di verità a P ed a Q.

Gli altri connettivi logici che ci interessano sono:

- la *disgiunzione*: $\vee$
- la *negazione*: $\neg$
- l'*implicazione*: $\rightarrow$

disgiunzione

La disgiunzione $\vee$ traduce la "o" e, nonostante il nome, indica una opzione non disgiuntiva (ovvero, come nel latino *vel*): $P \vee Q$ (letto "P o Q") significa che *almeno una* tra P e Q è vera. La sua tavola di verità è:

P	Q	P $\vee$ Q
V	V	V
V	F	V
F	V	V
F	F	F

La negazione $\neg$ traduce il "non": $\neg P$ è la proposizione che assume il valore di veità opposto a quello di P. La tavola di verità è cioè la seguente: *negazione*

P	$\neg$ P
V	F
F	V

L'implicazione $\rightarrow$ esprime l'implicazione *logica*, ovvero il fatto che dalla verità di una proposizione (premessa) segue la verità di un'altra (conseguenza): $P \rightarrow Q$ (letta "P implica Q") significa che Q è vera quando P è vera. La tavola di verità è dunque la seguente: *implicazione*

P	Q	P $\rightarrow$ Q
V	V	V
V	F	F
F	V	V
F	F	V

Si osservi che, secondo la nostra definizione (ma anche secondo l'uso che, almeno nelle forme di pensiero che tendono a qualche rigore, ne è stato fatto), la verità di una implicazione *non* richiede la verità della premessa, anzi quando P è falsa, allora $P \rightarrow Q$ è vera qualsiasi sia la proposizione Q; questo fatto era stato osservato anche in antichità ed espresso nella formula: *ex falso sequitur quodlibet*.

Le tavole di verità per i singoli connettivi possono essere utilizzate in successione per ricavare le tavole di verità di proposizioni più articolate. Ad esempio, ricavaiamo la tavola di verità della proposizione

$$\neg Q \rightarrow \neg P$$

(dove conveniamo che la negazione $\neg$ venga letta con diritto di precedenza, ovvero con $\neg Q \rightarrow \neg P$ intendiamo $(\neg Q) \rightarrow (\neg P)$):

P	Q	$\neg P$	$\neg Q$	$\neg Q \rightarrow \neg P$
V	V	F	F	V
V	F	F	V	F
F	V	V	F	V
F	F	V	V	V

Vediamo un altro esempio:

$$(P \vee Q) \to (\neg Q \to P)$$

la cui tavola di verità è:

P	Q	$P \vee Q$	$\neg Q$	$\neg Q \to P$	$(P \vee Q) \to (\neg Q \to P)$
V	V	V	F	V	V
V	F	V	V	F	V
F	V	V	F	V	V
F	F	F	V	V	V

tautologie

Osserviamo l'utlimo esempio; l'esame della tavola di veirtà mostra che la proposizione $(P \vee Q) \to (\neg Q \to P)$ è *vera qualsiasi siano* i valori di verità delle proposizioni P e Q che la compongono. Una tale proposizione si dice **tautologia**. Il più tipico esempio di tautologia è la proposizione che esprime il cosiddetto "principio del terzo escluso": $P \vee \neg P$.

contraddizioni

Viceversa, una proposizione che è sempre *falsa*, qualsiasi siano i valori di verità delle proposizioni elementari che la compongono si dice una **contraddizione**. L'esempio base di contraddizione è la proposizione che esprime la '"reductio ab absurdum": $P \wedge \neg P$.

equivalenza logica

Osserviamo ora la tavola di verità della proposizione $\neg Q \to \neg P$, che abbiamo ricavato sopra: ci accorgiamo che, in corrispondenza ad ogni possibile assegnazione dei valori di verità di P e di Q, li valore di verità di tale proposizione coincide con quello della proposizione $P \to Q$. Si dice allora che le proposizioni $\neg Q \to \neg P$ e $P \to Q$ sono *logicamente equivalenti*. Da un punto di vista operativo, ciò significa che dimostrare la verità dell'una equivale a dimostrare la verità dell'altra.

Nota. L'esempio che abbiamo fornito di equivalenza logica esprime in effetti un metodo argomentativo utilizzato di frequente: per provare che da una certa affermazione P segue un'altra affermazione Q, si dimostra che la negazione di Q comporta necessariamente la negazione di P. Altri casi di equivalenze logiche che esprimono comuni, e legittime, tecniche di ragionamento sono descritte nell'esercizio che segue e nell'esercizio 1.18.

Esercizio (Prima Legge di De Morgan). Siano P e Q proposizioni. Si provi che $\neg(P \wedge Q)$ è logicamente equivalente a $\neg P \vee \neg Q$.

Soluzione. Basta confrontare le due tavole di verità:

P	Q	$P \wedge Q$	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
V	V	V	F	F	F	F
V	F	F	F	V	V	V
F	V	F	V	F	V	V
F	F	F	V	V	V	V

Poiché, per qualsiasi assegnazione dei valori di verità a P ed a Q, il val;ore di verità assunto da $\neg(P \wedge Q)$ coincide con quello assunto da $\neg P \vee \neg Q$, si conclude che le due proposizioni sono logicamente equivalenti.

Introduciamo ora un connettivo logico $\leftrightarrow$ (che leggeremo "se e solo se"), che esprima *l'equivalenza logica* tra due proposizioni. Precisamente, definiamo $P \leftrightarrow Q$ come $(P \rightarrow Q) \wedge (Q \rightarrow P)$. La tavola di verità del connettivo $\leftrightarrow$ (che si ricava da quelle di $\wedge$ e di $\rightarrow$) è:

se e solo se

P	Q	P $\leftrightarrow$ Q
V	V	V
V	F	F
F	V	F
F	F	V

Fatto questo, è facile osservare che *due proposizioni (composte) A e B sono logicamente equivalenti se e soltanto se $A \leftrightarrow B$ è una tautologia.*

1.6 Esercizi.

Esercizio 1.1. Si dica quali fra le seguenti affermazioni sono corrette.

1) $\emptyset \in \{\emptyset, 2\}$;
2) $\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$;
3) $\emptyset \subseteq \{\emptyset, \{\emptyset\}\}$;
4) $\{1\} \in \{1, 2\}$;
5) $\{\{1\}\} \subseteq \{1, 2\}$;
6) $\emptyset = \{\ x \mid x \in \mathbb{Z}, x^2 < 1\ \}$;
7) $\emptyset = \{\ x \mid \{1, x\} = \{1, 2, 3\}\ \}$;

Esercizio 1.2. Si descrivano gli insiemi $\mathcal{P}(\{1, 2, 3, 4\})$, e $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$

Esercizio 1.3. Siano A, B insiemi. Si dimostri che $A \subseteq B$ se e solo se $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Esercizio 1.4. Si cerchi di dimostrare (eventualmente aiutandosi con i diagrammi di Wenn) le uguaglianze tra insiemi degli enunciati delle Proposizioni 1.3.1, 1.3.2 e 1.3.3.

Esercizio 1.5. Siano A, B e C insiemi. Si provi che $(A \cup B) \cap C = A \cup (B \cap C)$ se e solo se $A \subseteq C$.

Esercizio 1.6. Siano A e B insiemi. Si provi che

$$P(A) \cap P(B) = P(A \cap B)$$

$$P(A) \cup P(B) \subseteq P(A \cup B);$$

e si mostri che, nel caso della unione, in genere non vale l'uguaglianza.

Esercizio 1.7. Siano A e B insiemi. Si provi che $A \setminus B = B \setminus A$ se e solo se $A = B$.

Esercizio 1.8. Siano A e B insiemi. Si provi che $A \setminus (A \setminus B) = A \cap B$.

Esercizio 1.9. Per ogni intero $n > 0$, sia $D_n = \{d \mid d \in \mathbb{Z}$ e d divide $n\}$. Si provi che

$$\bigcup_{0<n\in\mathbb{N}} (\mathbb{Z} \setminus D_n) = \mathbb{Z} \setminus \{1, -1\}.$$

Esercizio 1.10. Siano A, B e C insiemi. Si provi che

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

Esercizio 1.11. Siano A e B insiemi. Si dimostri che $(A \setminus B) \cup (A \cap B) = A$.

Esercizio 1.12. Siano X, Y insiemi. Si dimostri che le seguenti condizioni sono equivalenti:

$$1)\ X \setminus Y = X \qquad 2)\ Y \setminus X = Y \qquad 3)\ X \cap Y = \emptyset$$

Esercizio 1.13. Siano A, B, C insiemi. Si provi che $\mathcal{P}(A \setminus (B \cup C)) = \mathcal{P}(A \setminus B) \cap \mathcal{P}(A \setminus C)$.

Esercizio 1.14. Siano A, B e C insiemi. Si provi che $A \setminus B = A \setminus C$ se e solo se $A \cap B = A \cap C$.

Esercizio 1.15. Sia $\mathbb{N}_o$ l'insieme dei numeri naturali diversi da zero.
Per ogni $n \in \mathbb{N}_o$, sia $B_n = \{\ x | x \in \mathbb{R}$ e $\frac{1}{n} \leq |x| \leq n\ \}$. Si determinino:

$$\bigcup_{n\in\mathbb{N}_o} B_n \qquad \text{e} \qquad \bigcap_{n\in\mathbb{N}_o} B_n.$$

Esercizio 1.16. Sia $\mathbb{N}_o$ l'insieme dei numeri naturali diversi da zero.
Per ogni $n \in \mathbb{N}_o$, sia $A_n = \{\ x | x \in \mathbb{Q}$ e $nx \in \mathbb{Z}\ \}$. Si determinino:

$$\bigcup_{n\in\mathbb{N}_o} A_n \qquad \text{e} \qquad \bigcap_{n\in\mathbb{N}_o} A_n.$$

Esercizio 1.17. 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.

Esercizio 1.18. (*Seconda Legge di De Morgan*) Siano P e Q proposizioni. Si provi che $\neg(P \vee Q)$ è logicamente equivalente a $\neg P \wedge \neg Q$.

Esercizio 1.19. 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.

Esercizio 1.20. Siano P, Q ed R proposizioni. Si scriva la tavola di verità della proposizione $((\neg P \wedge Q) \rightarrow R) \leftrightarrow (R \rightarrow ((\neg Q \vee P))$.

Capitolo 2

Applicazioni

2.1 Applicazioni.

applicazioni

Siano A e B insiemi. Un'**applicazione** (o **funzione**) di A in B è una legge che ad **ogni** elemento di A associa, o fa corrispondere, **uno ed un solo** elemento dell'insieme B. Per dire che f è una applicazione di A in B si scrive

$$f: \ A \longrightarrow B.$$

e, se all'elemento $a \in A, f$ fa corrispondere l'elemento $b \in B$, si scrive $b = f(a)$; l'elemento b si chiama allora *immagine* di a tramite f.

Questa notazione si riferisce ad una generica applicazione di A in B. Volendo descrivere invece una specifica applicazione occorre anche enunciare la legge che agli elementi di A associa elementi di B. È conveniente illustrare le notazioni in questo caso mediante un esempio. Supponiamo di volere introdurre la applicazione (che vogliamo chiamare f) dall'insieme dei numeri interi nell'insieme dei numeri naturali che ad ogni numero intero associa il suo quadrato. Si usa allora uno dei due schemi seguenti:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & z & \mapsto & z^2 \end{array}$$

oppure

$$f: \ \mathbb{Z} \longrightarrow \mathbb{N} \quad \text{è l'applicazione definita da, per ogni } z \in Z, \ f(z) = z^2.$$

dominio e codominio

Se $f: \ A \longrightarrow B$ è una applicazione, si dice che A è il **dominio** di f e che B è il **codominio** di f. Per ogni elemento a del dominio, $f(a)$ si chiama l'immagine di a (tramite f). Si osservi che $f(a)$ deve essere definita per **ogni** elemento $a \in A$.

Due applicazioni, $f: A \longrightarrow B$ e $g: A' \longrightarrow B'$, sono **uguali** se

$$A = A' \ , \ B = B' \ \text{ e per ogni } \ a \in A \ \text{ si ha } \ f(a) = g(a).$$

Nota. Questa definizione di uguaglianza tra applicazioni richiede, forse, un commento. Per definire un'applicazione o funzione $f : A \to B$ non è necessario specificare la "modalità", o l'eventuale algoritmo, mediante la quale per ogni elemento $a \in A$ si "trova" (o si cotruisce, o si determina) il corrispondente elemento $f(a) \in B$, cosa che anzi a volte non è possibile fare; l'importante è che sia stabilito in modo chiaro e univoco quale sia il corrispondende in B di ciascun elemento di A (il che non significa che si sia effettivamente in grado di detrminarlo - qualunque cosa ciò significhi - caso per caso). Pertanto, due applicazioni dall'inseme A all'insieme B sono la "stessa applicazione" se e soltanto se ad ogni elemento di $a \in A$ fanno corrispondere lo stesso elemento di $b \in B$, indipendendemente da come ciascuna arriva in pratica da a a b.

Ad esempio, se P è l'insieme dei punti di un piano, e $\mathcal{C}$ è l'insieme di tutte le circonferenze sullo stesso piano, possiamo definire una applicazione $\mathcal{C} \to P$ che ad ogni circonferenza assegna il suo centro: il modo geometrico con cui si trova il centro di una circonferenza non è parte della definizione. Oppure, sempre sullo stesso piano P possiamo fissare un'origine O, e quindi definire due applicazioni $f, g : P \to P$, stabilendo che ad ogni punto a del piano l'applicazione f associa il punto che si ottiene mediante una rotazione con centro O di 370^o in senso antiorario, mentre g associa il punto che che si ottiene mediante una rotazione con centro O di 90^o in senso orario; poiché – come si vede facilmente – a ciascun punto del piano f e g finiscono per associare entrambe un medesimo punto, si ha che f e g sono la stessa applicazione: $f = g$.

---

immagini

Ancora, un po' di ulteriore e utile terminologia che si incontra in questo contesto. Sia $f : A \longrightarrow B$ un'applicazione, e sia $S \subseteq A$. Si chiama **immagine** di S tramite f, e si denota con $f(S)$, il sottoinsime di B i cui elementi sono le immagini degli elementi di S; quindi

$$f(S) = \{ \ f(a) \mid a \in S \ \}.$$

L'immagine $f(A)$ dell'intero dominio di f, si chiama semplicemente **immagine di** f, e si denota anche con $Im(f)$. Si tenga sempre ben presente che, per ogni sottoinsieme non vuoto S di A, $f(S)$ è un **sottoinsime non vuoto** di B; ad esempio, se $a \in A$ e $S = \{a\}$, allora $f(S) = \{f(a)\}$.

Esempio. Sia $f: \mathbb{Z} \longrightarrow \mathbb{N}$ l'applicazione definita da, per ogni $x \in \mathbb{Z}: \ f(x) = x^2 + 1$; e sia $S = \{0, 1, -1\}$. Allora

$$f(S) = \{f(0), f(1), f(-1)\} = \{1, 2, 2\} = \{1, 2\} \ ,$$

$$Im(f) = \{ \ x^2 + 1 \mid x \in Z \ \} = \{1, 2, 5, 10, 17, 26, 37, 50, \ldots\}.$$

immagini inverse

Sia $f : A \longrightarrow B$ un'applicazione, e sia $Y \subseteq B$. Si chiama **immagine inversa** di Y (o controimmagine, o retroimmagine di Y) tramite f, e si denota con $f^{-1}(Y)$, il sottoinsime di A costituito dagli elementi di A la cui immagine tramite f appartiene a Y; quindi

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

Chiaramente: $f^{-1}(B) = A$. Si tenga ben presente che, per ogni sottoinsime Y di B, $f^{-1}(Y)$ é sempre un **sottoinsime** di A che, come si vede anche da alcuni degli esempi forniti, può essere vuoto.

Esempio. Sia $f : \mathbb{Z} \longrightarrow \mathbb{N}$ l'applicazione definita da, per ogni $x \in \mathbb{Z}$: $f(x) = x^2$.

- sia $Y = \{4\}$; allora $f^{-1}(Y) = \{2, -2\}$;
- sia $Y = \{3, 5, 8\}$; allora $f^{-1}(Y) = \emptyset$;
- sia $Y = \{0, 1, 2, 3\}$; allora $f^{-1}(Y) = \{0, 1, -1\}$;
- sia Y l'insieme dei numeri primi; allora $f^{-1}(Y) = \emptyset$.

Nota. Osserviamo, lasciandone la facile verifica come esercizio, che data una applicazione $f : A \longrightarrow B$ e $S \subseteq A$, $Y \subseteq B$, allora:

$$S \subseteq f^{-1}(f(S)) \qquad \text{e} \qquad f(f^{-1}(Y) \subseteq Y.$$

---

applicazioni suriettive

Un'applicazione $f : A \longrightarrow B$ si dice **suriettiva** se

$$\textit{per ogni } b \in B \textit{ esiste un } a \in A \textit{ tale che } f(a) = b.$$

Se $f : A \longrightarrow B$ è un'applicazione, si definisce *immagine* di f (e si denota con $Im(f)$ oppure $f(A)$) l'insieme degli elementi del codominio B che sono immagine di qualche elemento di A (ovvero: l'insieme dei $b \in B$ tali che esista $a \in A$ con $f(a) = b$).

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

Quindi, un'aplicazione $f : A \longrightarrow B$ è suriettiva se e soltanto se $B = f(A)$. Inoltre, a partire da un'applicazione $f : A \longrightarrow B$, è sempre possibile definire in modo naturale un'applicazione suriettiva $\overline{f} : A \longrightarrow f(A)$ ponendo, per ogni $x \in A$, $\overline{f}(x) = f(x)$.

Esempi. 1) L'applicazione definita in precedenza:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & z & \mapsto & z^2 \end{array}$$

non è suriettiva: infatti $2 \notin Im(f)$ (naturalmente, in questo caso, molti altri elementi del codominio $\mathbb{N}$ non sono immagine di alcun elemento del dominio tramite f $(3, 5, 6, \text{etc.})$; per provare che f non è suriettiva basta evidenziarne uno). Invece, l'applicazione

$$\begin{array}{rccc} q: & \mathbb{R} & \longrightarrow & \mathbb{R}_{\geq 0} \\ & z & \mapsto & z^2 \end{array}$$

(dove con $\mathbb{R}_{\geq 0}$ denotiamo l'insieme dei numeri reali positivi) è suriettiva: infatti ogni numero reale positivo b è il quadrato di un numero reale (in matematica dire "è il quadrato di un numero..." significa "è il quadrato di *almeno un* numero..."). Se $b > 0$ allora b è il quadrato di due numeri reali distinti di segno opposto; indicheremo sempre con $\sqrt{b}$ la radice quadrata positiva di b).

2) L'applicazione *valore assoluto* $f : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$ definita da, per ogni $x \in \mathbb{R}$:

$$f(x) = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

è suriettiva (si osservi che il valore assoluto non è "il numero senza segno" - espressione che non ha un significato preciso).

Esercizio. Sia X un insieme non vuoto e sia $Y \subseteq X$ (fissato). Definiamo l'applicazione $\delta : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$, ponendo, per ogni $A \in \mathcal{P}(X)$: $\delta(A) = A \Delta Y$. Provare che δ è suriettiva.

Soluzione. Bisogna provare che per ogni elemento $B \in \mathcal{P}(X)$ (il codominio di δ) esiste un $A \in \mathcal{P}(X)$ (il dominio di δ) tale che $B = \delta(A)$. Ora, posto un tale B, prendendo $A = B \Delta Y$, si ha (applicando le proprietà della diffferenza simmetrica):

$$\delta(A) = A \Delta Y = (B \Delta Y) \Delta Y = B \Delta (Y \Delta Y) = B \Delta \emptyset = B$$

come si voleva. Quindi δ è un'applicazione suriettiva.

---

applicazioni iniettive

Un'applicazione $f : A \longrightarrow B$ si dice **iniettiva** se

$$\textit{per ogni } x, y \in A : \quad \textit{se } \ x \neq y \ \ \textit{allora } \ f(x) \neq f(y).$$

Equivalentemente (ed è questo ciò che usualmente si adotta in pratica) $f : A \longrightarrow B$ è iniettiva se e solo se

$$\textit{per ogni } x, y \in A : \quad \textit{se } \ f(x) = f(y) \ \textit{ allora } \ x = y.$$

Esempi. 1) L'applicazione $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definita da, per ogni $x \in \mathbb{Z}$, $f(x) = x^2$; non è iniettiva: infatti, ad esempio, $f(-1) = 1 = f(1)$.

2) L'applicazione $g : \mathbb{N} \longrightarrow \mathbb{Z}$ definita da, per ogni $x \in \mathbb{Z}$: $f(x) = x^2$, è iniettiva: infatti, se x, y sono numeri naturali tali che $x^2 = y^2$, allora $x = y$.

Esercizio. Sia X un insieme non vuoto e sia $Y \subseteq X$ (fissato). Consideriamo di nuovo l'applicazione $\delta : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$, ponendo, per ogni $A \in \mathcal{P}(X)$: $\delta(A) = A\Delta Y$, e proviamo che δ è iniettiva.

Soluzione. Siano $A, A_1 \in \mathcal{P}(X)$ (il dominio di δ) e supponiamo che $\delta(A) = \delta(A_1)$; proviamo che $A = A_1$. Per definizione di δ si ha $A\Delta Y = A_1\Delta Y$. Sia $x \in A$. Se $x \notin Y$, allora

$$x \in A \setminus Y \subseteq A\Delta Y = A_1\Delta Y = (A_1 \setminus Y) \cup (Y \setminus A_1)$$

e siccome $x \notin Y \setminus A_1$, deve essere $x \in A_1 \setminus Y \subseteq A_1$. Se invece $x \in Y$, allora $x \in A \cap Y$, e in particolare, $x \notin A\Delta Y = A_1\Delta Y$; quindi $x \in Y \cap A_1$, e dunque $x \in A_1$. Pertanto, in ogni caso $x \in A_1$. Questo prova che $A \subseteq A_1$. Allo stesso modo si prova che $A_1 \subseteq A$. Dunque $A = A_1$, e ciò prova che δ è un'applicazione iniettiva.

applicazioni biettive

Un'applicazione $f : A \longrightarrow B$ si dice **biettiva** se è sia iniettiva che suriettiva. Le applicazioni biettive realizzano quelle che spesso sono chiamate *corrispondenze biunivoche*.
Si tratta di un concetto basilare: come vedremo più avanti le applicazioni biettive sono quelle che si possonoinvertire. Per il momento vediamone alcuni esempi.

Esempi. 1) Sia D l'insieme dei numeri naturali *dispari*, e sia $f : \mathbb{Z} \longrightarrow D$, l'applicazione definita da, per ogni $n \in \mathbb{Z}$, $f(n) = 1 - 2n$.
Allora, f è iniettiva; infatti, per ogni $n, m \in \mathbb{Z}$,

$$f(n) = f(m) \;\Rightarrow\; 1 - 2n = 1 - 2m \;\Rightarrow 2n = 2m \;\Rightarrow\; n = m.$$

f è suriettiva. Sia, infatti, $d \in D$, allora $d-1$ è un numero pari, e quindi $(d-1)/2 \in \mathbb{Z}$; prendendo $n = -(d-1)/2$, si ha

$$f(n) = 1 - 2n = 1 - 2\frac{1-d}{2} = d,$$

il che prova che f è suriettiva. Poiché F è sia iniettiva che suriettiva, f è una biezione.

2) Sia $a \in \mathbb{Q}$ un numero razionale fissato. Poniamo $A = \mathbb{Q} \setminus \{a\}$, e $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Sia quindi $g : A \longrightarrow \mathbb{Q}^*$, l'applicazione definita da, per ogni $x \in A$,

$$g(x) = \frac{3}{a-x}.$$

g è iniettiva; infatti, per ogni $x, y \in A$,

$$g(x) = g(y) \;\Rightarrow\; \frac{3}{a-x} = \frac{3}{a-y} \;\Rightarrow\; a - x = a - y \;\Rightarrow\; x = y.$$

g è suriettiva; sia $y \in \mathbb{Q}$, ci chiediamo se esiste $x \in A$ tale che $y = g(x) = 3/(a-x)$, ovvero x è tale che $a - x = 3/y$. Ora, poiché $y \neq 0$ è razionale, anche $x = a - \frac{3}{y}$ è razionale, inoltre, poiché $y \neq 0$, $x \neq a$. Quindi $x = a - \frac{3}{y} \in A$, e

$$g(x) = \frac{3}{a - (a - \frac{3}{y})} = y.$$

Dunque g è suriettiva, e pertanto biettiva.

2.2 Composizione di applicazioni.

composizione

Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$, due applicazioni (si osservi che si assume che il dominio di g coincida col codominio di f). L'**applicazione composta** $g \circ f$ (si legge f composta g) è l'applicazione

$$g \circ f \ : \ A \ \longrightarrow \ C$$

definita da, per ogni $a \in A$: $(g \circ f)(a) = g(f(a))$. In termini discorsivi, l'applicazione composta $g \circ f$ è l'applicazione che si ottiene applicando prima f e, di seguito, g.

Esempi. 1) Sia $\mathbb{R}_{\geq 0}$ l'insieme dei numeri reali maggiori o uguali a zero (che spesso si denota anche con $[0, +\infty]$). La funzione logaritmo è un'applicazione $log : \mathbb{R}_{\geq 0} \to \mathbb{R}$, che ad ogni $x \in \mathbb{R}_{\geq 0}$ associa $log\, x$ (il logaritmo naturale in base e). Sia $q : \mathbb{R} \to \mathbb{R}_{\geq 0}$ è l'applicazione definita da $q(x) = x^2$; allora la composizione $q \circ log : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, è la funzione che, di solito (e un poco impropriamente), si denota con log^2: per ogni $x \in \mathbb{R}_{\geq 0}$,

$$(q \circ log)(x) = (log\, x)^2 = log^2 x.$$

Mentre $log \circ q : \mathbb{R} \to \mathbb{R}$ è la funzione data da, per ogni $x \in \mathbb{R}$,

$$(log \circ q)(x) = log(x^2).$$

2) Siano $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definita da $f(z) = |z|$; $g : \mathbb{N} \longrightarrow \mathbb{Z}$ definita da $f(x) = -x$; allora

$g \circ f : \ \mathbb{Z} \longrightarrow \mathbb{Z}$ è tale che, per ogni $z \in \mathbb{Z} : \ g \circ f(z) = g(f(z)) = g(|z|) = -|z|$;
$f \circ g : \ \mathbb{N} \longrightarrow \mathbb{N}$ è tale che, per ogni $x \in \mathbb{N} : \ f \circ g(x) = f(g(x)) = f(-x) = |-x| = x$;

(l'ultima uguaglianza deriva dal fatto che, poichè $x \in \mathbb{N}$, x è positivo).

Gli esempi precedenti mostrano anche che, in generale, $g \circ f \neq f \circ g$. Dunque la composizione di applicazioni non è un'operazione commutativa. Tuttavia, come mostra la prossima proposizione, essa è associativa.

Proposizione 2.2.1. *Siano A, B, C, D insiemi; $f : A \to B$, $g : B \to C$, $h : C \to D$ applicazioni. Allora*

associatività

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

Dimostrazione. Innanzi tutto osserviamo che sia $h \circ (g \circ f)$ che $(h \circ g) \circ f$ sono applicazioni con dominio A e codominio D. Ora, per ogni $a \in A$:

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

Quindi $h \circ (g \circ f) = (h \circ g) \circ f$. ■

Sia A un insieme. L'applicazione che ad ogni elemento di A associa se stesso si chiama **identità** (o applicazione identica) di A , e si denota con ι_A o con 1_A. Quindi:

appl. identica

$$\begin{array}{rccc} \iota_A : & A & \longrightarrow & A \\ * & a & \mapsto & a \end{array}$$

Per esempio l'applicazione dal piano P in sé che ad ogni punto del piano associa il punto che si ottiene mediante una rotazione di un angolo giro completo attorno ad un'origine fissata, è l'identità ι_P.

Proposizione 2.2.2. *Siano A, B insiemi; $f : A \longrightarrow B$ un'applicazione; ι_A, ι_B le applicazioni identiche su A e su B rispettivamente. Allora*

(1) $\iota_B \circ f = f$;

(2) $f \circ \iota_A = f$.

Un'applicazione $f : A \longrightarrow B$ si dice **invertibile** se esiste un'applicazione $g : B \longrightarrow A$ tale che

applicazioni invertibili

$$g \circ f = \iota_A \quad \text{e} \quad f \circ g = \iota_B.$$

Cominciamo col provare che se un'applicazione è invertibile, allora ha un'unica inversa.

Proposizione 2.2.3. . *Sia $f : A \longrightarrow B$ una applicazione; supponiamo che esistano applicazioni g, $h : B \longrightarrow A$ tali che $g \circ f = \iota_A$ e $f \circ h = \iota_B$. Allora $g = h$.*

Dimostrazione. Siano f, g e h come nelle ipotesi. Allora,

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

quindi $h = g$. ■

Da questa Proposizione segue l'importante osservazione che *appl. inversa*

se $f : A \to B$ è invertibile esiste una **unica** *applicazione $g : B \longrightarrow A$ tale che*
$$g \circ f = \iota_A \qquad e \qquad f \circ g = \iota_B.$$

Tale applicazione g si chiama l'applicazione **inversa** di f , e si denota con f^{-1}.

Vogliamo ora capire (aiutandoci con i diagrammi di Wenn) quali applicazioni siano invertibili. Immaginiamo quindi di avere data una applicazione $f : A \to B$ che sia invertibile, e sia $g : B \to A$ la sua inversa.
Allora, in primo luogo, $f \circ g = i_B$; ovvero per ogni elemento b di B, applicando prima g (ottenendo $g(b) \in A$) e quindi f, si deve tornare al medesimo b. Cioè: $f(g(b)) = b$.

Questo in particolare ci dice che ogni elemento di B dev'essere immagine di qualche elemento di a, ovvero che f è suriettiva. Dunque: *condizione necessaria perché un'applicazione f sia invertibile, è che f sia suriettiva.* Questa condizione non è però sufficiente. Ad esempio l'applicazione da $\mathbb{Z}$ in $\mathbb{N}$ che ad ogni numero intero associa il suo valore assoluto, è suriettiva ma non è invertibile.
Per giungere ad una condizione sufficiente per l'invertibilità dobbiamo integrare la condizione sulla suriettività con un'altra condizione necessaria che si ricava dall'altra relazione fra le applicazioni inverse f e g, ovvero da $g \circ f = \iota_A$. Supponiamo che esitano due elementi $a, a' \in A$ con $a \neq a'$ e tali che $f(a) = b = f(a')$; allora, se f avesse un'inversa g dovrebbe essere

$$a = \iota_A(a) = (g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a') = \iota_A(a') = a'$$

che è assurdo (vedi disegno). Dunque, se esiste g, allora per ogni $a, a' \in A$ con $a \neq a'$, deve essere che $f(a) \neq f(a')$. Questa è una seconda condizione necessaria per l'invertibilità di f che si esprime dicendo che f è iniettiva.

Tornando alla questione dell'invertibilità di una applicazione $f : A \to B$, abbiamo quindi trovado che condizione necessaria è che f sia sia suriettiva che biettiva. Un'applicazione con queste proprietà si dice **biettiva**.

appl. biettive

Si può provare ora che questa condizione (la biettività di f) è anche *sufficiente* a che f ammetta un'inversa. Dunque si ha

Teorema 2.2.4. *Una applicazione è invertibile se e soltanto se è biettiva.*

Quindi, il concetto di applicazione biettiva è fondamentale; le applicazioni biettive sono quelle che si possono 'invertire'.

Esempi. 1) È biettiva (e quindi invertibile) l'applicazione $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, definita da, per ogni $x \in \mathbb{Z} :\ f(x) = x + 2$; la sua inversa è l'applicazione $g : \mathbb{Z} \longrightarrow \mathbb{Z}$, definita da, per ogni $x \in \mathbb{Z} :\ g(x) = x - 2$.

2) L'applicazione $\delta :\ \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ considerata in precedenti esempi (si fissa un $Y \subseteq X$, e quindi si pone, per ogni $A \in \mathcal{P}(X),\ \delta(A) = A\Delta Y$), è biettiva in quanto, come abbiamo visto, è suriettiva e iniettiva. Essa coincide con la sua inversa; infatti, per ogni $A \in \mathcal{P}(X)$,

$$(\delta \circ \delta)(A) = \delta(\delta(A)) = \delta(A\Delta Y) = (A\Delta Y)\Delta Y = A\Delta(Y\Delta Y) = A\Delta\emptyset = A.$$

3) Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ definita da, per ogni $x \in \mathbb{Q} :\ f(x) = 2x - 1$. Si verifica senza difficoltà che f è biettiva. Determiniamo la sua inversa $f^{-1} : \mathbb{Q} \longrightarrow \mathbb{Q}$. Poichè $f \circ f^{-1}$ deve essere la applicazione identica su $\mathbb{Q}$, si dovrá avere, per ogni $y \in \mathbb{Q}$,

$$y = f(f^{-1}(y)) = 2 \cdot f^{-1}(y) - 1$$

da cui, risolvendo una elementare equazione, si ricava:

$$f^{-1}(y) = \frac{y+1}{2}\ , \quad \text{per ogni } y \in \mathbb{Q}$$

che è la regola che definisce la applicazione inversa $f^{-1} : \mathbb{Q} \longrightarrow \mathbb{Q}$.

4) Sia $A = \mathbb{Q} \setminus \{1\}$ e sia $f : A \longrightarrow A$ definita da, per ogni $x \in A\ :\ f(x) = \frac{x+1}{x-1}$. Allora f è invertibile e coincide con la propria inversa. Infatti, per ogni $x \in A$ si ha :

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

quindi $f \circ f = \iota_A$ e dunque $f^{-1} = f$.

Vediamo ora alcune importanti proprietà relative alla composizione di applicazioni iniettive e/o suriettive, ed alle loro evenmtuali inverse. Le dimostrazioni possono essere omesse.

Proposizione 2.2.5. *Siano* $f : A \longrightarrow B$ *e* $g : B \longrightarrow C$ *due applicazioni. Allora* *comp. di appl. biettive*

(1) *se* f *e* g *sono iniettive, allora* $g \circ f$ *è iniettiva ;*

(2) *se* f *e* g *sono suriettive, allora* $g \circ f$ *è suriettiva ;*

(3) *se* f *e* g *sono biettive, allora* $g \circ f$ *è biettiva.*

Dimostrazione. (1) Siano f e g iniettive, e siano $a, a' \in A$ tali che

$$(g \circ f)(a) = (g \circ f)(a') \ ,$$

ciò significa : $g(f(a)) = g(f(a'))$. Quindi, poichè g è iniettiva:

$$f(a) = f(a')$$

da cui, poichè f è iniettiva :

$$a = a'$$

provando pertanto che $g \circ f$ è iniettiva.

(2) Siano f e g suriettive, e sia $c \in C$. Poichè g è suriettiva, esiste $b \in B$ tale che $c = g(b)$, e, poichè f è suriettiva, esiste $a \in A$ tale che $b = f(a)$. Ma allora:

$$g \circ f(a) = g(f(a)) = g(b) = c$$

provando pertanto che $g \circ f$ è suriettiva.

(3) Segue immediatamente dai punti (1) e (2). ∎

Proposizione 2.2.6. *Siano* $f : A \longrightarrow B$ *e* $g : B \longrightarrow C$ *due applicazioni invertibili. Allora:* *inversa della composta*

(1) f^{-1} *è invertibile e* $(f^{-1})^{-1} = f$ *;*

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

Dimostrazione. (1) è ovvia. Dimostriamo (2). Poichè f e g sono invertibili, esse sono biettive per il Teorema 2.2.4, quindi, per la Proposizione 8, $g \circ f : A \longrightarrow C$ è biettiva e dunque, ancora per il Teorema 2.2.4, è invertibile. Ora, osserviamo che:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = (g \circ (f \circ f^{-1})) \circ g^{-1} = (g \circ \iota_B) \circ g^{-1} = g \circ g^{-1} = \iota_C$$

ed allo stesso modo :

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (\iota_B \circ f) = f^{-1} \circ f = \iota_A$$

Dunque, per la unicità della applicazione inversa, $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$. ∎

2.3 Esercizi.

Esercizio 2.1. Si dica quali fra le seguenti applicazioni sono suriettive.

(a) $f: \mathbb{N} \longrightarrow \mathbb{N}$ definita da: $f(x) = 3x$, per ogni $x \in \mathbb{N}$.

(b) $g: \mathbb{Q} \longrightarrow \mathbb{Q}$ definita da: $g(x) = \frac{x-2}{2}$, per ogni $x \in \mathbb{Q}$.

(c) $h: \mathbb{N} \longrightarrow \mathbb{Q}^+$ definita da: $h(x) = \frac{n}{n+1}$, per ogni $x \in \mathbb{N}$.
(dove $\mathbb{Q}^+ = \{x \mid x \in \mathbb{Q}, 0 < x\}$).

(d) $\eta : \mathbb{N} \longrightarrow \mathbb{N}$, definita da:

$$\eta(n) = \begin{cases} 2n & \text{se } n \text{ è pari} \\ 3n & \text{se } n \text{ è dispari} \end{cases}$$

Esercizio 2.2. Si dica quali fra le applicazioni dell'esercizio precedente sono iniettive.

Esercizio 2.3. Si dimostri che l'applicazione $f: \mathbb{N} \longrightarrow \mathbb{Z}$ definita da:

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

è biettiva.

Esercizio 2.4. 1) Si dimostri che l'applicazione

$$\begin{array}{rcl} f: \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \times \mathbb{Z} \\ (x, y) & \mapsto & (3x + 4y, x + 2y) \end{array}$$

è iniettiva ma non suriettiva.

Esercizio 2.5. Sia $f: A \longrightarrow B$ una applicazione, e siano $S, T \subseteq A$. Si provi che

$$\begin{array}{ll} (1) & f(S \cup T) = f(S) \cup f(T); \\ (2) & f(S \cap T) \subseteq f(S) \cap f(T); \\ (3) & f(S) \setminus f(T) \subseteq f(S \setminus T); \end{array}$$

e si mostri, mediante opportuni esempi che le inclusioni ai punti $(2), (3)$ possono essere proprie.

Esercizio 2.6. Siano $f_1, f_2, f_3 : \mathbb{Z} \to \mathbb{Z}$ le applicazioni definite da, per ogni $x \in \mathbb{Z}$,

$$f_1(x) = 2x + 1 \qquad f_2(x) = (x-1)^2 \qquad f_3(x) = x^2 + 1.$$

Si descrivano le applicazioni composte $f_2 \circ f_1$, $f_2 \circ f_3$, $f_1 \circ f_3$, e $f_3 \circ f_2 \circ f_1$.

Esercizio 2.7. Si dimostri che l'applicazione

$$\begin{array}{rcl} f & : & \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}\times\mathbb{Q} \\ & & (x,y) \mapsto (3x+4y, x+2y) \end{array}$$

è biettiva, e si determini la sua inversa.

Esercizio 2.8. Si dimostri che l'applicazione $h : \mathbb{Q} \longrightarrow \mathbb{Q}$, definita da: $h(x) = 3x - |x|$, per ogni $x \in \mathbb{Q}$, è biettiva, e si determini la sua inversa.

Esercizio 2.9. Siano $f : \mathbb{Q}\setminus\{0\} \longrightarrow \mathbb{Q}\setminus\{0\}$ e $g : \mathbb{Q}\setminus\{0\} \longrightarrow \mathbb{Q}\setminus\{1\}$ applicazioni definite da:

$$f(x) = \frac{1}{x} \quad \text{e} \quad g(x) = x+1\ , \quad \text{per ogni } x \in \mathbb{Q}\setminus\{0\}\ .$$

Si provi che l'applicazione composta $g \circ f$ è biettiva e si determini la sua inversa.

Esercizio 2.10. Sia X un insieme non vuoto e siano f, g due applicazioni di X in X. Si provi che se $f^{-1}(\{y\}) \subseteq g^{-1}(\{y\})$ per ogni $y \in X$, allora $f = g$.

Esercizio 2.11. Sia $f : \mathbb{N} \longrightarrow \mathbb{N}$, definita da, per ogni $n \in \mathbb{N}$:

$$f(n) = \begin{cases} \frac{n}{3} & \text{se} \quad 3|n \\ 3n-1 & \text{se} \quad 3 \not| n \end{cases}$$

Si provi che f è suriettiva ma non iniettiva.

Esercizio 2.12. Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$ due applicazioni. Si dimostri che:

(i) se $g \circ f$ è iniettiva , allora f è iniettiva;

(ii) se $g \circ f$ è suriettiva , allora g è suriettiva.

Si completi poi la analisi, trovando degli esempi in cui g non è iniettiva ma $g \circ f$ è iniettiva, e in cui f non è suriettiva ma $g \circ f$ è suriettiva.

Esercizio 2.13. Sia A un insieme e $f, g : A \longrightarrow A$ applicazioni. Si dimostri che:

a) Se f è suriettiva e $g \circ f = f$ allora $g = \iota_A$.

b) Se f è iniettiva e $f \circ g = f$ allora $g = \iota_A$.

Esercizio 2.14. Siano X, Y insiemi non vuoti, e sia $f : X \longrightarrow Y$ un'applicazione. Si dimostri che f è iniettiva se e solo se per ogni $T \subseteq X$, $f(X \setminus T) \subseteq Y \setminus f(T)$.

Esercizio 2.15. Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ l'applicazione definita da, per ogni $x \in \mathbb{Q}$, $f(x) = x - |\frac{x}{2}|$. Provare che f è biettiva e determinare f^{-1}.

Esercizio 2.16. Sia D l'insieme dei numeri interi dispari, e sia $f : \mathbb{Z} \longrightarrow D$ l'applicazione definita da, per ogni $z \in \mathbb{Z}$:

$$f(z) = \begin{cases} 2z - 1 & \text{se } z \text{ è dispari} \\ 2z + 3 & \text{se } z \text{ è pari} \end{cases}$$

Provare che f è una biezione e determinare f^{-1}.

Esercizio 2.17. Siano $f, g : \mathbb{Z} \to \mathbb{Z}$ due applicazioni date. Si definisca $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ ponendo, per ogni $(a, b) \in \mathbb{Z} \times \mathbb{Z}$:

$$\phi(a, b) = (f(a) + g(b), f(a) - g(b)) \ .$$

(a) Si provi che ϕ è iniettiva se e solo se f, g sono entrambe iniettive.

(b) Si trovino due applicazioni suriettive f, g tali che ϕ non è suriettiva.

Esercizio 2.18. Siano $f, g : \mathbb{N} \to \mathbb{N}$ definite da, per ogni $n \in \mathbb{N}$:

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

$$g(n) = n + 10 \ .$$

(1) Si calcoli $f \circ g$ e $g \circ f$.

(2) Si dica se esiste $h : \mathbb{N} \to \mathbb{N}$ tale che $h \circ f = \iota_{\mathbb{N}}$.

Capitolo 3

I Numeri Interi I

3.1 Il Principio di Induzione.

L'insieme $\mathbb{N}$ dei numeri naturali gode della seguente proprietà (che ci appare ovvia, ma che di fatto è uno degli assiomi di $\mathbb{N}$): *buon ordinamento di* $\mathbb{N}$

ogni sottoinsieme **non vuoto** *di* $\mathbb{N}$ *ha un elemento* **minimo**.

Questa proprietà si esprime dicendo che l'insieme $\mathbb{N}$ è **bene ordinato** (infatti è chiamata *assioma del buon ordinamento*). Ad esempio, rispetto all'ordine naturale, l'insieme dei numeri interi $\mathbb{Z}$, cosi come ogni intervallo $[a, b] \subset \mathbb{R}$ con $a < b$, *non sono* bene ordinati[1], giacché in entrambi i casi è possibile trovare dei sottoinsiemi non vuoti che non hanno minimo (ad esempio $\mathbb{Z}$ stesso nel primo caso, e il sottoinsieme $(a, b] = \{x | x \in \mathbb{R},\ a < x \leq b\}$ nel secondo caso.

Vediamo in azione questo assioma nella dimostrazione di un fatto ben noto, ma importante: la divisione con resto nei numeri interi. *divisione con resto*

Teorema 3.1.1. *Siano* $a, b \in \mathbb{Z}$ *e* $b \neq 0$ *; allora esistono* $q, r \in \mathbb{Z}$ *tali che*

$$a = qb + r \qquad e \qquad 0 \leq r < |b| \ ,$$

Inoltre, assegnati gli interi a, b *allora* q, r *sono univocamente individuati da questa condizione.*

Dimostrazione. Dati $a, b \in \mathbb{Z}$ con $b \neq 0$, consideriamo l'insieme

$$S = \{\ s \in \mathbb{N} \mid s = a - bz \ \text{ per qualche } \ z \in \mathbb{Z}\ \} \ .$$

[1] ricordo che $[a, b] = \{x | x \in \mathbb{R},\ a \leq x \leq b\}$.

Ora, $S \neq \emptyset$; infatti $-b|a| \in \mathbb{Z}$ e, poichè $b^2 \geq 1$, abbiamo $a + b^2|a| \geq 0$, dunque

$$S \ni a - b(-b|a|) = a + b^2|a| \ .$$

Quindi, per il principio del buon ordine di $\mathbb{N}$, l'insieme S ha un minimo; sia r tale minimo. Allora, poichè $r \in S$, esiste $q \in \mathbb{Z}$ tale che $0 \leq r = a - bq$, cioè :

$$a = qb + r.$$

Resta da provare che $r < |b|$. Supponiamo, per assurdo $r \geq |b|$, allora esiste $y \in \mathbb{N}$ tale che $r = |b| + y$; ma allora

$$y = r - |b| = a - bq - |b| = a - b(q \pm 1) \in S$$

e quindi, poichè $r = \min(S)$, deve essere $r \leq y$ che è assurdo.
Dunque $r < |b|$.
La verifica dell'unicità degli interi q, r soddisfacenti alla condizione

$$a = qb + r \qquad e \qquad 0 \leq r < |b| \ ,$$

è lasciata per esercizio. ■

Induzione

Il principio di induzione è un importante strumento deduttivo in teoria dei numeri interi (ma anche in tutti quei casi in cui determinate situazioni possono essere parametrizzate mediante numeri naturali). Esso è logicamente equivalente all'assioma del buon ordinamento dei numeri naturali. *induzione*

Principio di induzione. *Sia $n_0 \in \mathbb{N}$, e supponiamo che per ogni $n \geq n_0$ sia assegnata una proposizione $P(n)$ e che siano soddisfatte le seguenti condizioni:* *principio di induzione*

(1) $P(n_0)$ è vera;

(2) per ogni $n \geq n_0$, se $P(n)$ è vera allora anche $P(n+1)$ è vera.

Allora $P(n)$ è vera per ogni $n \geq n_0$.

Esempio 1. Dimostriamo che, *per ogni numero naturale* $n \geq 1$ si ha: *esempi*

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

in questo caso, $n_0 = 1$ e, per ogni $n \geq 1$ la proposizione $P(n)$ è l'uguaglianza descritta, che, in forma compatta, si scrive

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

Per provare questa affermazione, utilizziamo il principio di induzione. Dobbiamo dunque verificare che l'insieme delle proposizioni $P(n)$ soddisfa alle due condizioni richieste per l'applicazione del principio:

(1) $P(1)$ è vera; infatti essa si riduce a $1 = \frac{1(1+1)}{2}$ che è una uguaglianza vera.

(2) Sia $n \geq 1$ e supponiamo che $P(n)$ sia vera (questa si chiama *ipotesi induttiva*), cioè che

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \ ,$$

e dimostriamo che *allora* anche $P(n+1)$ è vera. Infatti :

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

quindi $P(n+1)$ è vera.

Per il principio di induzione, si ha che $P(n)$ è vera per ogni $n \geq 1$.

Per il prossimo esempio, ricordo la definizione di **fattoriale**: per $n \geq 1$ si definisce *n-fattoriale* come *fattoriale*

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

inoltre si pone, per definizione, $1! = 1$ e $0! = 1$.

Esempio 2. Si provi che per ogni numero naturale $n \geq 1$ si ha $2^{2n}(n!)^2 > (2n)!$.

(1) Si inizia con il provare che l'affermazione vale per $n = 1$; come spesso accade, si tratta di una banale verifica; si ha $2^{2\cdot 1}(1!)^2 = 2^2 = 4$, mentre $(2 \cdot 1)!. = 2! = 1 \cdot 2 = 2$, e dunque $2^{2\cdot 1}(1!)^2 > (2 \cdot 1)!.$ (che è la proposizione per $n = 1$).

(2) Supponiamo ora l'affermazione sia vera per $n \geq 1$; per $n+1$ si ha

$$2^{2(n+1)}((n+1)!)^2 = 2^{2n+2}(n! \cdot (n+1))^2 = 2^2 \cdot 2^{2n} \cdot (n!)^2 \cdot (n+1)^2 = 4(n+1)^2 \cdot \left[2^{2n}(n!)^2\right] ,$$

e quindi, applicando l'ipotesi induttiva:

$$2^{2(n+1)}((n+1)!)^2 > 4(n+1)^2 \cdot (2n)! > (2n+1)(2n+2) \cdot (2n)! = (2(n+1)!).$$

Per il principio di induzione, si conclude che la disuguaglianza è vera per ogni $n \geq 1$.

Nota. Il principio di induzione può anche essere utilizzato per provare proposizioni sull'insieme dei numeri interi, distinguendo il caso dei numeri positivi da quello dei numeri negativi.

Esempio 3. Dimostriamo che, per ogni $z \in \mathbb{Z}$ $z^3 - z$ è divisibile per 6.

Come primo caso, supponiamo $z \geq 0$, utilizzando il principio di induzione.

(1) La affermazione è vera per $n = 0$, infatti

$$0^3 - 0 = 0 = 0 \cdot 6 \ , \text{ cioè } \quad 6 \ \text{ divide } \ 0^3 - 0 \ .$$

(2) Supponiamo la affermazione sia vera per n, cioè che (ipotesi induttiva) 6 divide n^3-n. Allora:

$$(n+1)^3-(n+1) = n^3+3n^2+3n+1-n-1 = (n^3-n)+3n(n+1)$$

è divisibile per 6 dato che 6 divide n^3-n e divide $3n(n+1)$ (quest'ultima affermazione segue dal fatto che $n(n+1)$ è certemente un numero pari).
Quindi per il principio di induzione la nostra affermazione è vera per ogni numero intero $z \geq 0$.
Supponiamo ora $z \in \mathbb{Z}$ e $z \leq 0$; allora $-z \geq 0$ e quindi, per il caso precedente, 6 divide

$$(-z)^3-(-z) = -z^3+z = -(z^3-z)$$

e dunque 6 divide z^3-z, completando la dimostrazione.

Come altro esempio di applicazione del principio di induzione, dimostriamo una formula già enunciata in un capitolo precedente.

Proposizione 3.1.2. *. Sia A un insieme finito; allora $|\mathcal{P}(A)| = 2^{|A|}$.*

Dimostrazione. Sia $n = |A|$, e procediamo per induzione su n.
L'affermazione è vera per $n = 0$, in questo caso infatti $A = \emptyset$ e $|\mathcal{P}(\emptyset)| = 1$.
Supponiamo ora che l'affermazione sia vera per insiemi di ordine n (con $n \geq 0$) e proviamo che allora vale per quelli di ordine $n+1$. Sia A insieme con $|A| = n+1$, allora $A \neq \emptyset$; sia a un fissato elemento di A e sia $B = A \setminus \{a\}$. Ora, ogni sottoinsieme di A è un sottoinsieme di B oppure è del tipo $X \cup \{a\}$ con $X \subseteq B$. Quindi i sottoinsiemi di A sono esattamente il doppio dei sottoinsiemi di B. Ma $|B| = n$ e quindi, per ipotesi induttiva, B ha esattamente 2^n sottoinsiemi. Dunque:

$$|\mathcal{P}(A)| = |B| + |B| = 2^n + 2^n = 2^{n+1}$$

provando che la affermazione è vera per insiemi di ordine $n+1$.
Per il principio di induzione la Proposizione è dimostrata.

---

induzione - 2^a forma

Principio di induzione (2^a forma). *Sia $n_0 \in \mathbb{N}$, e supponiamo che per ogni $n \geq n_0$ sia assegnata una proposizione $P(n)$ e che siano soddisfatte le seguenti condizioni:*

(1) $P(n_0)$ è vera;

(2) per ogni $n \geq n_0$, se $P(t)$ è vera per ogni numero naturale t con $n_0 \leq t \leq n-1$, segue che anche $P(n)$ è vera.

Allora $P(n)$ è vera per ogni $n \geq n_0$.

Anche se apparentemente più forte, questa seconda forma è equivalente alla prima, come si potrebbe facilmente provare. Un caso di applicazione dell'induzione in questa forma è nella dimostrazione del teorema fondamentale dell'aritmetica che vedremo più avanti.

3.2 Rappresentazioni b-adiche.

La nostra usuale rapprentazione decimale dei numeri interi positivi è basata sulla convenzione che la posizione delle diverse cifre "corrisponde" (da destra a sinistra) a potenze crescenti del numero 10; ad esempio, scrivere $n = 3215$ significa

rappres. decimale

$$n = 5 \cdot 10^0 + 1 \cdot 10^1 + 2 \cdot 10^2 + 3 \cdot 10^3.$$

Si tratta cioè di una notazione in base 10. La scelta di 10 è (dal punto di vista matematico) del tutto arbitraria: la stessa cosa può essere fatta scegliendo come base qualunque numero naturale $b \geq 2$. In questo caso c'è bisogno di b simboli distinti per i numeri da 0 a $b-1$, e le cifre (da destra a sinistra) corrispondono alle potenze crescenti di b.

Teorema 3.2.1. *Sia b un numero intero $b \geq 2$. Allora ogni intero positivo n si può scrivere in modo unico nella forma*

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b + a_0,$$

dove $k \geq 0$ è il minimo intero tale che $b^k \leq n < b^{k+1}$, e gli $a_0, a_1, a_2, \ldots, a_k$ sono interi tali che

$$\begin{cases} 0 \leq a_i \leq b-1 \quad \textit{per} \quad i = 0, 1, \ldots, k-1 \\ \\ 1 \leq a_k \leq b-1 \end{cases}$$

Tale rappresentazione di n si chiama rappresentazione in base b, o rappresentazione b-adica, di n. Ad esempio, la rappresentazione 2-adica di $n = 1958$ è

rappres. in base b

$$1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0;$$

si dice anche che

$$11110100110$$

(ovvero, la sequenza delle "cifre" $a_k a_{k-1} \ldots a_2 a_1 a_0$) è la scrittura in base 2 di 1958. La rappresentazione in base 7 dello stesso intero è invece

$$5 \cdot 7^3 + 4 \cdot 7^2 + 6 \cdot 7 + 5$$

e quindi la scrittura 7-adica di 1958 è 5465.

Dimostrazione. Fissata la base $b \geq 2$, sia $n \in \mathbb{N}$. Dimostriamo, per induzione su n, l'esistenza di una rappresentazione b-adica di n e la sua unicità.

Cominciamo con l'esistenza. Se $0 \leq n \leq b-1$, la cosa è ovvia. Sia quindi $n \geq b$. Dividiamo n per b,

$$n = qb + r \qquad \text{con} \quad 0 \leq r \leq b-1.$$

Poiché $n \geq b$, e $b \geq 2$, si ha $1 \leq q < n$. Per ipotesi induttiva

$$q = a'_k b^k + \ldots + a'_2 b^2 + a'_1 b + a'_0$$

con $0 \leq a'_i \leq b-1$ per $i = 0, 1, \ldots, k$ e $a'_k \neq 0$, e dove k è il massimo esponente tale che $b^k \leq q$. Allora, ponendo $a_0 = r$,

$$n = (a'_k b^k + \ldots + a'_2 b^2 + a'_1 b + a'_0)b + a_0 = a'_k b^{k+1} + \ldots + a'_2 b^3 + a'_1 b^2 + a'_0 b + a_0,$$

che è una rappresentazione b-adica di n.

Proviamo ora l'unicità. Supponiamo di avere due rappresentazioni b-adiche di $n \geq b$,

$$a_k b^k + \ldots + a_2 b^2 + a_1 b + a_0 = n = a'_k b^k + \ldots + a'_2 b^2 + a'_1 b + a'_0.$$

Siccome $n \geq b$ si ha $k \geq 1$ (il caso $n < b$ è banale). Allora, poiché $0 \leq a_0 \leq b-1$ e $n = (a_k b^{k-1} + \ldots + a_2 b + a_1)b + a_0$, si ha che $q = a_k b^{k-1} + \ldots + a_2 b + a_1$ e a_0 sono, rispettivamente il quoziente ed il resto della divisione di n per b. La stessa cosa vale per la seconda rappresentazione. Per l'unicità di quoziente e resto si ha dunque $a_0 = a'_0$ e

$$a_k b^{k-1} + \ldots + a_2 b + a_1 = a'_k b^{k-1} + \ldots + a'_2 b + a'_1.$$

Per ipotesi induttiva si conclude che $a_i = a'_i$ per ogni $i = 0, 1, 2, \ldots, k$. ∎

La dimostrazione del Teorema 3.2.1 suggerisce anche un metodo per calcolare le cifre di una rappresentazione b-adica, che lasciamo a chi legge di rendere esplicito (si comincia dividendo n per b, $n = qb + r$, e si prende $a_0 = r$, dopo di che ...).

Esercizio. Scrivere il numero 2007, rispettivamente, in base 2, 3, 6 e 7.

Soluzione. Vediamo la scrittura del numero (decimale) $n = 2007$ in base 7. Si divide il numero per 7, ottenendo $n = 286 \cdot 7 + 5$; quindi, **5** è la prima cifra (a destra) della rappresentazione in base 7. Si procede dividendo il quoziente ottenuto di sopra: $286 = 40 \cdot 7 + 6$ (la seconda cifra è quindi **6**. Si procede dividendo l'ultimo quoziente: $40 = 5 \cdot 7 + 5$, che fornisce la terza cifra (da destra), **5**, ed anche la quarta, che è ancora **5**. In conclusione la scrittura di $n = 2007$ in base 7 è **5565**. L'eventuale verifica della correttezza si esegue sviluppando in base 7:

$$5 \cdot 7^3 + 5 \cdot 7^2 + 6 \cdot 7 + 5 = 5 \cdot 343 + 5 \cdot 49 + 6 \cdot 7 + 5 = 1715 + 245 + 42 = 2007.$$

Procedendo in modo simile, si trova che la scrittura di 2007 in base 2 è 11111010111; quella in base 3 è 2202100, e quella in base 6 è 13143.

3.3 Divisibilità e numeri primi.

divisori e multipli

La definizione di divisibilità per numeri interi è precisa.

Dati due numeri interi $a, b \in \mathbb{Z}$, si dice che a **divide** b (e si scrive $a|b$) se esiste un $c \in \mathbb{Z}$ tale che $ac = b$. Si dice allora che a è un *divisore* di b, o, viceversa, che b è un *multiplo* di a.

Chiaramente, se $b \in Z$, dalla definizione discende che $1, -1, b$ e $-b$ sono divisori di b. Un divisore a di b si dice *proprio* se a è diverso da $1, -1, b, -b$.

M.C.D.

Veniamo subito alla definizione esatta di Massimo Comun Divisore. Siano $a, b \in Z$. Si chiama **massimo comun divisore** (MCD) di a, b ogni numero intero d che soddisfa alle seguenti condizioni

- $d|a$ e $d|b$;
- per ogni $x \in \mathbb{Z}$, se $x|a$ e $x|b$ allora $x|d$.

esistenza del M.C.D

Teorema 3.3.1. *Siano $a, b \in \mathbb{Z}$ due numeri interi. Allora*

(1) esiste un MCD d di a, b ;

(2) esistono $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$;

(3) se d_1 è un altro MCD di a, b , allora $d_1 = d$ oppure $d_1 = -d$.

Dimostrazione. Se $a = b = 0$ si osserva che il loro MCD è 0 e che le proprietà (1), (2) e (3) sussistono. Quindi supponiamo che a e b non siano entrambi nulli; in tal caso si ha $a^2 + b^2 > 0$ e dunque l'insieme di numeri naturali

$$S = \{\ s|\ s \in \mathbb{N} \text{ e } 0 \neq s = ax + by \text{ con } x, y \in \mathbb{Z}\ \}$$

non è vuoto e quindi, per il buon ordinamento di $\mathbb{N}$, ammette un minimo.
Sia $d = \min(S)$. Proviamo che d è un MCD di a, b. Poichè $d \in S$, esistono $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$. Mostriamo ora che $d|a$. Dividendo a per d, troviamo interi $q, r \in \mathbb{Z}$ tali che

$$a = qd + r \quad \text{e} \quad 0 \leq r < d$$

(dato che $d > 0$). Allora

$$r = a - dq = a - (\alpha a + \beta b)q = a(1 - \alpha q) + b(-\beta q)$$

se fosse $r > 0$, allora $r \in S$ e quindi $r \geq d = \min(S)$ contraddicendo la condizione sul resto $r < d$. Quindi deve essere $r = 0$, cioè $a = qd$ che significa $d|a$.
Allo stesso modo si prova che $d|b$.

Sia ora $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$; allora $c|\alpha a$ e $c|\beta b$, e quindi $c|\alpha a + \beta b = d$.
Dunque abbiamo provato che d è un MCD di a, b ; osserviamo che, poichè $d = \alpha a + \beta b$ anche il punto (2) è dimostrato.

Per dimostrare il punto (3), supponiamo che d_1 sia un altro MCD di a, b. Allora, in particolare, $d|d_1$ e $d_1|d$; cioè esistono $x, y \in \mathbb{Z}$ tali che $d = xd_1$ e $d_1 = yd$. Da ciò segue

$$d = xd_1 = x(yd) = (xy)d$$

e, poichè $d \neq 0$, questo implica $xy = 1$, e siccome $x, y \in \mathbb{Z}$, deve essere $x = y = 1$ oppure $x = y = -1$ che dà $d_1 = d$ oppure $d_1 = -d$. ∎

Dunque, dati due interi a, b non entrambi nulli, esiste un MCD d di a, b con $d \geq 1$; tale MCD lo denotiamo con (a, b). Come mostra la dimostrazione del Teorema, esso è, di fatto, il più piccolo numero positivo che si può scrivere nelle forma del punto (2) dell'enunciato.Ad esempio, poiché

$$6 \cdot 27 + (-15) \cdot 31 = 1$$

si ha che $(26, 31) = 1$.
Due interi a, b non entrambi nulli si dicono **coprimi** se $(a, b) = 1$. *numeri coprimi*
Dal Teorema precedente e dalla sua dimostrazione, si ricava il seguente importante

Criterio. *Due interi a, b non entrambi nulli sono coprimi se e solo se esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$.*

Un concetto di fondamentale importanza nella storia e nella pratica della matematica è quello di numero primo. Un numero intero p si dice **primo** se *numeri primi*

- $p \neq 0, 1, -1$;
- per ogni $a \in \mathbb{Z}$ se a divide p allora $a \in \{1, -1, p, -p\}$.

Nota. Quindi, un intero è un primo se è diverso da $0, 1, -1$, e non ha divisori propri. In particolare, si osservi che, per definizione, 1 **non** è un numero primo.

Il Lemma seguente descrive un'importante proprietà dei numeri primi.

Lemma 3.3.2. *Siano $a, b, p \in \mathbb{Z}$ con p primo:*

$$\textit{se} \quad p|ab \quad \textit{allora} \quad p|a \quad \textit{o} \quad p|b \ .$$

Dimostrazione. Supponiamo che $p|ab$. Se $p|a$ siamo a posto; assumiamo quindi anche che p non divida a. Allora $(a, p) = 1$, quindi esistono $x, y \in \mathbb{Z}$ tali che $xa + yp = 1$, da cui si ottiene

$$b = 1 \cdot b = xab + ypb \ ;$$

poichè $p|ab$, da ciò segue che p divide b. ∎

Nota. Procedendo per induzione su n si prova facilmente che se $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e p è un primo tale che $p|a_1 \cdot a_2 \cdots a_n$, allora $p|a_i$ per almeno un $i = 1, 2, \ldots, n$.

Dimostriamo ora il cosiddetto Teorema fondamentale dell'Aritmetica

Teorema fondam. aritmetica

Teorema 3.3.3. *Sia $z \in \mathbb{Z}$ un intero diverso da $0, 1, -1$. Allora esistono numeri primi $p_1, p_2, \ldots, p_n$ tali che*

$$z = p_1 \cdot p_2 \cdot p_3 \cdots p_n.$$

Inoltre tale fattorizzazione è unica a meno del segno dei numeri primi e del loro ordine nel prodotto.

Dimostrazione. (esistenza) Supponiamo prima $z > 0$ (quindi $z \geq 2$) e applichiamo il principio di induzione nella seconda forma.
Se $z = 2$ allora la cosa è banale. Supponiamo ora che $z \geq 3$ e che, per ipotesi induttiva, una fattorizzazione in prodotto di primi esista per ogni $2 \leq k \leq z - 1$.
Se z è primo, allora è gia fattorizzato (con un solo fattore). Supponiamo quindi che z non sia primo. Allora z ha almeno un divisore proprio k ; quindi $z = kb$ con $2 \leq k, b \leq z - 1$. Ma, per ipotesi induttiva, k e b sono un prodotto di numeri primi, e quindi anche z è tale. Assumiamo ora $z < 0$; allora $-z > 0$ e quindi, per quanto appena visto, $-z = p_1 \cdot p_2 \cdots p_n$, con $p_1, p_2, \ldots, p_n$ numeri primi; quindi $z = (-p_1) \cdot p_2 \cdot p_3 \cdots p_n$. La prova di esistenza è completata.

(unicità) Supponiamo che $p_1, p_2, \ldots, p_n$ e $q_1, q_2, \ldots, q_s$ siano primi tali che

$$p_1 \cdot p_2 \cdots p_n = z = q_1 \cdot q_2 \cdots q_s \ .$$

Allora $p_1|z = q_1 \cdot q_2 \cdots q_s$, quindi per l'osservazione che segue il Lemma precedente, p_1 divide almeno uno dei q_i. A meno di riordinare $q_1, q_2, \ldots, q_s$ possiamo supporre che $p_1|q_1$, ma allora, essendo primi, $p_1 = q_1$ oppure $p_1 = -q_1$.
Dividendo ora z per p_1 si ottiene dunque

$$p_2 \cdot p_3 \cdots p_n = \frac{z}{p_1} = \pm q_2 \cdot q_3 \cdots q_s \ .$$

Procedendo in questo modo alla fine si ricava $n = s$, ed anche l'unicità dei primi nelle due fattorizzazioni, a meno dell'ordine e dei segni. ∎

Esercizio. Sia $p \in \mathbb{Z}$, $p \neq 0, 1, -1$. Supponiamo che per ogni $a, b \in \mathbb{Z}$ sia verificata

$$p|ab \quad \Rightarrow \quad p|a \ \ o \ \ p|b.$$

Si provi che p è un numero primo.

Soluzione. $p \neq 0, 1, -1$ per ipotesi. Sia bZ un divisore di p; allora esiste $c \in \mathbb{Z}$ tale che $p = cb$. Ora, da ciò segue in particolare che $p|cb$; quindi, per ipotesi, $p|b$ oppure $p|c$. Se

$p|b$ si ha $b = \pm p$; mentre da $p|c$ segue $b = \pm 1$. Dunque, in ogni caso $b \in \{1, -1, p, -p\}$ e pertanto p è un primo.

Teorema di Euclide

Una delle applicazioni più famose del teorema di fattorizzazione in primi è la dimostrazione dell'esistenza di infiniti numeri primi; un risultato dovuto a Euclide (sostanzialmente con la stessa dimostrazione) e che ammette diverse altre dimostrazioni (anche molto diverse).

Teorema di Euclide. *Esistono infiniti numeri primi positivi.*

Dimostrazione. Supponiamo per assurdo che l'insieme dei numeri primi positivi sia finito, e siano allora $p_1, p_2, \ldots, p_t$ tutti i numeri primi positivi distinti. Consideriamo il numero intero

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_t + 1 \ .$$

Allora $N \geq 2$ e c'è un fattore primo q di N. Essendo primo, q deve essere uno dei p_i; ma allora $q|p_1 \cdot p_2 \cdots p_t$ e quindi q divide $N - p_1 \cdot p_2 \cdots p_t = 1$, assurdo. ∎

m.c.m.

Minimo Comune Multiplo. Siano $a, b \in Z$. Si chiama **minimo comune multiplo** (m.c.m.) di a, b ogni numero intero m che soddisfa alle seguenti condizioni

- $a|m$ e $b|m$;
- per ogni $x \in \mathbb{Z}$, se $a|x$ e $b|x$ allora $m|x$.

Lasciamo per esercizio la dimostrazione dell'analogo del Teorema 3.3.1, ovvero che ogni coppia di interi entrambi non nulli a e b esiste un m.c.m.; anzi, più precisamente ce ne sono due, uno l'opposto dell'altro; quello positivo si denota con m.c.m.(a, b), o a volte, anche con $[a, b]$.

Avendo a disposizione la fattorizzazione in potenze di numeri primi dei due interi (non nulli) a e b, è facile determinare il loro MCD ed il loro m.c.m.
Siano a e c numeri interi non nulli, che per semplicità supponiamo entrambi positivi, e siano

$$a = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} \quad \text{e} \quad c = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$$

le loro fattorizzati mediante potenze di numeri primi distinti $p_1, p_2, \ldots, p_k$, e dove abbiamo eventualmente aggiunto potenze di esponente zero per quei primi che sono divisori di uno solo dei due numeri. Supponiamo che c divida a; allora esiste un intero $r = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ tale che $a = cr$ quindi

$$a = p_1^{s_1 + r_1} p_2^{s_2 + r_2} \ldots p_k^{s_k + r_k}$$

da cui segue in particolare $r_i \leq n_i$ per ogni $i = 1, 2 \ldots, k$.

Siano ora a, b interi (positivi) non entrambi nulli. Se uno dei due è zero, allora il secondo è un MCD di a e b. Supponiamo quindi che siano entrambi non nulli e fattorizziamoli come potenze di primi:

$$a = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} \qquad b = p_1^{m_1} p_2^{m_2} \ \ldots p_k^{m_k}$$

con il solito accorgimento sugli esponenti. Consideriamo ora l'elemento

$$d = p_1^{\min\{n_1,m_1\}} p_2^{\min\{n_2,m_2\}} \ \dots \ p_k^{\min\{n_k,m_k\}} \ ;$$

chiaramente d divide sia a che b e, dalla osservazione fatta sopra, segue facilmente che d è un MCD di a e b.
Se invece prendiamo

$$m = p_1^{\max\{n_1,m_1\}} p_2^{\max\{n_2,m_2\}} \ \dots \ p_k^{\max\{n_k,m_k\}},$$

allora $m = \text{m.c.m}(a, b)$.

3.4 L' Algoritmo di Euclide.

Algoritmo di Euclide

L'algoritmo di Euclide (che, come suggerisce il nome, è uno degli algoritmi più antichi) è un metodo meccanico per determinare il MCD di due numeri interi (ma si applica anche in altri contesti - come ad esempio quello dei polinomi). Cominciamo con un esercizio.

Esercizio. Siano a, b numeri interi non nulli, e sia r il resto della divisione di a per b. Si provi che $(a, b) = (b, r)$.

Soluzione. r è il resto della divisone di a per b; quindi $0 \leq r \leq |b|$ ed esiste un quoziente $q \in \mathbb{Z}$ tale che $a = qb+r$. Sia $d = (a, b)$. Allora d divide a e b, e quindi d divide $a = qb = r$; pertanto d è un divisore comune di b ed r. Viceversa; se c è un divisore comune di b ed r, allora c divide $qb - r = a$, e quindi c è un divisore comune di a e b e pertanto $c|d$. Da ciò segue che $d = (b, r)$.

Veniamo all'algoritmo vero e proprio. Siano a, b numeri interi non nulli, che possiamo supporre positivi (infatti, per come è definito, è chiaro che $(a, b) = (|a|, |b|)$.
Poniamo $a_1 = a$ e $a_2 = b$. Iniziamo con dividere a_1 per a_2:

$$a_1 = q_1 a_2 + a_3 \quad \text{con} \quad 0 \leq a_3 < |a_2|$$

quindi si divide a_2 per a_3, ottendo un resto a_4 con $0 \leq a_4 < a_3$. Si prosegue con tale catena di divisioni; ovvero arrivati ad a_i si definisce a_{i+1} come il resto della

divisione di a_{i-1} per a_i:

$$\begin{aligned}
&a_1 = q_1 a_2 + a_3\\
&a_2 = q_2 a_3 + a_4\\
&a_3 = q_3 a_4 + a_5\\
&\ldots\ldots\\
&\ldots\ldots\\
&a_{i-1} = q_{i-1} a_i + a_{i+1}\\
&\ldots\ldots
\end{aligned}$$

in questo modo si ottiene una sequenza di resti

$$|a_2| > a_3 > a_4 > \ldots > a_{i-1} > a_i > \ldots > a_n = 0$$

Poichè tali resti sono numeri interi, tale sequenza arriva a zero dopo un numero finito di passi (che abbiamo indicato con n). Sia quindi a_{n-1} l'ultimo resto non nullo. Utilizzando l'esercizio precedente si provi che $a_{n-1} = (a_1, a_2) = (a, b)$.

Esempio. Calcolare il MCD di 6468 e 2275. Si ha

$$\begin{aligned}
&6468 = 2 \cdot 2275 + 1918\\
&2275 = 1 \cdot 1918 + 357\\
&1918 = 5 \cdot 357 + 133\\
&357 = 2 \cdot 133 + 91\\
&133 = 1 \cdot 91 + 4291 = 2 \cdot 42 + 7\\
&42 = 6 \cdot 7 + 0
\end{aligned}$$

quindi $(6468, 2275) = 7$.

Osserviamo come l'algoritmo di Euclide, dati due interi positivi a e b, oltre a fornire il loro MCD $d = (a, b)$, consente di trovare coefficienti interi α e β tali che $d = a\alpha + b\beta$. Vediamo come, mediante l'esempio di sopra. Quindi $a = 6468$, $b = 2275$, e $d = 7$. Riutilizzando all'indietro le uguaglianze determinate dalle divisioni successive si ha

$$\begin{aligned}
7 &= 91 + (-2)42 = 91 + (-2)(133 - 91) = 3 \cdot 91 + (-2)133 =\\
&= 3(357 - 2 \cdot 133) + (-2)133 = 3 \cdot 357 + (-8)133 =\\
&= 3 \cdot 357 + (-8)(1918 - 5 \cdot 357) = (-8)1918 + 43 \cdot 357 =\\
&= (-8)1918 + 43(2275 - 1918) = 43 \cdot 2275 + (-51)1918 =\\
&= 43 \cdot 2275 + (-51)(6468 - 2 \cdot 2275) = (-51)6468 + 145 \cdot 2275.
\end{aligned}$$

3.5 Esercizi.

Esercizio 3.1. Applicando il principio di induzione si dimostrino le seguenti affermazioni.

- Per ogni $n \geq 1$: $1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2$.
- Per ogni $n \geq 1$: $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.
- Per ogni $n \geq 1$: $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots n \cdot n! = (n+1)! - 1$.

Esercizio 3.2. Si determinino tre numeri razionali a, b, c tali che, per ogni $n \geq 1$ si abbia

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = an^3 + bn^2 + cn.$$

Esercizio 3.3. Sia $a \in \mathbb{R}, a > 0$; si dimostri che, per ogni numero intero $n \geq 2$ si ha

$$(1+a)^n > 1 + na.$$

Esercizio 3.4. Si scrivano le rappresentazioni in base 2, 3, 7, 11 del numero 2002 (si faccia attenzione che per la base 11 c'è bisogno di un simbolo per le cifre in più, che rappresenti il numero 10).

Esercizio 3.5. Il numero 2002 è detto "palindromo" perché la sua rappresentazione decimale è palindroma, ovvero è uguale se letta in entrambi i versi. Naturalmente la palindromia non è una proprietà intrinseca di un numero ma dipende dal numero e dalla base per la rappresentazione. Si determinino tutte le basi $2 \leq b \leq 10$ tale che la rappresentazione b-adica del numero 1785 è palindroma.

Esercizio 3.6. Si provi che per ogni intero $n \geq 3$ esiste una base $b < n$ tale che la rappresentazione b-adica di n è palindroma. Si provi che non esiste alcuna base b tale che la rappresentazione b-adica del numero 39 è composta da almeno tre cifre ed è palindroma.

Esercizio 3.7. Trovare due numeri interi a e b tali che $19a + 21b = 1$.

Esercizio 3.8. Calcolare il MCD di 4415 e 1554.

Esercizio 3.9. Siano a, b, c numeri interi non nulli. Si dimostri che $(a, (b, c)) = ((a, b), c)$.

Esercizio 3.10. Siano a, b, c numeri interi non nulli. Si dimostri che se a divide bc allora $a/(a, b)$ divide c.

Esercizio 3.11. Siano a, b numeri interi positivi non nulli. Si provi che

$$[a, b] = \frac{ab}{(a, b)}.$$

Capitolo 4

Cardinalità degli insiemi

Il concetto di biezione (corrispondenza biunivoca) consente di formulare una teoria rigorosa intorno alla "quantità" di elementi di un insieme. Mediante tale teoria, il "numero", inteso come misuratore di quantità, è esteso a comprendere quantità infinite, consentendone inoltre il confronto.
In questo approccio non si dice "che cosa" sia il "numero di elementi" (eventualmente infinito) di un insieme, ma si specifica *quando* due insiemi hanno lo stesso numero di elementi: ed è quando è possibile stabilire una biezione tra i due insiemi. Ciò, in fondo, è quello che si fa normalmente mentre si apprende a contare: ad esempio, un insieme è riconosciuto come formato da *cinque* elementi se è in corrispondenza biunivoca con l'insieme delle dita di una mano (o con qualunque altro insieme che sappiamo già contenere cinque elementi).
Già Galileo aveva osservato che, poiché ad ogni numero naturale si può associare (mediante la moltiplicazione per 2) in modo univoco un numero pari, si deve concludere che i numeri pari "sono tanti" quanti i numeri naturali, pur costituendone un sottoinsieme proprio. Galileo icomprese che quest'ultima apparente antinomia era in realtà una caratteristica degli insiemi infiniti, ma non sviluppò oltre le sue intuizioni. I tempi non erano ancora maturi per una teoria matematica dell"infinito, che fu sviluppata da G. Cantor[1] nella seconda metà del diciannovesimo secolo,

4.1 Teoria di Cantor.

Si dice che due insiemi A e B hanno la stessa **cardinalità** (oppure che sono *equipotenza*

[1] Georg Cantor, 1845–1918.

equipotenti) se esiste una applicazione *biettiva*

$$f : A \longrightarrow B.$$

In tal caso si scrive $|A| = |B|$.

Dalle proprietà delle applicazioni biettive segue che la relazione di equipotenza gode delle proprietà seguenti.

- Ogni insieme A è equipotente a se stesso (tramite l'applicazione identica ι_A).
- Se A è equipotente a B, allora B è equipotente ad A (tramite l'applicazione inversa).
- Se A è equipotente a B, e B è equipotente a C, allora A è equipotente a C (tramite l'applicazione composta).

insiemi finiti

Un insieme A si dice **finito** se esiste $n \in \mathbb{N}$, ed una biezione tra A e l'insieme $\{1, 2, \ldots, n\}$; in questo caso si dice che A ha **ordine** (o **cardinalità**) n, e scrive $|A| = n$. Un insieme che non è finito si dice infinito.

Esempio (G. Galilei). Sia $P = 2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$ l'insieme dei numeri naturali pari. L'applicazione $f : \mathbb{N} \longrightarrow P$ definita da $f(n) = 2n$ è biettiva. Quindi l'insieme dei numeri naturali $\mathbb{N}$ è equipotente ad un suo sottoinsieme proprio (in questo caso P, ma si possono fare esempi del genere con qualsiasi sottoinsieme infinito di $\mathbb{N}$). Questa eventualità non si può verificare negli insiemi finiti; si può facilmente provare che un insieme è infinito se e solo se è equipotente ad un suo sottoinsieme proprio (anzi, questa proprietà può essere assunta come definizione di un insieme infinito).

numerabilità

Un insieme A si dice **numerabile** se esiste una biezione tra A e l'insieme $\mathbb{N}$ dei numeri naturali.

Proposizione 4.1.1. *L'insieme $\mathbb{Z}$ dei numeri interi è numerabile.*

Dimostrazione. L'applicazione definita nell'esercizio 2.3 è una biezione da $\mathbb{N}$ in $\mathbb{Z}$, quindi l'insieme $\mathbb{Z}$ dei numeri interi è numerabile. ∎

Molto meno intuitivo è il fatto che l'insieme dei numeri razionali $\mathbb{Q}$ è numerabile. Per dimostrarlo, cominciamo osservando che ogni numero razionale risulta da una coppia ordinata (numeratore e denominatore) di numeri interi. Cominciamo quindi con l'esaminare il caso del prodotto diretto $\mathbb{Z} \times \mathbb{Z}$.

Proposizione 4.1.2. *Sia A un insieme numerabile. Allora anche il prodotto diretto $A \times A$ è numerabile.*

Dimostrazione. Sia A un insieme numerabile, e sia $f : \mathbb{N} \to A$ una biezione. Allora, si verifica facilmente che l'applicazione

$$\begin{array}{rcl} \mathbb{N} \times \mathbb{N} & \to & A \times A \\ (a, b) & \mapsto & (f(a), f(b)) \end{array}$$

è una biezione. Quindi $|A \times A| = |\mathbb{N} \times \mathbb{N}|$. Pertanto è sufficiente provare che $\mathbb{N} \times \mathbb{N}$ è numerabile.
Ora, ogni numero naturale $n \geq 1$ può essere scritto in uno ed un sol modo nella forma $n = 2^a m$ con m dispari. Da ciò segue che l'applicazione

$$\begin{array}{rcl} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \setminus \{0\} \\ (a, b) & \mapsto & 2^a(2b + 1) \end{array}$$

è una biezione. Poiché $\mathbb{N} \setminus \{0\}$ è numerabile, si conclude che $\mathbb{N} \times \mathbb{N}$ è numerabile. ∎

La proprietà seguente non è difficile da provare (ma ne omettiamo la dimostrazione).

Proposizione 4.1.3. *(1) Ogni sottoinsieme di un insieme numerabile è finito o numerabile.*

(2) Siano A, B insiemi e $f : A \longrightarrow B$ una applicazione suriettiva. Se A è numerabile allora B è finito o numerabile.

Possiamo ora cosa passare al caso specifico dei numeri razionali.

Proposizione 4.1.4. *L'insieme $\mathbb{Q}$ dei numeri razionali è numerabile.*

$\mathbb{Q}$ *è numerabile*

Dimostrazione. Osserviamo che ogni numero razionale $a \neq 0$ si scrive in modo unico nella forma $a = \frac{m(a)}{n(a)}$ con $m(a) \in \mathbb{Z}$, $n(a) \in \mathbb{N}$ e $MCD(m(a), n(a)) = 1$. Quindi la applicazione

$$f : \mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{Z}$$

definita da

$$f(0) = (0, 0) \text{ e, per ogni } 0 \neq a \in \mathbb{Q},\ f(a) = (m(a), n(a))$$

è iniettiva; dunque, posto $Y = f(\mathbb{Q})$, abbiamo $|Y| = |\mathbb{Q}|$. Ora $Y \subseteq \mathbb{Z} \times \mathbb{Z}$. Ma $\mathbb{Z}$ è numerabile per l'esempio (2), quindi $\mathbb{Z} \times \mathbb{Z}$ è numerabile per la Proposizione 4.1.2, e dunque Y è numerabile per la Proposizione 4.1.3. ∎

Diverso il caso dei numeri reali; l'insieme $\mathbb{R}$, infatti, non può essere enumerato.

Proposizione 4.1.5. *L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.*

$\mathbb{R}$ *non è numerabile*

Dimostrazione. Per la proposizione 4.1.3, è sufficiente dimostrare che un sottoinsieme di $\mathbb{R}$ non è numerabile. Vediamo che non è numerabile l'intervallo

$$A = [0,1] = \{\ x \mid x \in \mathbb{R}\ , 0 \leq x \leq 1\ \}\ .$$

Osserviamo che ogni $x \in A$ ha una rappresentazione decimale del tipo $0, x_0x_1x_2\ldots$, con $x_i \in \{0,1,2,\ldots,9\}$ (si tenga presente che $1 = 0,999999\ldots$). Tale rappresentazione è unica se si conviene che non debba avere un numero finito di cifre diverse da zero (cioè conveniamo, ad esempio, di scrivere $0,24457 = 0,244569999\ldots$) Supponiamo per assurdo che esita una applicazione biettiva $f : \mathbb{N} \longrightarrow A$, allora per ogni $n \in \mathbb{N}$ si può scrivere

$$f(n) = 0, x_{n,0}x_{n,1}x_{n,2}\ldots$$

con $x_{n,i} \in \{0,1,2,\ldots,9\}$.
Ora, per ogni $i \in \mathbb{N}$ si scelga un numero naturale

$$a_i \in \{0,1,2,\ldots,9\} \ \text{ con } \ a_i \neq 0, x_{i,i}$$

e si consideri il numero reale, appartenente ad A :

$$y = 0, a_0a_1a_2a_3\ldots$$

Poichè f è una biezione, esiste $k \in \mathbb{N}$ tale che $y = f(k) = 0, x_{k,0}x_{k,1}x_{k,2}\ldots$; ma allora $x_{k,k} = a_k$ che è una contraddizione.
Quindi una tale f non esiste e dunque $A = [0,1]$ non è numerabile. ∎

Quest'ultima tecnica dimostrativa è chiamata a volte "procedimento diagonale", ed è, nella sostanza, ciò che si utilizza per provare il famoso Teorema di Cantor.

Teorema di Cantor

Teorema (di Cantor). *Sia A un insieme e sia $\mathcal{P}(A)$ l'insieme delle parti di A. Allora $|\mathcal{P}(A)| \neq |A|$.*

Dimostrazione. Sia A un insieme e supponiamo, per assurdo, che esista una biezione

$$f : A \longrightarrow \mathcal{P}(\mathcal{A}).$$

Sia allora $U = \{a \in A \mid a \notin f(a)\}$. U è un sottoinsieme di A, quindi, poiché f è suriettiva, esiste $x \in A$ tale che $U = f(x)$. Ora, deve verificarsi una delle seguenti possibilità: $x \in U$, oppure $x \notin U$. Supponiamo che $x \in U$, in tal caso, per definizione di U, $x \notin f(x) = U$, il che è assurdo. Sia quindi $x \notin U = f(x)$, allora, ancora per la definizione di U si ha l'assurdo $x \in U$. Queste contraddizioni provano che una tale f non esiste, e dunque che $|\mathcal{P}(A)| \neq |A|$. ∎

In particolare quindi, $\mathcal{P}(\mathbb{N})$ non è numerabile. Si dice che un insieme X ha la **cardinalità del continuo** se $|X| = |\mathcal{P}(\mathbb{N})|$. Non sarebbe difficile dimostrare che $\mathbb{R}$ ha la cardinalità del continuo.

continuo

4.2 Insiemi finiti

Per questa sezione fissiamo due insiemi finiti A e B, con $|A| = n$ e $|B| = m$.

Con queste notazioni, le seguenti affermazioni sono facilmente verificabili:

(1) $|A \times B| = |A||B| = mn$;

(2) se A e B sono disgiunti : $|A \cup B| = |A| + |B| = m + n$; in generale

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

---

card. di un prodotto

La prima delle due uguaglianze si può facilmente generalizzare ad un prodotto di un numero k di insiemi finiti: se $A_1, \ldots, A_k$ sono insiemi finiti, allora

$$|A_1 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k|;$$

in particolare, se $|A| = n$, allora $|A^k| = n^k$.

Anche la uguaglianza (2) si generalizza; la prima parte in modo ovvio:

- se $A_1, \ldots, A_k$ sono insiemi finiti *a due a due disgiunti*, allora

$$|A_1 \cup \ A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \ldots + |A_k| \ ;$$

card. di una unione

il caso generale non è altrettanto banale; posto $X = \{1, 2, \ldots, k\}$, si ha

$$|A_1 \cup \ A_2 \cup \cdots \cup A_k| = \sum_{\emptyset \neq I \subseteq X} (-1)^{|I|+1} |\bigcap_{i \in I} A_i| \ .$$

ad esempio, nel caso di tre insiemi:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

---

numero di applicazioni

Vogliamo ora determinare il numero di applicazioni da A in B; sia quindi

$$B^A = \{ \ f \mid f : A \longrightarrow B \ \text{ applicazione } \}.$$

Osserviamo che, se $A = \{a_1, a_2, \ldots, a_n\}$, allora una applicazione $f : A \longrightarrow B$ è univocamente individuata dalla n-upla delle immagini $(f(a_1), f(a_2), \ldots, f(a_n)) \in B^n$; detto in modo più preciso, l'applicazione $\Gamma : B^A \longrightarrow B^n$ definita da, per ogni $f \in B^A$,

$$\Gamma(f) = (f(a_1), f(a_2), \ldots, f(a_n))$$

è una biezione. Quindi $|B^A| = |B^n| = m^n$. Abbiamo quindi dimostrato

Proposizione 4.2.1. *Se A e B sono insiemi finiti, allora il numero di applicazioni da A in B è uguale a $|B|^{|A|}$.*

Sia $n \in \mathbb{N}$; ricordo che si definisce $n!$ (n **fattoriale**) nel modo seguente: *fattoriale*

$$0! = 1 \text{ e, se } n \geq 1,\ n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n \ .$$

Ora, ci chiediamo quale sia il numero di applicazioni *iniettive* da A in B. Riferendoci all'applicazione $\Gamma : B^A \longrightarrow B^n$ utilizzata in precedenza, vediamo che le applicazioni iniettive corrispondono alle n-uple di elementi *distinti* di B. *applicazioni iniettive*
Ora per costruire tutte le n-uple $(b_1, b_2, \ldots, b_n) \in B^n$ ad elementi distinti, possiamo pensare di poter scegliere

- b_1 in m modi possibili (ogni elemento di B);
- b_2 in $m-1$ modi possibili (ogni elemento di B con l'esclusione di b_1);
- b_3 in $m-2$ modi possibili (ogni elemento di B con l'esclusione di b_1, b_2);

e così via. Questo processo finisce con b_n per cui abbiamo $m-n$ scelte fra gli elementi di B. In totale le n-uple ad elementi distinti sono quindi : $m(m-1)(m-2)\cdots(m-n)$.

Abbiamo quindi dimostrato

Proposizione 4.2.2. *Se A e B sono insiemi finiti con $|A| = n \leq m = |B|$, allora il numero di applicazioni iniettive da A in B è uguale a*

$$m(m-1) \ \ldots \ (m-n+1) = \frac{m!}{(m-n)!} \ .$$

In particolare, ricordando che per un insieme finito A, un'applicazione $f : A \to A$ è biettiva se e solo se è iniettiva, si deduce

Proposizione 4.2.3. *Sia A un insieme finito con $|A| = n$, allora il numero di applicazioni biettive da A in se stesso è uguale a $n!$.*

Coefficienti binomiali. Sia A un insieme finito con n elementi e $k \in \mathbb{N}, k \leq n$. Ci proponiamo di calcolare il numero di sottoinsiemi di A che contengono esattamente k elementi. Tale numero, che non dipende da A ma solo da n e k si denota con *coeffic. binomiali*

$$\binom{n}{k}$$

e si chiama *coefficiente binomiale n su k*.

Chiaramente, $\binom{n}{0} = 1 = \binom{n}{n}$ (poiché A ha un solo sottoinsieme con 0 elementi che è l'insieme vuoto, ed un solo sottoinsieme con n elementi che è A stesso).
Per calcolare i coefficienti binomiali in generale,, fissiamo un insieme U con $|U| = k$, e consideriamo l'insieme Ω di tutte le applicazioni iniettive di di U in A. Osserviamo che se $f \in \Omega$ allora la sua immagine $f(U)$ è un sottoinsieme di ordine k di A; viceversa, se $X \subseteq A$ e $|X| = k$, allora esiste una biezione da U in X, e quindi una applicazione iniettiva $f : U \longrightarrow A$ tale che $f(U) = X$.
Su Ω definiamo ora una relazione $\sim$ ponendo, per ogni $f, g \in \Omega, f \sim g$ se $f(U) = g(U)$. Chiaramente, $\sim$ è una equivalenza. Se $f \sim g$ allora posto $X = f(U) = g(U)$, esiste una unica applicazione $\overline{g} : X \longrightarrow U$ tale che $g \circ \overline{g} = \iota_X$ e quindi $f \circ \overline{g}$ è una biezione di X; da ciò segue che ogni classe di equivalenza modulo $\sim$ contiene esattamente tante applicazioni quante sono le applicazioni biettive da X in X, numero che, per quanto visto, è uguale a $|X|! = k!$. Ora, il numero di classi di equivalenza è uguale al numero di sottoinsiemi di A con k elementi. Quindi:

$$\binom{n}{k} = |\Omega/\sim| = \frac{|\Omega|}{k!} = \frac{n!}{(n-k)!k!} \ .$$

in conclusione abbiamo

Teorema 4.2.4. *Sia A un insieme finito con $|A| = n$, e sia $k \in \mathbb{N}, k \leq n$; allora il numero di sottoinsiemi di A che contengono esattamente k elementi è :* *valore dei coeffic. binomiali*

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} \ .$$

Il nostro prossimo obiettivo è la dimostrazione della formula di Newton per il calcolo delle potenze di un binomio. Il primo passo consiste nel provare le seguenti utili proprietà dei coefficienti binomiali.

Lemma 4.2.5. *Siano $k, n \in \mathbb{N}$ con $k \leq n$. Allora* *proprietà dei coeffic. binomiali*

(1) $\binom{n}{k} = \binom{n}{n-k}$;

(2) $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$.

Dimostrazione. (1) Osservando che se A è un insieme con n elementi, la regola $X \longrightarrow A \setminus X$ definisce una biezione tra l'insieme dei sottoinsiemi di ordine k di A e l'insieme dei sottoinsiemi di ordine $n-k$; quindi il numero dei sottoinsiemi di ordine k coincide con quello dei sottoinsiemi di ordine $n-k$.
Oppure, calcolando direttamente:

$$\binom{n}{n-k} = \frac{n!}{(n-(n-k))!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

(2) Abbiamo

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

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

$$=\frac{(n-1)!(n-k+k)}{k!(n-k)!}=\frac{(n-1)!n}{k!(n-k)!}=\frac{n!}{k!(n-k)!}=\binom{n}{k}.$$

Ciò conclude la dimostrazione. ∎

Teorema 4.2.6. (del binomio di Newton). *Siano $a,b\in\mathbb{Z}$ numeri interi, e $0\neq n\in\mathbb{N}$. Allora* *formula di Newton*

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

Dimostrazione. Per induzione su n.
Se $n=1$ allora la formula è valida; infatti:

$$(a+b)^n=a+b=\binom{1}{0}a^1b^0+\binom{1}{1}a^0b^1\ .$$

Sia ora $n\geq 2$, e per ipotesi induttiva supponiamo:

$$(a+b)^{n-1}=\sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-1-k}\ .$$

Allora, utilizzando la formula (2) del Lemma precedente:

$$\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}\ =a^n+\sum_{k=1}^{n-1}\binom{n}{k}a^kb^{n-k}\ +b^n=$$

$$=a^n+\sum_{k=1}^{n-1}\binom{n-1}{k-1}a^kb^{n-k}\ +\sum_{k=1}^{n-1}\binom{n-1}{k}a^kb^{n-k}\ +b^n=$$

$$=a\cdot\Big(a^{n-1}+\sum_{j=0}^{n-2}\binom{n-1}{j}a^jb^{n-1-j}\Big)+\Big(\sum_{k=1}^{n-1}\binom{n-1}{k}a^kb^{n-1-k}\ +b^{n-1}\Big)\cdot b=$$

$$= a \cdot \sum_{j=0}^{n-1} \binom{n-1}{j} a^j b^{n-1-j} \; + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k} \; \cdot b =$$

$$= a(a+b)^{n-1} + (a+b)^{n-1} b = (a+b)(a+b)^{n-1} = (a+b)^n \; .$$

Per il principio di induzione, la formula è vera per ogni $n \geq 1$. ∎

Come applicazione, ridimostriamo una formula già vista.

Sia A insieme finito con $|A| = n$. Allora $|\mathcal{P}(A)| = 2^n$.

Infatti :

$$|\mathcal{P}(A)| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = (1+1)^n = 2^n \; .$$

4.3 Esercizi.

Esercizio 4.1. Siano A un insieme numerabile, e B un insieme finito (ma non vuoto) o numerabile. Si dimostri che $A \times B$ è numerabile. Si provi quindi che se $A_1, A_2, \ldots, A_n$ sono insiemi numerabili, allora $A_1 \times A_2 \times \cdots \times A_n$ è numerabile.

Esercizio 4.2. Si dimostri la Proposizione 6.2.

Esercizio 4.3. Sia n un intero positivo dispari, e sia $X = \{1, 2, 3, ..., n\}$. Quanti sono i sottoinsiemi di X di ordine maggiore o uguale a $n/2$?

Esercizio 4.4. Sia $X = \{1, 2, 3, 4, 5\}$.

(a) Quanti sono i sottoinsiemi di X che contengono 1 ?

(b) Quanti sono i sottoinsiemi A di X tali che $A \cap \{2, 3\} \neq \emptyset$ che contengono 1 ?

(c) Quante sono le applicazioni iniettive di X in $\{1, 2, 3\}$?

(d) Quante sono le applicazioni iniettive di $\{1, 2, 3\}$ in X ?

(e) Quante sono le applicazioni suriettive di X in $\{1, 2, 3\}$?

Esercizio 4.5. Calcolare il numero di applicazioni suriettive f dell'insieme $A = \{1, 2, 3, 4, 5, 6\}$ nell'insieme $B = \{1, 2, 3\}$ tali che per ogni $b \in B$ sia $|f^{-1}(b)| \leq 2$.

Capitolo 5

Relazioni

Un'applicazione dall'insieme A nell'insieme B è una corrispondenza che *ad ogni* elemento di A fa corrispondere *uno ed un solo* elemento di B. Si tratta di un concetto fondamentale e di grande importanza, che tuttavia non copre l'intero ambito che associamo (più o meno vagamente) all'idea di corrispondenza (o di relazione) tra oggetti di uno o diversi insiemi.

5.1 Generalità.

relazioni

Sia A un insieme, una **relazione** (binaria) su A è un sottoinsieme del prodotto $A \times A$.

Se $\rho \subseteq A \times A$ è una relazione su A, e la coppia ordinata (a, b) appartiene a ρ, si scrive $a\rho b$, invece di $(a, b) \in \rho$, e si legge 'a è in relazione con b'.

Ad esempio, dati due numeri interi a, b, si dice che a *divide* b se esiste un $c \in \mathbb{Z}$ tale che $ac = b$. La relazione di divisibilità nell'insieme dei numeri interi $\mathbb{Z}$ è quindi descritta dal seguente sottoinsieme di $\mathbb{Z} \times \mathbb{Z}$:

$$\{ (a, b) \mid a, b \in \mathbb{Z} \text{ ed esiste } c \in \mathbb{Z} \text{ tale che } ac = b \}$$

In pratica, però, solo raramente si definisce una relazione descrivendo per esteso il sottoinsieme del prodotto. La relazione di divisibilità si descrive più naturalmente nella maniera seguente:

è la relazione $|$ sull'insieme $\mathbb{Z}$, definita da, per ogni $a, b \in Z$, $a|b$ se a divide b.

Un'applicazione $f : A \to A$ è un tipo di relazione molto particolare; per ogni elemento $a \in A$ esiste *uno ed un unico* elemento $f(a) \in A$ tale che $(a, f(a))$ appartiene alla relazione.

Nota. Abbiamo dato la definizione di relazione su un insieme A, ma anche questo concetto si può generalizzare a due insiemi A e B, ed in tal caso prende il nome di *corrispondenza*: quindi, una corrispondenza dell'insieme A nell'insieme B è un sottoinsieme di $A \times B$ (e dunque una relazione su A non è altro che una corrispondenza da A in se stesso.

La definizione di relazione che abbiamo dato, che è quella che serve, è ovviamente molto ampia. Un insieme ammette moltissime relazioni (ad esempio, se A è finito di ordine n, il numero di relazioni su A coincide con la cardinalità di $\mathcal{P}(A \times A)$ che è 2^{n^2}), la maggior parte delle quali è - dal punto di vista della matematica - intrattabile o inutile. Relazioni che siano significative e interessanti si ottengono imponendo ulteriori condizioni. Oltre alle applicazioni (che abbiamo già trattato) i due tipi più importanti di relazione sono le *relazioni d'equivalenza* e le *relazioni d'ordine*, che descriveremo brevemente nel seguito.

5.2 Relazioni d'equivalenza.

Sia ρ una relazione sull'insieme A. *equivalenze*

1) ρ si dice **riflessiva** se, per ogni $a \in A$: $a\rho a$

2) ρ si dice **simmetrica** se, per ogni $a\ , b \in A$: da $a\rho b$ segue $b\rho a$

3) ρ si dice **transitiva** se, per ogni $a\ , b\ , c \in A$: da $a\rho b$ e $b\rho c$ segue $a\rho c$

Ad esempio, la relazione di divisibilità nei numeri interi è riflessiva e transitiva, ma non è simmetrica.

Una relazione si dice **relazione di equivalenza** se è *riflessiva, simmetrica e transitiva.*

Esempi. 1) La relazione ρ sull'insieme $\mathbb{R}$ dei numeri reali definita da, per ogni $x, y \in \mathbb{R}$: $x\rho y$ se $|x| = |y|$, è una relazione di equivalenza.

2) Sia Σ l'insieme di tutte le circonferenze del piano. La relazione

$$\{\ (C, C') \mid C, C' \in \Sigma\ ,\ C \text{ e } C' \text{ hanno lo stesso centro }\}$$

è una equivalenza su Σ.

3) Sia $A = \mathbb{N} \times \mathbb{N} \setminus \{0\}$ l'insieme delle coppie ordinate di numeri naturali la cui seconda componente è diversa da zero. La relazione ω su A definita da

$$\text{per ogni } (a, b)\ , (c, d) \in A\ :\ (a, b)\omega(c, d) \quad \text{se} \quad ad = bc$$

è una relazione di equivalenza. Infatti, riflessività e simmetria sono di immediata verifica; dimo-striamo la transitività. Siano $(a,b),(c,d),(r,s) \in A$ tali che : $(a,b)\omega(c,d)$ e $(c,d)\omega(r,s)$; allora, per definizione di ω : $ad = bc$ e $cs = dr$; quindi, se $c = 0$ allora $a = 0 = r$ e dunque $as = 0 = br$, se invece $c \neq 0$:

$$as(cd) = ad \cdot cs = bc \cdot dr = br(cd)$$

da cui segue, essendo $cd \neq 0$, $as = br$; dunque, in ogni caso $(a,b)\omega(r,s)$.
(Si dica se la relazione definita allo stesso modo sull'insieme $\mathbb{N} \times \mathbb{N}$ è ancora una equivalenza.)

Per relazioni che sono di equivalenza si utilizzano solitamente simboli che suggeriscono la simmetria della relazione stessa, come $\sim$, $\equiv$, ω , $\simeq$, etc.

Osservazione. Ogni insieme non vuoto A ammette sempre almeno due relazioni di equivalenza:

l'uguaglianza : $x \sim y$ se e solo se $x = y$, che corrisponde all'insieme
$\{\ (x,y) \mid x,y \in A,\ x = y\ \}$;

la relazione banale : $x \sim y$ per ogni $x,y \in A$, corrispondente all'intero prodotto $A \times A$.

Tali equivalenze sono distinte se e solo se $|A| \geq 2$. Osserviamo inoltre che la proprietà riflessiva per una relazione ρ sull'insieme A equivale alla condizione che, come sottoinsiemi di $A \times A$, $\{\ (x,x) \mid x \in A\ \} \subseteq \rho$. Quindi possiamo dire che l' uguaglianza e la relazione banale sono la minima e la massima tra le equivalenze di A.

classi di equivalenza

Sia $\sim$ una relazione di equivalenza sull'insieme A, e sia $a \in A$. L'insieme di tutti gli elementi di A che sono in relazione con a si chiama **classe di equivalenza di** a (modulo $\sim$) e si denota con $[a]_\sim$. Quindi:

$$[a]_\sim = \{\ b \mid b \in A\ , a \sim b\ \}.$$

La proprietà riflessiva dell'equivalenza assicura che, per ogni $a \in A : a \sim a$, quindi $a \in [a]_\sim$. In particolare $[a]_\sim \neq \emptyset$ per ogni $a \in A$, ed inoltre

$$\bigcup_{a \in A} [a]_\sim = A.$$

È importante sottolineare che $[a]_\sim$ è un sottoinsieme di A e che, anche se (come elementi) $a \neq b$, $[a]_\sim$ e $[b]_\sim$ possono avere elementi in comune (Proposizione

5.2.1); vedremo poi (Proposizione 5.2.2) che se $[a]_\sim$ e $[b]_\sim$ hanno elementi in comune, allora coincidono come sottoinsiemi di A.

Ad esempio, se ρ è l'equivalenza sull'insieme $\mathbb{R}$ dell'esempio 1), allora, per ogni $x \in \mathbb{R}$ la classe di equivalenza di x è $[x]_\rho = \{x, -x\}$.
Riferendosi all'esempio 2) di sopra, la classe di equivalenza di una circonferenza C è l'insieme di tutte le circonferenze concentriche a C.

uguaglianza tra classi

Vediamo subito il fondamentale criterio di uguaglianza tra classi di equivalenza

Proposizione 5.2.1. *Sia $\sim$ una relazione di equivalenza sull'insieme A, e siano $a, b \in A$. Allora*

$$[a]_\sim = [b]_\sim \quad \textit{se e solo se} \quad a \sim b.$$

Dimostrazione. Sia $[a]_\sim = [b]_\sim$. Allora, per la proprietà riflessiva, $b \in [b]_\sim = [a]_\sim$ e quindi, per definizione di $[a]_\sim$, $a \sim b$.
Viceversa, sia $a \sim b$. Allora anche $b \sim a$ per simmetria. Sia $x \in [a]_\sim$; allora $a \sim x$ e quindi, per transitività : $b \sim x$, cioè $x \in [b]_\sim$, provando che $[a]_\sim \subseteq [b]_\sim$. Allo stesso modo si dimostra l'inclusione inversa, e dunque l'uguaglianza $[a]_\sim = [b]_\sim$. ■

Quindi se $b \in [a]_\sim$ allora $[a]_\sim = [b]_\sim$. In tal caso a e b si dicono *rappresentanti* della stessa classe di equivalenza $[a]_\sim$.

Proposizione 5.2.2. *Sia $\sim$ una relazione di equivalenza sull'insieme A, e siano $a, b \in A$. Se $[a]_\sim \cap [b]_\sim \neq \emptyset$ allora $[a]_\sim = [b]_\sim$.*

Dimostrazione. Supponiamo che $[a]_\sim \cap [b]_\sim \neq \emptyset$, e sia $x \in [a]_\sim \cap [b]_\sim$. Per definizione di classi di equivalenza, si ha allora $a \sim x$ e $b \sim x$, da cui, per la proprietà simmetrica (che ci dà $x \sim b$) e la proprietà transitiva, si ottiene $a \sim b$. Ciò implica, per la Proposizione 5.2.1, $[a]_\sim = [b]_\sim$. ■

insieme quoziente

Sia $\sim$ una relazione di equivalenza sull'insieme A. L'insieme di tutte le classi di equivalenza di elementi di A si chiama **insieme quoziente** (di A modulo $\sim$) e si denota con $A/\sim$. Quindi

$$A/\sim = \{\ [a]_\sim \mid a \in A\ \}.$$

Data una equivalenza $\sim$ sull'insieme A, gli elementi dell'insieme quoziente $A/\sim$ sono quindi *sottoinsiemi* di A, **non vuoti, disgiunti** (per la Proposizione 5.2.2), e **la cui unione è l'intero** insieme A.

Una famiglia di sottoinsiemi di un dato insieme A che soddisfa alle tre proprietà enunciate in grassetto di sopra, si dice **partizione** di A. Precisamente :

Sia A un insieme non vuoto. Una famiglia $\mathcal{F}$ di sottoinsiemi di A si dice **partizione** di A se : *partizioni*

i) $X \neq \emptyset$ per ogni $X \in \mathcal{F}$;

ii) $\bigcup_{X \in \mathcal{F}} X = A$;

iii) per ogni $X, Y \in \mathcal{F}$: se $X \neq Y$ allora $X \cap Y = \emptyset$.

Quindi l'insieme quoziente di A modulo una relazione di equivalenza è una partizione di A.

Nota. Viceversa, si vede facilmente che se $\mathcal{F}$ è una partizione di A, allora la relazione $\sim_{\mathcal{F}}$ su A definita da

$$a \sim_{\mathcal{F}} b \quad \text{se esiste } X \in \mathcal{F} \quad \text{tale che } \{a, b\} \subseteq X$$

è una relazione di equivalenza. Inoltre, se $\mathcal{F}$ è l'insieme quoziente $A/\sim$ allora $\sim_{\mathcal{F}}$ coincide con $\sim$.
Fissato un insieme A, il concetto di relazione di equivalenza e quello di partizione su A sono quindi equivalenti.

Un concetto utile è quello dell'applicazione che ad ogni elemento di un insieme A su cui è data una equivalenza, associa la corrispondente classe di equivalenza. Precisamente: sia $\sim$ una relazione di equivalenza sull'insieme A. La **proiezione canonica** di A su $A/\sim$ è l'applicazione $\pi : A \longrightarrow A/\sim$ definita da, per ogni $x \in A, \pi(x) = [x]_{\sim}$. *proiezione*

Esempio (*Equivalenza definita da un'applicazione*). Sia $f : A \longrightarrow B$ un'applicazione. L'equivalenza definita da f è la relazione $\sim_f$ sull'insieme A definita da, per ogni $x, y \in A$: $x \sim_f y$ se $f(x) = f(y)$. *equival. e applicazioni*

Si verifica facilmente che la relazione $\sim_f$ così definita è una equivalenza su A, infatti :

- (riflessività) : per ogni $a \in A$ si ha $f(a) = f(a)$ e dunque $a \sim_f a$.

- (simmetria): se $a, b \in A$ e $a \sim_f b$, allora $f(a) = f(b)$, dunque $f(b) = f(a)$ e $b \sim_f a$

- (transitività): siano $a, b, c \in A$ con $a \sim_f b$, $b \sim_f c$; allora $f(a) = f(b) = f(c)$ e dunque $f(a) = f(c)$ e $a \sim_f c$.

Per esempio, l'equivalenza ρ dell'esempio 1) di sopra è l'equivalenza definita dalla applicazione:

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\mapsto |x| \end{aligned}$$

2) L'equivalenza dell'esempio 2) è l'equivalenza definita dalla applicazione dall'insieme Σ di tutte le circonferenze nell'insieme dei punti del piano, che ad ogni circonferenza $C \in \Sigma$ associa il centro di C.

3) L'equivalenza ω dell'esempio 3) è l'equivalenza definita dalla applicazione:

$$\begin{array}{c} f: \ \mathbb{N} \times \mathbb{N} \setminus \{0\} \ \longrightarrow \ \mathbb{Q} \\ (a,b) \ \mapsto \ \frac{a}{b} \end{array}$$

Nota. Si osservi che una applicazione f è iniettiva se e solo se l'equivalenza definita da f è l'uguaglianza (e in tal caso l'insieme quoziente $A/\sim_f$ si può identificare con A).

5.3 Relazioni d'ordine.

Un relazione ρ sull'insieme A si dice **antisimmetrica** se, per ogni $a, b \in A$:

$$a\rho b \ \text{ e } \ b\rho a \ \ \Rightarrow \ \ a = b.$$

relazioni d' ordine

Una relazione ρ sull'insieme A si dice **relazione d'ordine** (o *ordinamento parziale*) se ρ è riflessiva, antisimmetrica e transitiva. Ovvero se, per ogni $a, b, c \in A$

(i) $a\rho a$

(ii) $a\rho b \ \text{ e } \ b\rho a \ \Rightarrow \ a = b$

(iii) $a\rho b \ \text{ e } \ b\rho c \ \Rightarrow \ a\rho c.$

Un **insieme parzialmente ordinato** (p.o.) è una coppia (A, ρ) dove A è un insieme e ρ una relazione di ordine su A.

Esempi. 1) Sono insiemi parzialmente ordinati

$$(\mathbb{R}, \leq) \quad (\mathbb{Q}, \leq) \quad (\mathbb{Z}, \leq) \quad (\mathbb{N}, \leq)$$

dove $\leq$ è l'ordine naturale (ad esempio definito su $\mathbb{R}$ da $x \leq y$ se $y - x \geq 0$, ovvero se esiste $a \in \mathbb{R}$ tale che $y - x = a^2$).

2) Se X è un insieme, allora $(\mathcal{P}(X), \subseteq)$ dove $\subseteq$ è l'inclusione tra insiemi, è un insieme parzialmente ordinato.

3) Sia $|$ la relazione di divisibilità su $\mathbb{N}$, definita da, per ogni $a, b \in \mathbb{N}$:

$$a|b \ \text{ se esiste } \ c \in \mathbb{N} \ \text{ tale che } \ ac = b.$$

Allora | è una relazione di ordine su $\mathbb{N}$. Infatti
- per ogni $n \in \mathbb{N},\ n1 = n$, quindi $n|n$ e la relazione è riflessiva.
- se $n|m$ e $m|n$, allora esistono $c, d \in \mathbb{N}$ tali che $m = cn$ e $n = dm$; da cui segue $m = cn = cdm$. Se $m = 0$, allora $n = dm = 0$; altrimenti si ha $cd = 1$ e poichè $cd \in \mathbb{N}$ deve essere $c = 1 = d$ e quindi $n = m$ e la relazione è antisimmetrica.
- Siano $n, m, s \in \mathbb{N}$ con $n|m,\ m|s$. Allora esistono $c, d \in \mathbb{N}$ tali che $m = cn$ e $s = dm$; quindi $s = dm = (dc)n$. Dunque $n|s$ e la relazione è transitiva.

Per indicare una generica relazione d'ordine su un insieme generico useremo di solito il simbolo $\leq$.

Un insieme parzialmente ordinato $(A, \leq)$ si dice **totalmente ordinato** se

$$\text{per ogni } \ a, b \in A,\ a \leq b \ \text{ o } \ b \leq a\ .$$

Gli esempi del tipo 1) di sopra sono insiemi totalmente ordinati. Quelli del tipo 2) non sono totalmente ordinati se $|X| \geq 2$; infatti se a_1, a_2 sono elementi distinti di X, allora $\{a_1\}, \{a_2\} \in \mathcal{P}(X)$ e $\{a_1\} \not\subseteq \{a_2\}\ , \{a_2\} \not\subseteq \{a_1\}$.
Infine, $(\mathbb{N}, |)$ nell' esempio 3) non è totalmente ordinato: ad esempio $2 \not| 3$ e $3 \not| 2$.

massimi e minimi

Sia $(A, \leq)$ un insieme parzialmente ordinato e sia $a \in A$:

1. a si dice elemento **massimo** di A se per ogni $b \in A,\ b \leq a$.

2. a si dice elemento **minimo** di A se per ogni $b \in A,\ a \leq b$.

Ad esempio, gli insiemi p.o. $(\mathbb{R}, \leq)\ , (\mathbb{Q}, \leq)\ , (\mathbb{Z}, \leq)$ non hanno né massimo né minimo. L'insieme $(\mathbb{N}, \leq)$ non ha massimo ed ha minimo 0.
Se X è un insieme, l'insieme p.o. $(\mathcal{P}(X), \subseteq)$ ha minimo $\emptyset$ e massimo X.
L'insieme p.o. $(\mathbb{N}, |)$ ha minimo 1 (infatti $1|n$ per ogni $n \in \mathbb{N}$) e massimo 0 (infatti $n|0$ per ogni $n \in \mathbb{N}$). Se però togliamo 0 e consideriamo $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, l'insieme p.o. $(\mathbb{N}^*, |)$ non ha massimo nè elementi massimali: infatti, se $n \in \mathbb{N}^*$ allora $n|2n$ e $n \neq 2n$.

Dalle definizioni segue, in particolare, che ogni elemento massimo (minimo) è anche un elemento massimale (minimale).
Osserviamo anche che un insieme p.o. può avere diversi elementi minimali (o massimali). Ad esempio nell'insieme p.o. $(\mathbb{N} \setminus \{1\}, |)$ dei numeri naturali diversi da 1 ordinato per divisibilità, gli elementi minimali sono tutti i numeri primi (positivi).

Questo non avviene per massimo e minimo: essi, se esistono, sono unici.

Proposizione 5.3.1. *Sia $(A, \leq)$ un insieme parzialmente ordinato. Se $(A, \leq)$ ha un elemento massimo (minimo), allora esso è l'unico massimo (minimo) di $(A, \leq)$.*

Dimostrazione. Sia $a \in A$ un elemento massimo di $(A, \leq)$ e sia b un massimale. Allora $b \leq a$ perchè a è massimo, e quindi, poichè b è massimale, $a = b$.
(la dimostrazione per il minimo è simile.) ∎

Dunque, il massimo (minimo) di $(A, \leq)$, quando esiste è unico; esso si denota con $\max(A)$ ($\min(A)$. Più in generale, se $(A, \leq)$ è un insieme p.o. e B è un sottoinsieme non vuoto di A, un elemento $x \in B$ si dice massimo (minimo) di B se, per ogni $b \in B$ si ha $b \leq x$ ($x \leq b$). Si dimostra allo stesso modo che se B ha un massimo (minimo) esso è unico, e si denota con $\max(B)$ ($\min(B)$).

Ad esempio in $(\mathbb{N}, |\ )$ consideriamo il sottoinsieme $B = \{3n \mid 0 \neq n \in \mathbb{N}\}$. Allora B non ha massimo, e $\min(B) = 3$.

maggioranti e minoranti

Sia $(A, \leq)$ un insieme parzialmente ordinato, sia $B \subseteq A$ e sia $a \in A$:

1. a si dice **maggiorante** di B se per ogni $b \in B,\ b \leq a$.
2. a si dice **minorante** di B se per ogni $b \in B,\ a \leq b$.

Esempi. 1) Nell'insieme p.o. $(\mathbb{Z}, \leq)$ il sottoinsieme $\mathbb{N}$ non ha maggioranti, mentre i suoi minoranti sono tutti gli interi $z \leq 0$.
In $(\mathbb{Q}, \leq)$ gli insiemi $B = \{\ x \in \mathbb{Q} \mid x \leq \frac{1}{3}\ \}$ e $C = \{\ x \in \mathbb{Q} \mid x < \frac{1}{3}\ \}$ hanno lo stesso insieme di maggioranti che è $\{\ x \in \mathbb{Q} \mid x \geq \frac{1}{3}\ \}$.
In $(\mathbb{R}, \leq)$ l'insieme dei maggioranti di $\{\ x \in \mathbb{Q} \mid x^2 \leq 2\ \}$ è $\{\ x \in \mathbb{R} \mid x \geq \sqrt{2}\ \}$.
2) Se X è un insieme non vuoto e $Y, Z \subseteq X$, l'insieme dei minoranti di $B = \{Y, Z\}$ nell'insieme p.o. $(\mathcal{P}(X), \subseteq)$ è $\{\ T \subseteq X \mid T \subseteq Y \cap Z\ \}$.
3) In $(\mathbb{N}, |)$ consideriamo il sottoinsieme $B = \{\ 6,\ 9,\ 15\ \}$; allora i minoranti di B sono $1, 3$ e i maggioranti di B sono tutti i multipli di 30.

Dalla Proposizione 5.3.1, risulta che se l'insieme dei maggioranti (minoranti) di un sottoinsieme B ha minimo (massimo), esso è unico. Da qui la seguente definizione.

estremo sup. e inf.

Sia $(A, \leq)$ un insieme parzialmente ordinato e sia $B \subseteq A$:

1. l'**estremo superiore** $\sup_A(B)$ di B in A è, se esiste, il minimo dei maggioranti di B.
2. l'**estremo inferiore** $\inf_A(B)$ di B in A è, se esiste, il massimo dei minoranti di B.

Dalla definizione segue immediatamente che se B ha massimo (minimo) allora $\max(B) = \sup_A(B)$ $(\min(B) = \inf_A(B))$.

Esempi. Con riferimento agli esempi di sopra, abbiamo

- $\inf_{\mathbb{Z}} \mathbb{N} = 0$; mentre $\mathbb{N}$ non ha estremo superiore in $(\mathbb{Z}, \leq)$.
- Se $B = \{x \in \mathbb{Q} \mid x < \frac{1}{3}\}$, $\inf_{\mathbb{Q}}(B) = \frac{1}{3}$.
- Se $C = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$, allora $\inf_{\mathbb{R}}(C) = -\sqrt{2}$, $\sup_{\mathbb{R}}(C) = \sqrt{2}$, mentre C non ha estremi inferiore e superiore in $(\mathbb{Q}, \leq)$.
- Se $Y, Z \subseteq X$, allora $\inf_{\mathcal{P}(X)}(\{Y, Z\}) = Y \cap Z$ e $\sup_{\mathcal{P}(X)}(\{Y, Z\}) = Y \cup Z$.
- $B = \{6,\ 9,\ 15\}$ non ha estremo inferiore in $(\mathbb{N}, |)$ mentre il suo estremo superiore è 90 .

Osserviamo che se X è un insieme e $\mathcal{S}$ un sottoinsieme non vuoto di $\mathcal{P}(X)$, allora

$$U = \bigcup_{X \in \mathcal{S}} X = \sup_{\mathcal{P}(X)}(\mathcal{S}) \qquad \text{e} \qquad W = \bigcap_{X \in \mathcal{S}} X = \inf_{\mathcal{P}(X)}(\mathcal{S})$$

infatti, U è un maggiorante di $\mathcal{S}$ in $(\mathcal{P}(X), \subseteq)$, e se Y è un maggiorante di $\mathcal{S}$ allora $X \subseteq Y$ per ogni $X \in \mathcal{S}$, e quindi $U \subseteq Y$. Dunque U è il minimo dei maggioranti di $\mathcal{S}$ e quindi $U = \sup_{\mathcal{P}(X)}(\mathcal{S})$. Similmente si osserva che W è il massimo dei minoranti di $\mathcal{S}$.

Un **reticolo** è un insieme parzialmente ordinato $(A, \leq)$ in cui, per ogni $a, b \in A$ esiste $\sup(\{a, b\})$ e $\inf(\{a, b\})$.

Se $(A, \leq)$ è un reticolo, e $a, b \in A$ si scrive

$$a \wedge b = \inf(\{a, b\}) \quad \text{e} \quad a \vee b = \sup(\{a, b\}).$$

Esempi. 1) Sia $(A, \leq)$ un insieme p.o., $a, b \in A$ e $a \leq b$, allora $a = \inf(\{a, b\})$ e $b = \sup(\{a, b\})$. Da ciò segue che ogni insieme totalmente ordinato è un reticolo.

2) Se X è un insieme non vuoto $(\mathcal{P}(X), \subseteq)$ è un reticolo. Per ogni $Y, Z \in \mathcal{P}(X)$:

$$Y \wedge Z = Y \cap Z \quad \text{e} \quad Y \vee Z = Y \cup Z.$$

3) $(\mathbb{N}, |)$ è un reticolo. Se $a, b \in \mathbb{N}$, allora $a \wedge b = MCD(a, b)$ e $a \vee b = m.c.m.(a, b)$.

4) Sia X un insieme, con $|X| \geq 4$ e sia $\mathcal{D} = \{\ Y \subseteq X \mid |Y|$ è dispari $\}$. Allora $(\mathcal{D}, \subseteq)$ è un un insieme p.o. ma non è un reticolo. Infatti, siano $a, b \in X$ con $a \neq b$ e poniamo $A = \{a\}$, $B = \{a\}$; allora $A, B \in \mathcal{D}$ e, per ogni $x \in X$ con $a \neq x \neq b$ il sottoinsieme $\{a, b, x\}$ è un elemento minimale nell'insieme dei maggioranti in $\mathcal{D}$ di $\{A, B\}$. Poichè $|X| \geq 4$ l'insieme dei maggioranti di $\{A, B\}$ ha almeno due elementi minimali e dunque non ha minimo, cioè non esiste l'estremo superiore in $\mathcal{D}$ di $\{A, B\}$.

5.4 Esercizi.

Esercizio 5.1. Si provi che la relazione $\sim$ definta sull'insieme $\mathbb{R}$ dei numeri reali da, per ogni $x, y \in \mathbb{R}$,

$$x \sim y \text{ se } x - y \in \mathbb{Z}$$

è una relazione di equivalenza.

Esercizio 5.2. Sia ρ la relazione sull'insieme $\mathbb{Z}$ dei numeri interi definita da:
per ogni $a, b \in \mathbb{Z}$, $a \rho b$ se $a^2 - b^2$ è divisibile per 4.
Si provi che ρ è una equivalenza e si determini la classe di equivalenza di 3.

Esercizio 5.3. Determinare tutte le relazioni di equivalenza dell'insieme $\{1, 2, 3\}$ e quelle dell'insieme $\{1, 2, 3, 4\}$.

Esercizio 5.4. Sia X un insieme non vuoto e sia $A = X^{\mathbb{N}}$ l'insieme di tutte le applicazioni dall'insieme $\mathbb{N}$ dei numeri naturali nell'insieme X. In A si consideri la relazione ω, definita ponendo, per ogni f , $g \in A$, $f \omega g$ se e solo se esiste $n \in \mathbb{N}$ tale che $f(i) = g(i)$ per ogni $i \geq n$. Si dimostri che ω è una relazione di equivalenza.

Esercizio 5.5. Sia ω una relazione di equivalenza sull'insieme A. Su $A \times A$ sia definita una relazione ρ ponendo, per ogni $(a, b), (c, d) \in A \times A$,

$$(a, b) \rho (c, d) \quad \text{se} \quad a \omega c \text{ o } b \omega d.$$

Si dica se ρ è una relazione di equivalenza.

Esercizio 5.6. Siano ρ, ρ' relazioni su un insieme A. Si definisca la *relazione composta* $\rho \circ \rho'$ ponendo, per ogni $x, y \in A$, $x(\rho \circ \rho')y$ se esiste $z \in A$ tale che $x \rho z$ e $z \rho' y$. Si provi che

(a) se ρ e ρ' sono riflessive, allora $\rho \circ \rho'$ è riflessiva;

(b) ρ è transitiva se e solo se $\rho \circ \rho \subseteq \rho$;

(c) si trovi un esempio in cui ρ e ρ' sono equivalenze ma $\rho \circ \rho'$ non è una equivalenza.

Esercizio 5.7. Nell'insieme $A = \mathbb{N} \times \mathbb{N}$ sia definita la relazione ω ponendo , per ogni $(a,b),(c,d) \in A:\ (a,b)\omega(c,d)$ se e solo se $b = d$.
Si provi che ω è una equivalenza, si descriva l'insieme quoziente A/ω, e si trovi una applicazione $f : A \longrightarrow \mathbb{N}$ tale che ω sia l'equivalenza definita da f.

Esercizio 5.8. Sull'insieme $\mathbb{N}^*$ dei numeri naturali non nulli si definiamo la relazione ρ ponendo, per ogni $x, y \in \mathbb{N}^*$, $x\rho y$ se $\frac{1}{x} \leq \frac{1}{y}$. Si dimostri che ρ è una relazione d' ordine su $\mathbb{N}^*$.

Esercizio 5.9. (Ordine lessicografico) Siano (A,ρ), (B,σ) due insiemi parzialment ordinati. Sul prodotto $A \times B$ definiamo la relazione $\leq$ ponendo, per ogni $(a,b),(a_1,b_1) \in A \times B$,

$$(a,b) \leq (a_1,b_1) \text{ se } a\rho a_1 \text{ e } a \neq a_1 \text{ oppure } a = a_1 \text{ e } b\sigma b_1.$$

Si dimostri che $\leq$ è una relazione d'ordine su $A \times B$. Si dimostri che $(A \times B, \leq)$ è totalmente ordinato se e solo se tali sono (A,ρ) e (B,σ).

Esercizio 5.10. Sia $(A,\leq)$ un insieme parzialmente ordinato. Sull'insieme A^A di tutte le applicazioni di A in sè definiamo la relazione ρ ponendo, per ogni $f, g \in A^A$, $f\rho g$ se $f(a) \leq g(a)$ per ogni $a \in A$. Si dimostri che ρ è una relazione d'ordine parziale. Si provi che ρ è una relazione d'ordine totale se e solo se $|S| = 1$.

Esercizio 5.11. Sia $(A,\leq)$ un insieme parzialmente ordinato, e siano $a, b \in A$. Si dimostri che le seguenti affermazioni sono equivalenti

1. $a = \inf(\{a,b\})$;
2. $a \leq b$;
3. $b = \sup(\{a,b\})$.

Esercizio 5.12. Sia $(A,\leq)$ un insieme totalmente ordinato. Si dimostri che ogni sottoinsieme **finito** e non vuoto di A ha massimo e minimo.

Esercizio 5.13. Sull'insieme $\mathbb{N}^*$ dei numeri naturali non nulli definiamo la relazione ρ ponendo, per ogni $n, m \in \mathbb{N}^*, n\rho m$ se esiste $b \in \mathbb{N}^*$ tale che $m = n^b$. Si dimostri che ρ è una relazione d'ordine. Si dica per quali coppie $n, m \in \mathbb{N}^*$ esiste l'estremo superiore di $\{n, m\}$.

Esercizio 5.14. Sia $(A,\leq)$ un reticolo. Si provi che, per ogni $x, y, z \in A$ si ha:

1. $x \wedge (y \wedge z) = (x \wedge y) \wedge z)$;
2. $x \vee (y \vee z) = (x \vee y) \vee z)$;

3. $x \wedge (x \vee y) = x = x \vee (x \wedge y)$.

Esercizio 5.15. Su $\mathbb{Q}$ definiamo la relazione ρ ponendo, per ogni $x, y \in \mathbb{Q}$, $x \rho y$ se esiste $n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$ tale che $y = nx$. Si dimostri che $(\mathbb{Q}, \rho)$ è un insieme parzialmente ordinato. Si dica se è totalmente ordinato. Si determinino, se esistono, gli estremi inferiore e superiore dei sottoinsiemi $\{\frac{1}{2^m} \mid 0 \neq m \in \mathbb{N}\}$ e $\{\frac{1}{3}, \frac{3}{2}\}$. Si dica se $(\mathbb{Q}, \rho)$ è un reticolo.

Capitolo 6

Numeri Interi II

6.1 Equazioni diofantee

Con *equazione diofantea* (dal matematico alessandrino Diofanto) si intende genericamente una equazione algebrica le cui soluzioni sono cercate in prefissate classi di numeri; in particolare quando le soluzioni cercate sono numeri interi. Allo studio della risolubilità (e delle soluzioni) di particolari equazioni diofantee è riconducibile una considerevole parte della teoria dei numeri, così come sono molteplici gli strumenti sviluppati nel corso dei secoli per affrontare simili questioni.

Un primo facile caso di equazione diofantea è collegato al Teorema 3.3.1

Proposizione 6.1.1. *Siano a, b ed n numeri interi (con a e b non entrambi nulli); allora l'equazione*

$$ax + by = n$$

ammette soluzioni in $\mathbb{Z}$ se e solo se $(a, b)|n$.

Dimostrazione. Siano a, b, n numeri interi, con a e b non entrambi nulli, e sia $d = (a, b)$.

Supponiamo che esistano $x, y \in \mathbb{Z}$, tali che $ax + by = n$. Poiché d divide sia a che b, a/d e b/d sono numeri interi, e quindi

$$\frac{n}{d} = \frac{a}{d} \cdot x + \frac{b}{d} \cdot y$$

è un numero intero. Dunque d divide n.

Viceversa, supponiamo che d divida n, e sia $c = n/d$ (che è un numero intero). Per il Teorema 3.3.1 esistono interi α e β tali che $\alpha a + \beta b = d$. Ponendo $u = c\alpha$

e $w = c\beta$, si ha $u, w \in \mathbb{Z}$ e

$$au + bw = c\alpha a + c\beta b = c(\alpha a + \beta b) = cd = n$$

e dunque la coppia ordinata $(u,\, w)$ è una soluzione dell'equazione $ax + by = n$. ∎

In generale, se $a_1, a_2, \ldots, a_k$ sono interi non nulli, allora esiste il loro MCD positivo, che è denotato con $(a_1, a_2, \ldots, a_k)$, ed è definito nel modo ovvio. Si provi, ragionando per induzione su k che $(a_1, a_2, \ldots, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k)$, e dunque che esistono interi $\alpha_1, \alpha_2, \ldots \alpha_k$ tali che

$$(a_1, a_2, \ldots, a_k) = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k.$$

Si provi quindi che l'equazione $a_1x_1 + a_2x_2 + \cdots + a_kx_k = n$ ammette soluzioni intere se e solo se $(a_1, a_2, \ldots, a_k)$ divide n.

Nota. Sia a un intero. Con $a\mathbb{Z}$ si denota l'insieme di tutti i multipli interi di a, ovvero

$$a\mathbb{Z} = \{\ az \mid z \in \mathbb{Z}\ \}.$$

Sia $b \in \mathbb{N}$ un altro numero intero, e poniamo, per definizione

$$a\mathbb{Z} + b\mathbb{Z} = \{x + y \mid x \in a\mathbb{Z},\ y \in b\mathbb{Z}\ \} = \{\ az_1 + bz_2 \mid z_1, z_2 \in \mathbb{Z}\ \}.$$

Allora, la Proposizione 6.1.1 dice precisamente che, se a e b sono non entrambi nulli

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}.$$

Esercizio. Sia $n \in \mathbb{N}^*$ e siano a, b interi non nulli tali che $(a, b)|n$. Sia (x_o, y_o) una soluzione dell'equazione diofantea $ax + by = n$. Si provi che l'insieme delle soluzioni di tale equazione è

$$\left\{ \left(x_o + t\frac{b}{(a,b)},\, y_o - t\frac{a}{(a,b)} \right) \;\middle|\; t \in \mathbb{Z} \right\}.$$

Un poco più complicata è la situazione in cui si richiede l'esistenza di soluzioni non negative. La dimostrazione del seguente risultato è lasciata per esercizio.

Lemma 6.1.2. *Siano $a, b \in \mathbb{N}^*$ tali che $(a, b) = 1$. Se $n \geq a(b-1)$, allora esistono interi non negativi x, y tali che $ax + by = n$.*

Un esempio assai famoso di equazione diofantea è il cosiddetto *ultimo teorema di Fermat*, che fu enunciato da P. Fermat nel 1637. Fermat scrisse di averne trovato una dimostrazione 'mirabile', ma di non avere lo spazio per riportarla (egli stava appunto annotando un testo di Diofanto). Dopo secoli di sforzi (inefficaci a dimostrare l'asserzione di Fermat, ma importantissimi per lo sviluppo di molte idee matematiche), l'ultimo teorema di Fermat è stato finalmente dimostrato da Andrew Wyles verso la fine del secolo scorso, utilizzando metodi assai profondi di geometria algebrica.

Teorema 6.1.3. (Fermat - Wyles). *Sia n un numero naturale. Se $n \geq 3$, non esistono soluzioni intere dell'equazione*

$$x^n + y^n = z^n$$

tali che $xyz \neq 0$.

Il caso invece in cui l'esponente n è uguale a 2 è elementare.

Proposizione 6.1.4. *Ogni soluzione intera dell'equazione*

$$x^2 + y^2 = z^2$$

si scrive nella forma $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$, dove $(m, n) = 1$.

Dimostrazione. Si verifica facilmente che per ogni $k, n, m \in \mathbb{N}^*$, con $(n, m) = 1$, la terna $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$ è una soluzione dell'equazione data (ed è detta, per ovvî motivi, *terna pitagorica*).
Viceversa, siano $x, y, z \in \mathbb{N}^*$ tali che $x^2 + y^2 = z^2$, e sia $k = (x, y)$. Osserviamo che allora $k = (x, z) = (y, z)$. Siano $a, b, c \in \mathbb{N}^*$, con

$$x = ka, \quad y = kb, \quad z = kc \ .$$

Allora $(a, b) = (a, c) = (b, c) = 1$ e $a^2 + b^2 = c^2$. Dunque

$$c^2 = a^2 + b^2 = (a + b)^2 - 2ab \ .$$

a e b non sono entrambi pari. Se fossero entrambi dispari, allora $a+b$ e c sarebbero pari, e quindi $4|c^2$ e $4|(a + b)^2$, da cui segue la contraddizione $4|2ab$. Possiamo quindi assumere che a sia dispari e b sia pari (e quindi c è dispari). Sia $d =$

$(c+a, c-a)$; allora $2|d$, ed inoltre $d|(c+a)+(c-a) = 2c$ (analogamente $d|2a$), e dunque, poiché a e c sono coprimi, $d = 2$. Siano ora $u, v \in \mathbb{N}^*$ tali che

$$c + a = 2u \qquad c - a = 2v \ .$$

Per quanto appena osservato $(u, v) = 1$. Inoltre

$$b^2 = c^2 - a^2 = (c+a)(c-a) = 4uv \ ;$$

e dunque u e v sono quadrati: sia $u = m^2$ e $v = n^2$. Allora,

- $b^2 = 4m^2n^2$, e quindi $b = 2mn$, e $y = 2kmn$.
- $2c = 2(u+v) = 2(m^2+n^2)$, e quindi $c = m^2+n^2$, e $z = k(m^2+n^2)$.
- $2a = 2(u-v) = 2(m^2-n^2)$, e quindi $a = m^2-n^2$, e $x = k(m^2-n^2)$. ∎

Esercizio. Provare che l'equazione $x^4 + y^4 = z^2$ non ha soluzioni intere non banali (cioè tali che $xyz \neq 0$). In particolare, quindi, il Teorema di Fermat è vero per l'esponente $n = 4$.

L'importanza delle equazione diofantee non risiede tanto nella loro applicabilità 'pratica' (anche all'interno della matematica stessa), quanto nel profluvio di idee - a volte molto sofisticate - a cui il loro studio ha dato e dà luogo (ad esempio la teoria degli anelli e degli ideali, che studieremo più avanti, è nata da un tentativo di attaccare la congettura di Fermat), e nella suggestione esercitata da problemi i cui enunciati sono comprensibili anche ad un livello assolutamente elementare.
Un esempio curioso è la congettura di Catalan, della quale, nella primavera del 2002, il matematico romeno Preda Mihailescu ha annunciato una dimostrazione.

Congettura di Catalan: *Siano* $2 \leq n, m \in \mathbb{N}$. *L'unica soluzione dell'equazione diofantea*

$$x^n = y^m - 1$$

si ha per $n = 2$, $m = 3$, ed è $x = 3$, $y = 2$.

(I soli numeri naturali consecutivi che sono potenze non banali di numeri interi sono 8 e 9.)

6.2 Congruenze

Le congruenze sono importanti relazioni d'equivalenza definite sull'insieme $\mathbb{Z}$ dei numeri interi (nella forma usata ancor oggi sono state introdotte da C.F. Gauss). Le ritroveremo in molte situazioni durante l'intero corso. Devono quindi diventare subito un oggetto familiare.

Definizione. Sia $n \geq 1$ un fissato numero naturale. Due interi a, b si dicono *congrui modulo* n se n divide $a - b$. In tal caso si scrive

$$a \equiv b \pmod{n}$$

In altri termini, due interi a, b sono congrui modulo n se e solo se esiste $z \in \mathbb{Z}$ tale che $a - b = zn$; ovvero se e solo se $b = a + nz$ per qualche $z \in \mathbb{Z}$.

Verifichiamo subito che, per ogni fissato $n \geq 1$, la relazione di congruenza modulo n è una equivalenza su $\mathbb{Z}$.

- vale la *riflessività*. Infatti, per ogni $a \in \mathbb{Z}$ si ha $0n = a - a$ e quindi $a \equiv a \pmod{n}$.

- vale la *simmetria*. Infatti, siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$. Allora $a - b = nz$ per qualche $z \in \mathbb{Z}$. Da ciò segue subito $b - a = n(-z)$ e quindi $b \equiv a \pmod{n}$.

- vale la *transitività*. Infatti, siano $a, b, c \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$. Allora esistono $z, z' \in \mathbb{Z}$ tali che $a - b = nz$ e $b - c = nz'$. Da ciò segue

$$a - c = (a - b) + (b - c) = nz + nz' = n(z + z')$$

e quindi $a \equiv c \pmod{n}$.

Fissato un $n \geq 1$, per ogni $a \in \mathbb{Z}$ la classe di equivalenza di a modulo la congruenza modulo n si chiama **classe di congruenza** di a modulo n. Quando il modulo n sia fissato e non vi siano possibilità di confusione, per comodità indicheremo la classe di congruenza di a semplicemente con $\overline{a}$ (o anche con $[a]$). Per quanto osservato sopra si ha quindi

$$\overline{a} = \{\ b \in \mathbb{Z} \mid a \equiv b \pmod{n}\ \} = \{\ b \in \mathbb{Z} \mid b = a + nz \ \text{ con } z \in \mathbb{Z}\ \}\ .$$

Un'altra maniera per denotare la classe di congruenza di a modulo n è quella di scrivere

$$a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\}.$$

Ad esempio, se $n = 5$,
$\overline{0} = \{\ b \in \mathbb{Z} \mid b = 5z \ \text{ con } z \in \mathbb{Z}\ \} = \{\ 5z \mid z \in \mathbb{Z}\ \} = \{0, 5, -5, 10, -10, 15, -15, \ldots\}$,
$\overline{1} = \{\ 1 + 5z \mid z \in \mathbb{Z}\ \} = \{1, 6, -4, 11, -9, 16, -14, \ldots\}$, e così via.

Dato $n \geq 1$, l'insieme di tutte la classi di congruenza modulo n (cioè l'insieme quoziente di $\mathbb{Z}$ modulo la congruenza modulo n) lo denoteremo con $\mathbb{Z}/n\mathbb{Z}$.

Osserviamo che la congruenza modulo 1 non è altro che la relazione banale su $\mathbb{Z}$; infatti per ogni $a, b \in \mathbb{Z}$, 1 divide $a - b$. Rispetto alla congruenza modulo 1 esiste quindi una sola classe di equivalenza che è $\mathbb{Z}$ stesso. Se invece consideriamo la congruenza modulo 2, osserviamo che due interi a, b sono congrui modulo 2 se e solo se sono entrambi pari o entrambi dispari. Dunque rispetto alla congruenza modulo 2 esistono due classi di equivalenza: una costituita da tutti i numeri pari e la seconda da tutti i numeri dispari (cioè $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$). Tutto ciò si può generalizzare; fissato $n \geq 1$, il numero di classi di congruenza modulo n è esattamente n.

Preliminarmente, facciamo la seguente semplice ma importante osservazione. Dato il modulo $n \geq 1$, possiamo dividere ogni intero a per n

$$a = nq + r \qquad \text{con} \quad 0 \leq r \leq n - 1;$$

pertanto n divide la differenza $a - r$, e dunque,

$$a \equiv r \pmod{n}.$$

Abbiamo cioè che, fissato il modulo $n \geq 1$, *un intero a è congruo modulo n al resto della divisione di a per n.* Enunciamo ora il risultato generale.

Teorema 6.2.1. *Sia $n \geq 1$ e, per ogni $a \in \mathbb{Z}$ indichiamo con $\overline{a}$ la classe di congruenza di a modulo n, e con $\mathbb{Z}/n\mathbb{Z}$ l'insieme quoziente. Allora*

$$\mathbb{Z}/n\mathbb{Z} = \{\ \overline{0},\ \overline{1},\ \overline{2}, \ldots, \overline{n-1}\ \}.$$

Quindi $|\mathbb{Z}/n\mathbb{Z}| = n$. Inoltre per ogni $a \in \mathbb{Z}$, $\overline{a} = \overline{r}$ dove r è il resto della divisione di a per n.

Dimostrazione. Sia $a \in \mathbb{Z}$. Per quanto abbiamo osservato sopra,

$$a \equiv r \pmod{n}$$

dove r è il resto della divisione di a per n. Quindi $\overline{a} = \overline{r}$. Poiché $0 \leq r \leq n - 1$, concludiamo che ogni classe di congruenza modulo n coincide con una delle

$$\overline{0},\ \overline{1},\ \overline{2}, \ldots, \overline{n-1}\ .$$

Rimane da provare che queste sono a due a due distinte. Siano quindi j, k tali che $0 \leq j \leq k \leq n - 1$ e supponiamo che, modulo n, $\overline{j} = \overline{k}$. Allora $k \equiv j \pmod{n}$ cioè n divide $k - j$. Ma $0 \leq k - j \leq n - 1$, dunque la sola possibilità che n divida $k - j$ è che $k = j$. Abbiamo così completato la dimostrazione. ∎

L'aspetto veramente importante delle congruenze è che con esse (o più precisamente con le classi di congruenza) è possibile eseguire le operazioni di somma e prodotto.

Teorema 6.2.2. *Sia $n \geq 1$, e siano $a, b, c, d \in \mathbb{Z}$ tali che*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases}$$

Allora $a + c \equiv b + d \pmod{n}$ *e* $ac \equiv bd \pmod{n}$.

Dimostrazione. Siano $a, b, c, d \in Z$ con $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Allora, n divide sia $a - b$ che $c - d$. Quindi

$$n \text{ divide } (a - b) + (c - d) = (a + c) - (b + d),$$

e dunque

$$a + c \equiv b + d \pmod{n}.$$

Similmente, n divide

$$(a - b)c + b(c - d) = ac - bc + bc - bd = ac - bd,$$

e dunque $ac \equiv bd \pmod{n}$. ∎

Esempio. Come esempio di applicazione del risultato precedente dimostriamo il seguente *criterio di divisibilità per* 11: un intero positivo n è divisibile per 11 se e solo se la somma delle cifre decimali di posto pari di n è congrua modulo 11 alla somma delle cifre decimali di posto dispari. Ad esempio, 13570645 è divisibile per 11 (il più noto criterio di divisibilità per 3 sarà trattato negli esercizi). Iniziamo con il provare, per induzione su $k \geq 1$, che

$$10^k \equiv (-1)^k \pmod{11}.$$

La cosa è immediata per $k = 1$. Sia $k \geq 2$. Allora, per ipotesi induttiva $10^{k-1} \equiv (-1)^{k-1} \pmod{11}$., ed inoltre $10 \equiv (-1) \pmod{11}$. Applicando la parte relativa al prodotto del Teorema 6.2.2 si ottiene allora

$$10^k = 10^{k-1} \cdot 10 \equiv (-1)^{k-1}(-1) \pmod{11},$$

completando così l'induzione. A questo punto, sia

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_2 10^2 + a_1 10 + a_0$$

la rappresentazione decimale del numero n e supponiamo, per semplicità, che k sia pari. Allora, per quanto osservato sopra, e ancora per la parte additiva del Teorema 6.2.2 si ha

$$\begin{aligned} n_0 &= a_k 10^k + a_{k-2} 10^{k-2} + \ldots + a_2 10^2 + a_0 \equiv \\ &\equiv a_k (-1)^k + a_{k-2} (-1)^{k-2} + \ldots a_2 (-1)^2 + a_0 \equiv \\ &\equiv a_k + a_{k-2} + \ldots a_2 + a_0 \pmod{11}, \end{aligned}$$

ed inoltre

$$\begin{aligned} n_1 &= a_{k-1}10^{k-1} + a_{k-3}10^{k-3} + \ldots + a_3 10^3 + a_1 10 \equiv \\ &\equiv a_{k-1}(-1)^{k-1} + a_{k-3}(-1)^{k-3} + \ldots a_3(-1)^3 + a_1(-1) \equiv \\ &\equiv -(a_{k-1} + a_{k-3} + \ldots a_3 + a_1) \pmod{11}. \end{aligned}$$

Ora $11|n$ se e solo se $n_0 + n_1 = n \equiv 0 \pmod{11}$, e questo, per quanto provato sopra, è a sua volta equivalente a

$$(a_k + a_{k-2} + \ldots a_2 + a_0) - (a_{k-1} + a_{k-3} + \ldots a_3 + a_1) \equiv 0 \pmod{11}$$

ovvero a

$$(a_k + a_{k-2} + \ldots a_2 + a_0) \equiv (a_{k-1} + a_{k-3} + \ldots a_3 + a_1) \pmod{11}$$

provando così il criterio annunciato.

Il Teorema 6.2.2 consente di valutare anche la congruenza di potenze. Infatti, siano $n \geq 1$ il modulo, $a \in \mathbb{Z}$ e $1 \leq k \in \mathbb{N}$. Allora, se $a \equiv r \pmod{n}$, si ha $a^k \equiv r^k \pmod{n}$. Ad esempio, poiché $2^5 \equiv 1 \pmod{31}$, si deduce che

$$2^{62} = 2^{5\cdot 12+2} = (2^5)^{12}2^2 \equiv 4 \pmod{31}.$$

Teorema 6.2.3. (Fermat). *Sia p un numero primo positivo, e sia $a \in \mathbb{Z}$ un intero non divisibile per p. Allora*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dimostrazione. Sia p un numero primo positivo, e sia $S = \{1, 2, \ldots, p-1\}$. Sia a un intero non divisibile per p, e per ogni $k \in S$ denotiamo con a_k il resto della divisione di $a \cdot k$ per p. Osserviamo che, poiché p è un primo e non divide né a né k, p non divide $a \cdot k$, e dunque $a_k \in S$; inoltre $a_k \equiv a \cdot k \pmod{p}$. Consideriamo l'applicazione $\Phi : S \longrightarrow S$ che ad ogni $k \in S$ associa a_k. Tale applicazione è iniettiva: infatti se, per $k, t \in S$, si ha $a_k = a_t$ allora $a \cdot k \equiv a \cdot t \pmod{p}$, ovvero p divide $a \cdot k - a \cdot t = a(k-t)$ e, siccome p non divide a, segue che p divide $k - t$ che, per la definizione di S, implica $k = t$. Dunque Φ è iniettiva; essendo S un insieme finito, ne segue che Φ è una biezione. Quindi

$$a_1 \cdot a_2 \cdot a_3 \ldots a_{p-1} = 1 \cdot 2 \cdot 3 \ldots (p-1) = (p-1)!$$

Pertanto

$$a^{p-1}(p-1)! = (a\cdot 1)(a\cdot 2)\ldots(a\cdot(p-1)) \equiv a_1 \cdot a_2 \cdot a_3 \ldots a_{p-1} \equiv (p-1)! \pmod{p},$$

cioè, p divide

$$a^{p-1}(p-1)! - (p-1)! = (a^{p-1}-1)(p-1)!$$

Poiché p è primo, esso non divide $(p-1)!$ e dunque deve dividere $a^{p-1}-1$, il che prova l'asserto del Teorema. ∎

Del Teorema di Fermat esistono diverse dimostrazioni; una seconda è basata sul seguente risultato di interesse indipendende.

Proposizione 6.2.4. *Sia p un primo positivo, e siano $a, b \in \mathbb{Z}$. Allora*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Dimostrazione. Sia p un primo positivo, e sia $1 \leq k \leq p-1$; allora p non divide $1 \cdot 2 \cdot 3 \cdot (k-1) \cdot k = k!$, e quindi

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!}$$

è un multiplo di p. Pertanto, applicando lo sviluppo del binomio di Newton (vedi, più avanti, il Teorema 4.2.6) ed il Teorema 6.2.2, si ha

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \ldots + \binom{p}{p-1}ab^{p-1} + b^p \equiv a^p + b^p \pmod{p}$$

completando la dimostrazione. ∎

A questo punto si provi per esercizio che, fissato un primo positivo p, per ogni intero a si ha $a^p \equiv a \pmod{p}$ (si osservi che si può assumere $a \in \mathbb{N}$, quindi si ragioni per induzione, usando la Proposizione 6.2.4). Da ciò segue che $a(a^{p-1}-1) \equiv 0 \pmod{p}$. Se p non divide a si conclude allora che p divide $a^{p-1}-1$, provando così il Teorema di Fermat.

Come complemento a questo paragrafo, vediamo in una serie di esercizi alcuni aspetti della teoria delle equazioni con congruenze. La lettera x va quindi intesa come una indeterminata, n, n_1, n_2 sono fissati numeri naturali diversi da 0.

Esercizio 1. Siano $a, b \in \mathbb{Z}$, e sia $c \in \mathbb{Z}$ una soluzione della congruenza $ax \equiv b \pmod{n}$. Si provi che ogni elemento della classe di congruenza di c modulo n è una soluzione della stessa congruenza.

Esercizio 2. Siano $a, b \in \mathbb{Z}$. Si provi che la congruenza $ax \equiv b \pmod{n}$ ammette soluzioni intere se e solo se (a, n) divide b.

Soluzione. Poniamo $d = (a, n)$. Supponiamo $d|b$. Allora esiste $c \in \mathbb{Z}$ tale che $b = dc$. Per il Teorema 3.3.1 esistono $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta n$. Quindi $b = \alpha ac + \beta nc$, cioè $ac\alpha = b - n\beta c$ e dunque $c\alpha$ è una soluzione della congruenza data.
Viceversa, supponiamo che esista una soluzione $c \in \mathbb{Z}$ della congruenza, cioè $ac \equiv b \pmod{n}$. Allora esiste $\alpha \in \mathbb{Z}$ tale che $b - ac = n\alpha$ da cui segue $b = ac + n\alpha$ e quindi $d|b$ (perchè $d|a$ e $d|n$).

Esercizio 3. (*Teorema Cinese dei resti*) Siano $n_1, n_2 \geq 1$ tali che $(n_1, n_2) = 1$. Si provi che per ogni coppia a, b di numeri interi il sistema di congruenze

$$\begin{cases} x \equiv a \pmod{n_1} \\ x \equiv b \pmod{n_2} \end{cases}$$

ammette soluzioni.

Soluzione. Per il Teorema 3.3.1 esistono $\alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha n_1 + \beta n_2$. Allora

$$a\beta n_2 = a - a\alpha n_1 \equiv a \pmod{n_1}$$

e

$$b\alpha n_1 = b - b\beta n_2 \equiv b \pmod{n_2}.$$

Quindi $c = a\beta n_2 + b\alpha n_1$ è una soluzione del sistema.

Si rifletta a come Il Teorema Cinese dei resti possa essere esteso in modo naturale a sistemi di tre o più congruenze.

6.3 Esercizi.

Esercizio 6.1. Si trovino le soluzioni intere dell'equazione $3xy + 7x = 15$.

Esercizio 6.2. Si risolva l'equazione diofantea

$$6x + 10y + 15z = 3.$$

Esercizio 6.3. Sia $2 \leq n \in \mathbb{N}$. Si provi che l'equazione $x^n = 2y^n$ non ha soluzioni nell'insieme dei numeri interi non nulli.

Esercizio 6.4. Si risolva l'equazione diofantea $x^2 - y^2 = 17$.

Esercizio 6.5. Si provi che l'equazione diofantea $x^2 - xy + y^2 = 0$ non ha soluzioni intere non banali.

Esercizio 6.6. Si determini la classe di congruenza modulo 7 del numero

$$19 + 24(11 - 12^7) - 1984(3^9 + 5151) + 344.$$

Esercizio 6.7. Si dimostri che, per ogni numero naturale n si ha $10^n \equiv 1 \pmod 9$.

Esercizio 6.8. Utilizzando l'esercizio precedente si provi che ogni numero intero è congruo modulo 9 alla somma delle cifre della sua rappresentazione decimale. Dedurre il noto criterio di divisibilità per 3: un numero intero è divisibile per 3 se e solo se la somma delle sue cifre decimali è divisibile per 3.

Esercizio 6.9. Siano $a, b \in \mathbb{Z}$, e $1 \leq n, m \in \mathbb{N}$. Si provi che

1) Se $a \equiv b \pmod n$, allora $(a, n) = (b, n)$.
2) Se $a \equiv b \pmod n$, e $a \equiv b \pmod m$, allora $a \equiv b \pmod{[n, m]}$.

Esercizio 6.10. Sia $4, n \in \mathbb{N}$. Si provi che se n non è primo allora $(n-1)! \equiv 0 \pmod n$.

Esercizio 6.11. Si risolvano le seguenti congruenze,

$$2x \equiv 5 \pmod 9, \qquad 15x \equiv 3 \pmod 6, \qquad x^2 \equiv 5 \pmod 6.$$

Esercizio 6.12. Si determini il sottoinsieme S dei numeri naturali x tali che:

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 3 \pmod 5 \end{cases}$$

Esercizio 6.13. Si dica per quali interi x si ha $x^3 \equiv 1 \pmod 5$.

Capitolo 7

Altri esercizi

Esercizio 7.1. Siano a, b numeri interi, con $b \geq 1$. Si provi che esistono unici interi t, s tali che $a = bt + s$ e $-\frac{b}{2} < s \leq \frac{b}{2}$.

Esercizio 7.2. Si dimostri che per ogni numero naturale $n \geq 1$ vale la formula

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n+1)(2n-1)}{3}.$$

Esercizio 7.3. Si dimostri, per induzione su n, che per ogni $n \geq 1$:

$$\sum_{i=1}^{n} (-1)^i i^2 = (-1)^n \frac{n(n+1)}{2}.$$

Esercizio 7.4. Procedendo per induzione su n, si dimostri che, per ogni $n \geq 2$ si ha:

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n} \ .$$

Esercizio 7.5. Sia $f : \mathbb{N} \longrightarrow \mathbb{N}$. Diciamo che f è strettamente crescente se f è iniettiva e per ogni $i \in \mathbb{N}$ si ha $f(i) \leq f(i+1)$.

(a) Procedendo per induzione su $k = n - m$, si dimostri che se f è strettamente crescente allora per ogni $n, m \in \mathbb{N}$ con $n \geq m$ si ha $f(n) \geq f(m) + k$.

(b) Siano $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ strettamente crescenti. Si dimostri che $f = g$ se e solo se $f(\mathbb{N}) = g(\mathbb{N})$.

Esercizio 7.6. Procedendo per induzione su n, si dimostri che, per ogni $n \geq 3$,

$$\binom{3n}{2n} \geq 4^n \ .$$

Esercizio 7.7. Calcolare $(1001, 4485)$, e quindi scriverlo come combinazione a coefficienti interi dei due numeri dati.

Esercizio 7.8. Siano a, b e c interi non nulli tali che $a|b$ e $c|b$. Si provi che

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{c}.$$

In particolare, se $d = (a, b)$, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Esercizio 7.9. Siano a, b e c interi non nulli. Si provi che

1) $(ca, cb) = c(a, b)$;

2) $[ca, cb] = c[a, b]$.

Esercizio 7.10. Sia n un numero interi. Si provi che $(2n + 1, 1 - n)$ è uguale a 1 o a 3.

Esercizio 7.11. Siano n e m interi positivi tali che

$$\begin{cases} n + m = 63 \\ [n, m] = 962 \end{cases}$$

Si determinino n e m.

Esercizio 7.12. Sia $1 < n \in \mathbb{N}$. Si provi che

$$u = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

non è un numero intero.

Esercizio 7.13. La successione di *Fibonacci* è definita da:

$$u_0 = 0,\ u_1 = 1, \quad \text{e} \quad u_{n+2} = u_{n+1} + u_n$$

(i primi termini di essa sono $0, 1, 1, 2, 3, 5, 8, 13, 21, 33 \ldots$). Provare i seguenti fatti

1) se $x = (1 + \sqrt{5})/2$ e $y = (1 - \sqrt{5})/2$, allora $u_n\sqrt{5} = x^n - y^n$ (x, y sono le radici reali dell'equazione $t^2 - t - 1$)

2) $(u_n, u_{n+1}) = 1$

3) $u_{m+n} = u_{n-1}u_m + u_n u_{m+1}$

4) se $r \in \mathbb{N}^*$, u_n divide u_{nr}

5) se $(m,n)=d$, allora $(u_m,u_n)=u_d$.

Esercizio 7.14. Sia $n\in\mathbb{N}$. Si provi che n, $n+2$ e $n+4$ sono numeri primi se e solo se $n=3$.

Esercizio 7.15. Determinare l'ultima cifra decimale di 9^{139}, e quella di 7^{2001}.

Esercizio 7.16. Si determinino le soluzioni della congruenza

$$39x\equiv 5 \pmod{14}.$$

Esercizio 7.17. Si risolva il seguente sistema di congruenze:

$$\begin{cases} 4x-y\equiv 3\,(\mathrm{mod}\ 13) \\ \\ 7x+2y\equiv 5\,(\mathrm{mod}\ 13) \end{cases}$$

Esercizio 7.18. Si risolva il seguenti sistema di congruenze:

$$\begin{cases} x\equiv 3\,(\mathrm{mod}\ 6) \\ x\equiv 5\,(\mathrm{mod}\ 7) \\ x\equiv 7\,(\mathrm{mod}\ 11) \end{cases}$$

Esercizio 7.19. Si dimostri che se $x,y,z\in\mathbb{N}$ sono tali che $x^2+y^2=z^2$, allora $xyz\equiv 0 \pmod{60}$.

Esercizio 7.20. Sia $a679b$ un numero di cinque cifre (in base 10) divisibile per 72. Determinare a e b.

Soluzioni di alcuni esercizi

2.3 Per $n+1$ si ha

$$(-1)^1 1^2=(-1)^1\frac{1(1+1)}{2}$$

che è certamente vera. Assumiamo ora che l'uguaglianza sia vera per $n\geq 1$ e dimostriamola per $n+1$. Si ha (l'ipotesi induttiva è applicata al passaggio alla seconda

riga):

$$\begin{aligned}\sum_{i=1}^{n+1}(-1)^i i^2 &= \sum_{i=1}^{n}(-1)^i i^2 \ + \ (-1)^{n+1}(n+1)^2 = \\ &= (-1)^n \frac{n(n+1)}{2} + (-1)^{n+1}(n+1)^2 = \\ &= (-1)^{n+1}(n+1)(-\frac{n}{2} + (n+1)) = (-1)^{n+1}(n+1)\frac{-n+2n+2}{2} = \\ &= (-1)^{n+1}(n+1)\frac{n+2}{2} = (-1)^{n+1}\frac{(n+1)(n+2)}{2}\end{aligned}$$

per il principio di induzione l'uguaglianza è vera per ogni $n \geq 1$.

2.6 1) Per $n = 3$ si ha:

$$\binom{3\cdot 3}{2\cdot 3} = \binom{9}{6} = \frac{7\cdot 8\cdot 9}{1\cdot 2\cdot 3} = 84 \geq 64 = 4^3.$$

2) Sia la disuguaglianza vera per n cioè: $\binom{3n}{2n} \geq 4^n$. Per $n+1$ abbiamo

$$\binom{3(n+1)}{2(n+1)} = \frac{(3n+3)!}{(2n+2)!(n+1)!} = \frac{1\cdot 2\ \ldots\ 3n\cdot(3n+1)(3n+2)(3n+3)}{(1\cdot 2\ \ldots\ 2n\cdot(2n+1)(2n+2))\cdot n!(n+1)} =$$

$$= \frac{(3n)!(3n+1)(3n+2)(3n+3)}{(2n)!\cdot(2n+1)(2n+2)\cdot n!\cdot(n+1)} == \frac{(3n)!}{(2n)!n!}\cdot\frac{(3n+1)(3n+2)(3n+3)}{(2n+1)(2n+2)(n+1)} =$$

$$= \binom{3n}{2n}\cdot\frac{(3n+1)(3n+2)(3n+3)}{(2n+1)(2n+2)(n+1)}.$$

Ora $\binom{3n}{2n} \geq 4^n$ per ipotesi induttiva e, poichè $n \geq 3$:

$$\frac{(3n+1)(3n+2)(3n+3)}{(2n+1)(2n+2)(n+1)} = \frac{(3n+1)(3n+2)}{(2n+1)(2n+2)}\cdot\frac{3n+3}{n+1} = \frac{9n^2+9n+2}{4n^2+6n+2}\cdot\frac{3}{1} \geq \frac{3}{2}\cdot\frac{3}{1} = \frac{9}{2} \geq 4.$$

Quindi:

$$\binom{3(n+1)}{2(n+1)} \geq \binom{3n}{2n}\cdot 4 \geq 4^n\cdot 4 = 4^{n+1}.$$

2.7 Si trova $(4485, 1001) = 13$, e $13 = 25\cdot 4485 + (-112)\cdot 1001$.

2.13 Sia 2^k la massima potenza di 2 minore o uguale a n (cioè $2^k \leq n < 2^{k+1}$), e sia m il minimo comune multiplo tra gli tutti gli interi $1,\ 2, \ldots, n$ escluso 2^k. Allora la massima potenza di 2 che divide m è 2^{k-1}. Ora abbiamo

$$mu = m + \frac{m}{2} + \cdots + \frac{m}{n}$$

dove ogni addendo del termine di destra è un intero con l'eccezione di $\frac{m}{2^k}$. Poiché, per quanto sopra osservato, $\frac{m}{2^k}$ non è un intero, ne segue che mu non è un intero, e quindi che u non è un intero.

2.14 Osserviamo che $x = (1+\sqrt{5})/2$ e $y = (1-\sqrt{5})/2$ sono le radici reali del polinomio $t^2 - t - 1$.

1) Per induzione su $n \in \mathbb{N}$. Per $n = 0$ la cosa è banale. Se $n = 1$: $x - y = \sqrt{5} = u_1\sqrt{5}$. Supposta l'uguaglianza vera per ogni $k < n \geq 2$, abbiamo

$$u_n\sqrt{5} = u_{n-1}\sqrt{5} + u_{n-2}\sqrt{5} = x^{n-1} - y^{n-1} + x^{n-2} - y^{n-2} =$$

$$= x^{n-2}(x+1) - y^{n-2}(y+1) = x^{n-2}x^2 - y^{n-2}y^2 = x^n - y^n \ .$$

2) Per induzione su n, tenendo conto che se d divide (u_n, u_{n+1}), allora d divide $u_{n+1} - u_n = u_{n-1}$.

3) e 4) si provano anche facilmente per induzione.

5) Possiamo supporre $m > n$. Per l'algoritmo della divisione $m = nq + r$, con $0 \leq r \leq n-1$. Per il punto 3),

$$u_m = u_{nq-1}u_r + u_{nq}u_{r+1}$$

da cui deriva che $(u_m, u_n) = (u_n, u_r)$. Continuando come nell'algoritmo di Euclide, si ricava il risultato.

2.17 Si osservi che l'ultima cifra decimale di $n = 9^{139}$ è il resto della divisione di n per 10, ovvero quell'intero quell'intero $0 \leq k \leq 9$, tale che $9^{139} \equiv k\,(mod\,10)$. Ora, si osserva che $9^2 = 81 \equiv 1\,(mod\,10)$. Inoltre, $139 = 2 \cdot 69 + 1$. Quindi, applicando il teorema 6.2.2,

$$9^{139} = 9^{2\cdot 69+1} = (9^2)^{69} \cdot 9 \equiv 9 \pmod{10}.$$

Dunque $k = 9$. Similmente si ragiona per 7^{2001} tenendo conto che $7^4 \equiv 1\,(mod\,10)$.

2.20 La soluzioni sono $x = 117$ e tutti gli interi congrui ad x modulo $462 = 6 \cdot 7 \cdot 11$.

2.21 Supponiamo che il sistema dato sia risolubile, e sia x_o una sua soluzione. Allora $n|x_o - a$ e $m|x_o - b$. Quindi (n, m) divide $x_o - a - (x_o - b) = b - a$. Viceversa, supponiamo che $(n, m)|b - a$. Allora, è risolubile la congruenza $nx \equiv b - a \pmod{m}$. Sia x_1 una sua soluzione, e sia $x_2 = a + nx_1$. Allora, per scelta, $x_2 \equiv a \pmod{n}$; inoltre $x_2 - b = a + nx_1 - b = nx_1 - (b - a) \equiv 0 \pmod{m}$. Dunque x_2 è una soluzione del sistema.

Soluzioni di alcuni esercizi

1.1. 1) Vero; 2) Falso; 3) V; 4) F; 5) F; 6) F (infatti: $\{x \mid x \in \mathbb{Z}, x^2 < 1\} = \{0\}$); 7) V.

1.3. Se $A \subseteq B$, allora ogni sottoinsieme di A è sottoinsieme di B, e quindi $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Viceversa, se $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, allora, in particolare $A \in \mathcal{P}(A) \subseteq \mathcal{P}(B)$, quindi $A \in \mathcal{P}(B)$, cioè $A \subseteq B$.

1.5. Sia $(A \cup B) \cap C = A \cup (B \cap C)$; allora, in particolare, $A \subseteq A \cup (B \cap C) = (A \cup B) \cap C \subseteq C$, e dunque $A \subseteq C$. Viceversa, sia $A \subseteq C$; allora, applicaando la proprietà distributiva, si ha $(A \cup B) \cap C = (A \cap C) \cup (B \cap C) = A \cup (B \cap C)$.

1.8 Sia $a \in A \setminus (A \setminus B)$; allora $a \in A$ e $a \notin A \setminus B$. La seconda condizione implica che $A \in B$ oppure $A \notin A$; ma siccome $a \in A$, deve essere $a \in B$, e dunque $a \in A \cap B$. Quindi $A \setminus (A \setminus B) \subseteq A \cap B$. Viceversa, sia $b \in A \cap B$; allora $b \in A$ e $b \in B$, e dunque $b \notin (A \setminus B)$. Poiché $b \in A$, si ha che $b \in A \setminus (A \setminus B)$, e pertanto $A \cap B \subseteq A \setminus (A \setminus B)$. Per la doppia inclusione si conclude che $A \setminus (A \setminus B) = A \cap B$.

1.9 Osserviamo che $\{-1, 1\} = D_1$, e che, per ogni $0 < n \in \mathbb{N}$, si ha $D_1 \subseteq D_n$. Quindi, per ogni $0 < n \in \mathbb{N}$, $\mathbb{Z} \setminus D_n \subseteq \mathbb{Z} \setminus D_1 = \mathbb{Z} \setminus \{-1, 1\}$. Dunque

$$\bigcup_{0<n\in\mathbb{N}} (\mathbb{Z} \setminus D_n) \subseteq \mathbb{Z} \setminus \{-1, 1\} = \mathbb{Z} \setminus D_1 \subseteq \bigcup_{0<n\in\mathbb{N}} (\mathbb{Z} \setminus D_n)$$

da cui l'uguaglianza.

2.1 Solo la (b) è suriettiva. Le altre non lo sono.

2.2 Sono tutte iniettive.

1.15 (risposta)

$$\bigcup_{n\in\mathbb{N}_0} B_n = \mathbb{R} \setminus \{0\} \qquad \bigcap_{n\in\mathbb{N}_0} B_n = \{1, -1\} \ .$$

1.16 $\bigcup_{n\in\mathbb{N}_0} A_n = \mathbb{Q}$. Infatti, sia $x = r/s \in \mathbb{Q}$; allora $sx = r \in \mathbb{Z}$ e quindi

$$x \in A_s \subseteq \bigcup_{n\in\mathbb{N}_0} A_n.$$

$Y = \bigcap_{n\in\mathbb{N}_0} A_n = \mathbb{Z}$. Infatti, $A_1 = \mathbb{Z}$ e quindi $Y \subseteq \mathbb{Z}$. Viceversa, sia $u \in \mathbb{Z}$; allora $nu \in \mathbb{Z}$ per ogni $n \in \mathbb{N}_0$ e dunque $u \in A_n$ per ogni $n \in \mathbb{N}_0$, cioè $u \in Y$ e quindi $\mathbb{Z} \subseteq Y$.

2.10 Sia $x \in X$ e sia $y = f(x)$. Allora $x \in f^{-1}(\{y\})$ e quindi, per le ipotesi su f e g, $x \in g^{-1}(\{y\})$, che significa $y = g(x)$. Ciò vale per ogni $x \in X$ e dunque $g = f$.

2.13 (a) Sia $a \in A$; poichè f è suriettiva esiste $x \in A$ tale che $f(x) = a$, e quindi $g(a) = g(f(x)) = g \circ f(x) = f(x) = a$. Dunque $g = \iota_A$.

(b) Sia $a \in A$; allora $f(a) = f \circ g(a) = f(g(a))$; poichè f è iniettiva, si ha $g(a) = a$. Dunque $g = \iota_A$.

2.14 Supponiamo che f soddisfi le ipotesi dell'esercizio, e siano $a, b \in X$ con $a \neq b$. Posto $T = \{b\}$ si ha allora $a \in X \setminus T$ e quindi, per ipotesi, $f(a) \in f(X \setminus T) \subseteq Y \setminus f(T)$. Dunque $f(a) \notin f(T) = f(\{b\}) = \{f(b)\}$ e quindi $f(a) \neq f(b)$ provando così che f è iniettiva.

2.16. (b) $f^{-1} : D \longrightarrow \mathbb{N}$ è data da

$$f^{-1} = \begin{cases} \frac{x+1}{2} & \text{se} \quad 4 \not| x+1 \\ \frac{x-3}{2} & \text{se} \quad 4 | x+1 \end{cases}$$