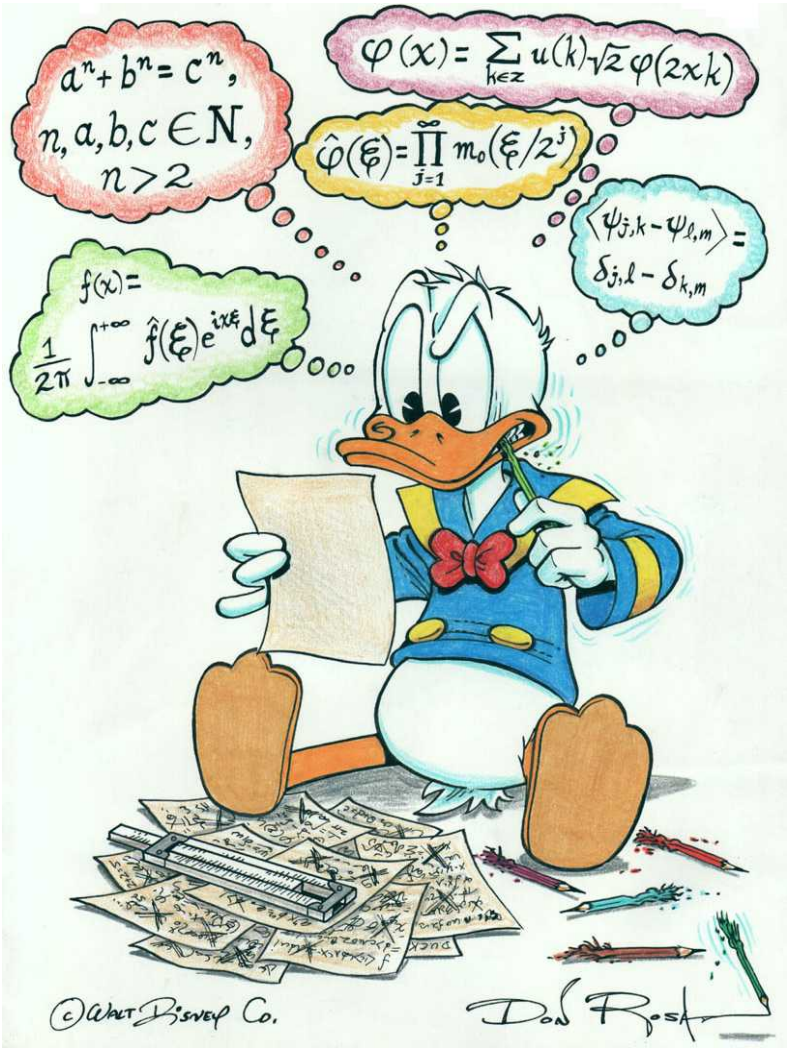
Marco Barlotti

Appunti di

Algebra

per l'insegnamento di "Matematica Discreta e Logca"
del corso di laurea triennale in Informatica

Vers. 3.3
Anno Accademico 2019-2020



In copertina un disegno originale (© Disney) di Keno Don Rosa.

PERCHE’ QUESTI APPUNTI, E COME USARLI

(Prefazione alla vers. 3.3)

Questi appunti vogliono costituire un supporto scritto alle lezioni di algebra che tengo per l’insegnamento di “Matematica discreta e Logica” per il Corso di Laurea triennale in Informatica presso l’Università di Firenze.

È una versione ormai stabile degli argomenti che svolgo a lezione, e si può considerare definitiva fatti salvi gli inevitabili aggiustamenti che fino all’ultimo possono presentarsi in quello che è per sua natura un *work in progress* sempre soggetto a verifiche sul campo.

Nell’usare questi appunti, lo studente deve tenere presente che, in quanto testo scritto, essi non sono la stessa cosa delle lezioni tenute in aula: ad esempio, la trattazione è talvolta più formale (e quindi più “pesante”) rispetto a quanto consente l’immediatezza dell’esposizione orale, dove ci si può “lasciare andare” all’uso di qualche notazione non del tutto ortodossa.

Inoltre, rispetto al programma effettivamente svolto a lezione, questi appunti comprendono alcune dimostrazioni in più ([1]) ma molti esercizi in meno (e quelli compresi non sono, in generale, risolti). Le dimostrazioni in più vogliono consentire allo studente interessato qualche approfondimento e servire come riferimento per eventuali consultazioni future. Esercizi in quantità certamente sufficiente per una buona preparazione all’esame vengono invece messi a disposizione (con la loro dettagliata risoluzione) sulla pagina *e*-learning dell’insegnamento via via che i relativi argomenti sono trattati a lezione; tali esercizi, e le loro soluzioni, non costituiscono però parte di questi appunti e quindi non possono essere consultati durante le prove di esame.

Firenze, 3.10.2019

Marco Barlotti

[1] Per la preparazione all’esame lo studente è invitato a fare riferimento al programmma consuntivo che sarà reso disponibile al termine del corso sulla pagina *e*-learning dell’insegnamento.

BIBLIOGRAFIA

[1] G. Devoto, G. C. Oli
Il dizionario della lingua italiana
Le Monnier, Firenze (1990)

[2] P. R. Halmos
Naive set theory
Van Nostrand, Princeton NJ (1966)

[3] P. R. Halmos
Teoria elementare degli insiemi
Feltrinelli, Milano (1970)

[4] G. Peano
Aritmetica generale e algebra elementare
Paravia, Torino (1902)

SOMMARIO

4. - Operazioni in un insieme

5. - Permutazioni

6. - Relazioni di ordine

7. - L'algoritmo di Euclide in $\mathbb{N}$

1.- INTRODUZIONE

1.1 - L'impostazione assiomatica.

Ogni teoria matematica si sviluppa mediante definizioni e teoremi su cui poggiano a cascata altre definizioni e altri teoremi. Ogni definizione spiega il significato di una parola, o di un gruppo di parole, mediante altre parole. Ma è possibile definire tutte le parole? O, forse, alcuni termini matematici possono essere definiti con vocaboli "non tecnici", cioè del tutto estranei alla teoria in esposizione, che quindi non hanno bisogno di spiegazione? La risposta è negativa per entrambe le domande.

Esempio 1.1.1

Si chiama *dizionario della lingua italiana* una raccolta di parole e locuzioni della lingua italiana (generalmente disposte in ordine alfabetico) per ciascuna delle quali è fornita una spiegazione del significato. Tale spiegazione è data usando soltanto parole della lingua italiana.
Nella edizione 1990 de "*Il dizionario della lingua italiana*" di Giacomo Devoto e Gian Carlo Oli ([1]) leggiamo:

UOMO := L'individuo di sesso maschile della specie umana.

UMANO := Proprio dell'uomo, in quanto rappresentante della specie.

Questo non è soddisfacente: infatti il lettore non può comprendere la spiegazione del sostantivo "UOMO" se non conosce il significato dell'aggettivo "UMANO"; e non può comprendere la spiegazione dell'aggettivo "UMANO" se non conosce il significato del sostantivo "UOMO".

Esempio 1.1.2

La più antica opera oggi conosciuta in cui la geometria viene trattata non come un sistema di regole pratiche e nozioni empiriche ma come una "scienza razionale" è costituita dagli "*Elementi*" di Euclide (matematico vissuto in Grecia nel III secolo a. C.). La teoria sviluppata da Euclide costituisce ancor oggi uno strumento semplice e efficace per descrivere la realtà fisica ([1]) attorno a noi e per studiare fenomeni di varia natura.

---

[1] almeno in prima approssimazione. Le descrizioni quantistico-relativistiche utilizzano una geometria "diversa", detta appunto "non euclidea".

Dovendo riferirsi a certi enti su cui costruire la geometria, Euclide ritenne necessario aprire la sua opera con una serie di "definizioni", ad esempio:

- Un punto è ciò che non ha parti.
- Una linea è una lunghezza senza larghezza.
- Una superficie è ciò che ha solo lunghezza e larghezza, ma non spessore.

Oggi queste "definizioni" non ci sembrano utilizzabili per sopportare il peso di una teoria. Non si comprende infatti come si possa spiegare che cos'è un "punto" mediante la nozione di "parte" senza poi precisare che cosa significhi "parte"; né come si possano definire "linea" e "superficie" mediante le parole "lunghezza", "larghezza" e "spessore" senza che queste vengano a loro volta definite.

Lo sviluppo (nel diciannovesimo secolo) della critica ai fondamenti della matematica (e in particolare della geometria euclidea) ha condotto a stabilire che una trattazione razionale e rigorosa deve procedere *assiomaticamente*: ciò significa che alla base della teoria non si deve porre un sistema di definizioni; si assegnano invece certe parole (dette *concetti primitivi*) e le regole precise (dette *assiomi*, o *postulati*) con le quali tali parole verranno utilizzate. In tal modo anziché definire gli enti fondamentali si descrivono piuttosto le relazioni logiche che intercorrono fra essi.

1.2 - La teoria degli insiemi.

La *teoria degli insiemi* può essere utilizzata per una costruzione organica e coerente di tutta la Matematica. Essa si è venuta sviluppando a partire dalla seconda metà del diciannovesimo secolo grazie ai lavori di (fra gli altri) Georg Cantor (1845 – 1918), Friedrich Ludwig Gotilds Frige (1848 – 1925) e Bertrand Russel (1872 – 1970), ed ha trovato una sistemazione ormai classica ad opera di Ernst Friedrich Ferdinand Zermelo (1871 – 1953) e Adolf Abraham Fraenkel (1891 – 1965).

Una rigorosa impostazione assiomatica (cfr. 1.1) esula certamente dalle nostre possibilità [2]. Noi utilizzeremo tuttavia il linguaggio degli insiemi; pur non formalizzandole esplicitamente, cercheremo di stabilire "regole del gioco" chiare e precise che ci consentano di utilizzare le parole "primitive" (*insieme*, *elemento*, *appartiene*, ...) senza cadere in formalismi esasperati ma evitando imprecisioni che possano poi dar luogo a contraddizioni logiche.

Useremo dunque la parola "*insieme*" per indicare un ente completamente caratterizzato dagli *elementi* che ad esso *appartengono*. Per sgombrare il campo da possibili fraintendimenti, chiariamo subito che

- si usa il termine "elemento" per indicare ciò che "appartiene" ad un "insieme", senza che ciò prefiguri due mondi distinti, quello degli "elementi" e quello degli "insiemi": anzi, gli elementi di un insieme possono benissimo essere essi stessi insiemi;
- poiché un insieme resta completamente caratterizzato dai suoi elementi, si conviene in particolare che: due insiemi sono lo stesso insieme (si dice anche che *coincidono*) se e solo se hanno gli stessi elementi.

[2] Il lettore interessato può consultare utilmente [2], se necessario nella traduzione italiana [3].

1.3 - Prime notazioni sugli insiemi.

Siano A, B insiemi.

Se a è un elemento di A (ciò si esprime anche dicendo che a *appartiene* ad A), scriveremo

$$a \in \mathrm{A}.$$

Se ogni elemento di A è anche elemento di B, diremo che A è un *sottoinsieme* di B (oppure che è *incluso*, o *contenuto* in B) e scriveremo

$$\mathrm{A} \subset \mathrm{B}\,.$$

Se $\mathrm{A} \subset \mathrm{B}$ e $\mathrm{B} \subset \mathrm{A}$, cioè se A e B hanno gli stessi elementi, A e B sono lo stesso insieme e scriveremo

$$\mathrm{A} = \mathrm{B}$$

(osserviamo qui esplicitamente che intenderemo sempre l'uguaglianza nel senso "leibniziano" di *identità*). In generale, se si deve provare che $\mathrm{A} = \mathrm{B}$, il procedimento migliore è appunto quello di mostrare che $\mathrm{A} \subset \mathrm{B}$ e $\mathrm{B} \subset \mathrm{A}$.

Le scritture

$$a \notin \mathrm{A}, \quad \mathrm{A} \not\subset \mathrm{B}, \quad \mathrm{A} \neq \mathrm{B}$$

indicano la negazione rispettivamente di

$$a \in \mathrm{A}, \quad \mathrm{A} \subset \mathrm{B} \quad \text{e} \quad \mathrm{A} = \mathrm{B}$$

(cioè significano rispettivamente: a non è un elemento di A, A non è un sottoinsieme di B, A e B non sono lo stesso insieme; quest'ultimo fatto si esprime anche dicendo che A e B sono *diversi* o *distinti*).

Se $\mathrm{A} \subset \mathrm{B}$ e $\mathrm{A} \neq \mathrm{B}$ (ciò si esprime dicendo che A è *incluso propriamente* in B, oppure che A è un *sottoinsieme proprio* di B), scriveremo anche

$$\mathrm{A} \overset{\subset}{\neq} \mathrm{B}\,.$$

Nel seguito supporremo noti dagli studi precedenti l'insieme $\mathbb{N}$ dei numeri naturali, l'insieme $\mathbb{Z}$ dei numeri interi relativi, l'insieme $\mathbb{Q}$ dei numeri razionali e l'insieme $\mathbb{R}$ dei numeri reali, con le nozioni di $\leq$ ("minore o uguale"), $<$ ("strettamente minore"), $\geq$ ("maggiore o uguale"), $>$ ("strettamente maggiore"), $+$ ("somma"), $-$ ("differenza"), $\cdot$ ("prodotto") e $:$ ("divisione") relative ai loro elementi. Indicheremo rispettivamente con $\mathbb{Z}^+$ e con $\mathbb{Z}^-$ l'insieme dei numeri interi positivi (cioè strettamente maggiori di zero) e l'insieme dei numeri interi negativi (cioè strettamente minori di zero); con $\mathbb{Q}^+$ e con $\mathbb{Q}^-$ l'insieme dei numeri razionali positivi e l'insieme dei numeri razionali negativi; con $\mathbb{R}^+$ e con $\mathbb{R}^-$ l'insieme dei numeri reali positivi e l'insieme dei numeri reali negativi. Identificheremo $\mathbb{N}$ con il sottoinsieme di $\mathbb{Z}$ formato dai numeri non negativi, così come identificheremo $\mathbb{Z}$ con un opportuno sottoinsieme di $\mathbb{Q}$ e identificheremo $\mathbb{Q}$ con un opportuno sottoinsieme di $\mathbb{R}$, cosicché potremo scrivere

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}\,.$$

Sempre dagli studi precedenti riterremo noti alcuni insiemi di natura geometrica, e in particolare certi sottoinsiemi dell'insieme dei punti del piano (rette, segmenti, circonferenze, cerchi, triangoli, ecc. ecc.).

1.4 - Come si definisce un insieme: mediante elenco degli elementi.

Accetteremo di definire un insieme indicandone tra parentesi graffe tutti gli elementi [3] separati da virgole (si ricordi che abbiamo stabilito che un insieme è completamente caratterizzato dai suoi elementi). Ad esempio, se $a_1, a_2, \ldots, a_n$ sono tutti e soli gli elementi dell'insieme A, scriveremo [4]

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

Postuliamo una volta per tutte l'esistenza di qualsiasi insieme definito secondo questa regola.

Esempi

1.4.1 **A** $= \{1, 5, 23, 49, 76\}$;

1.4.2 **B** $= \{\mathbb{N}, \mathbb{Q}, \mathbb{Z}\}$ (si osservi che $\mathbb{N} \in$ **B** ma $\mathbb{N} \notin$ **B**) ;

1.4.3 **C** $= \{5, 37, \mathbb{N}, \mathbb{Q}^+\}$;

1.4.4 **D** $= \{\mathbb{N}, \{\mathbb{N}\}\}$. Gli insiemi $\mathbb{N}$, $\{\mathbb{N}\}$, $\{\{\mathbb{N}\}\}$, $\{\{\{\mathbb{N}\}\}\}$, … sono tutti distinti fra loro.

1.5 - Coppie ordinate, n – ple ordinate, sequenze ordinate, matrici.

Sia A un insieme.

Se $a, b \in$ A, possiamo considerare (per quanto convenuto in 1.4) l'insieme $\{a, b\}$; per esso si ha sempre $\{a, b\} = \{b, a\}$ e (quando $a = b$) $\{a, a\} = \{a\}$.

Spesso è conveniente considerare anche un ente che sia caratterizzato non solo dagli elementi a e b ma anche dall'ordine in cui si considerano: tale ente si dice *coppia ordinata* [5] *con prima componente* a *e seconda componente* b, e si indica con

$$(a, b).$$

Si noti che, se a, a' $\in$ A e b, b' $\in$ B, si ha

$$(a, b) = (a', b') \qquad \text{se e solo se} \qquad a = a' \text{ e } b = b';$$

in particolare: se $a \neq b$, si ha *sempre*

$$(a, b) \neq (b, a)$$

e (quando $a = b$) la scrittura (a, a) indica ancora una coppia ordinata (e non può essere abbreviata in (a)) .

---

[3] che possono essere elementi di insiemi già definiti, oppure insiemi essi stessi.

[4] Si noti che questo modo di definire un insieme può essere utilizzato solo se tale insieme è finito (cfr. sez. 11.2).

[5] La definizione rigorosa di *coppia ordinata* è la seguente: $(a, b) := \{\{a\}, \{a, b\}\}$.

Più in generale, se $a_1, a_2, \ldots, a_n \in$ A (con $n \in \mathbb{N}\backslash\{0\}$), si dice $n-$*pla ordinata con* $i-$*sima componente* a_i e si indica con

$$(a_1, a_2, \ldots, a_n)$$

un ente caratterizzato non solo dagli elementi $a_1, a_2, \ldots, a_n$ ma anche dall'ordine in cui si considerano.

L'insieme di tutte le coppie ordinate di elementi di A si indica con A^2. Analogamente, l'insieme di tutte le $n-$ple ordinate di elementi di A (per un fissato $n \in \mathbb{N}\backslash\{0\}$) si indica con A^n.

Si dice *sequenza ordinata* di elementi di A una $n-$pla ordinata di elementi di A per qualche $n \in \mathbb{N}$ (che si dice *lunghezza* della sequenza); nella scrittura di una sequenza si omettono le parentesi esterne (e talvolta, se ciò non dà luogo ad ambiguità, anche le virgole).

Se σ è una sequenza ordinata di elementi di A, si dice *sottosequenza* di σ qualunque sequenza ordinata ottenuta prendendo alcuni elementi di σ (eventualmente anche tutti) nello stesso ordine in cui compaiono in σ.

Siano infine m, n numeri interi positivi.

Si dice *matrice* $m \times n$ *a elementi in* A una m-pla ordinata di n-ple ordinate di elementi di A .

Una matrice $m \times n$ potrebbe essere identificata con una mn-pla ordinata; in pratica, quando si parla di matrice gli elementi vengono scritti in una "tabella"

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{pmatrix}$$

nella quale si evidenziano le n-ple ordinate

$(a_{1,1}, a_{1,2}, \ldots, a_{1,n})$,
$(a_{2,1}, a_{2,2}, \ldots, a_{2,n})$,
$\ldots$,
$(a_{m,1}, a_{m,2}, \ldots, a_{m,n})$

dette *righe* della matrice, e le m-ple ordinate

$(a_{1,1}, a_{2,1}, \ldots, a_{m,1})$,
$(a_{1,2}, a_{2,2}, \ldots, a_{m,2})$,
$\ldots$,
$(a_{1,n}, a_{2,n}, \ldots, a_{m,n})$

dette *colonne* della matrice.

Sinteticamente, la matrice di termine generico $a_{i,j}$ si indica con $(a_{i,j})$; le sue righe si indicano con $a_{1,*}, a_{2,*}, \ldots, a_{m,*}$ e le sue colonne con $a_{*,1}, a_{*,2}, \ldots, a_{*,n}$.

L'insieme di tutte le matrici $m \times n$ a elementi in A si indica con $A^{m,n}$.

1.6 - Enunciati. Predicati.

Sia A un insieme. Si dice *enunciato* (*su* A) una frase che (interpretata con riferimento ad A) risulta vera oppure falsa.

Esempi

1.6.1 "$2 < 3$" è un enunciato (vero) su $\mathbb{N}$ (e su $\mathbb{Z}$, e su $\mathbb{R}$; ma non è un enunciato sull'insieme dei punti del piano);

1.6.2 "ci sono almeno 7 elementi" è un enunciato su qualunque insieme (e risulta vero o falso a seconda dell'insieme su cui lo si considera);

1.6.3 "ogni elemento è incidente con almeno una retta" è un enunciato (vero) sull'insieme dei punti del piano (e sull'insieme dei punti dello spazio; ma non è un enunciato su $\mathbb{N}$ o su $\mathbb{Z}$ o su $\mathbb{R}$);

1.6.4 "ambarabà ciccì coccò" non è un enunciato.

Siano A, X insiemi. Si dice *predicato* (o anche *proposizione aperta*) (*in* A) *con variabile libera* x *su* X una scrittura P(x) con la proprietà che

per ogni $x_0 \in$ X, la scrittura P(x_0) ottenuta sostituendo ([6]) ovunque x_0 a x in P(x) risulta un enunciato (su A).

Esempi

1.6.5 Sia A un insieme qualsiasi, e sia X $:= \mathbb{N}$; un predicato in A con variabile libera x su X è P(x) := "in A ci sono almeno x elementi";

1.6.6 Sia A l'insieme dei punti del piano, e sia X $:= \mathbb{N}$; un predicato in A con variabile libera x su X è P(x) := "comunque presi x elementi in A, c'è almeno una retta incidente ad essi";

1.6.7 Sia A = X $:= \mathbb{N}$; un predicato con variabile libera n su $\mathbb{N}$ è P(n) := "n è dispari";

1.6.8 Sia A = X $:= \mathbb{R}$; un predicato con variabile libera x su $\mathbb{R}$ è P(x) := "esiste un polinomio in una indeterminata a coefficienti interi che ha x come radice";

[6] nel senso definito in [1]: "mettere una cosa al posto di un'altra".

1.7 - Come si definisce un insieme: mediante una proprietà caratteristica.

Sia X un insieme. Accetteremo di definire un sottoinsieme A di X specificando una proprietà che ne caratterizza gli elementi fra tutti gli elementi di X. Precisamente, sia P(x) un predicato (in X) con variabile libera x su X (cosicché per ogni $x_0 \in$ X si ha che P(x_0) è vera oppure è falsa). Scriveremo

$$\mathrm{A} = \{x \in \mathrm{X} \,/\, \mathrm{P}(x)\}$$

(si legge: A è l'insieme degli x appartenenti a X tali che P(x))

per indicare il sottoinsieme di X formato da tutti e soli gli elementi x_0 per i quali P(x_0) è vera. Come vedremo (cfr. teorema 1.7.3), è essenziale che A sia "immerso" in un insieme X già definito.

Postuliamo una volta per tutte l'esistenza di qualsiasi insieme definito secondo questa regola.

Esempio 1.7.1

L'insieme dei numeri naturali il cui quadrato non supera 200 può essere indicato scrivendo

$$\{x \in \mathbb{N} \,/\, x^2 \leq 200\}.$$

Teorema 1.7.2

Esiste un (unico) insieme che non ha elementi; esso si dice *insieme vuoto* e si indica con $\emptyset$. Per ogni insieme I, si ha $\emptyset \subset \mathrm{I}$.

Dimostrazione – Sia A un qualunque insieme; allora l'insieme

$$\emptyset := \{x \in \mathrm{A} \,/\, x \neq x\}$$

esiste (perché è definito come convenuto sopra) e non ha elementi (perché $x \neq x$ è falso qualunque sia x).

Sia ora I un insieme: dobbiamo provare che $\emptyset \subset \mathrm{I}$, cioè che ogni elemento di $\emptyset$ appartiene a I. Se ciò fosse falso ci sarebbe in $\emptyset$ un elemento, chiamiamolo x_0, che non appartiene a I: in particolare ci sarebbe in $\emptyset$ almeno un elemento, e ciò è assurdo perché $\emptyset$ non ha elementi!

Ricordiamo infine che abbiamo convenuto che ogni un insieme è completamente caratterizzato dai suoi elementi: pertanto esiste un unico insieme privo di elementi (anche se può essere definito come sopra a partire da insiemi A diversi).

Un insieme distinto da $\emptyset$ sarà detto *non vuoto*.

Teorema 1.7.3

Non esiste un "insieme di tutti gli insiemi", cioè: non esiste un insieme di cui ogni insieme sia elemento.

Dimostrazione – Sia per assurdo U l'insieme di tutti gli insiemi, e si consideri

$$A = \{X \in U \,/\, X \notin X\}.$$

Se fosse $A \in A$, per definizione di A sarebbe $A \notin A$, e ciò è assurdo. Allora $A \notin A$; ma poiché $A \in U$ ne segue $A \in A$, ancora assurdo. Se si accetta il postulato di esistenza degli insiemi definiti come in 1.7 (e se si accetta il principio aristotelico del "terzo escluso"), bisogna dunque negare l'esistenza dell'insieme U.

Lo stesso ragionamento, dovuto a B. Russel (1872 – 1970), spiega perché nella definizione di A mediante una proprietà caratteristica abbiamo dovuto chiedere che A fosse sottoinsieme di un insieme X.

Esercizio 1.7.4

Fissato un insieme B, si consideri $A = \{X \in B \,/\, X \notin X\}$. Perché non c'è contraddizione? Può essere $A \in A$? Può essere $A \notin A$? Può essere $A \in B$?

1.8 - Come si definisce un insieme: come unione di insiemi già definiti.

Sia $\mathcal{I}$ un insieme di insiemi. Qualunque sia $\mathcal{I}$, postuliamo che esista un insieme i cui elementi sono tutti e soli gli elementi degli insiemi che appartengono a $\mathcal{I}$.

Tale insieme si indica con $\cup\mathcal{I}$ e si dice *unione* degli insiemi che appartengono a $\mathcal{I}$: ci torneremo sopra in 1.10.

1.9 - Come si definisce un insieme: come insieme delle parti.

Sia A un insieme. Qualunque sia A, postuliamo che esista un insieme i cui elementi sono tutti e soli i sottoinsiemi di A.

Tale insieme si indica con $\mathcal{P}(A)$ e si dice *insieme delle parti di* A. Si osservi che, per ogni insieme A, a $\mathcal{P}(A)$ appartengono $\emptyset$ e A.

Esempio 1.9.1

Sia A $= \{1,2,3\}$. Allora

$$\mathcal{P}(\mathrm{A}) = \{\ \mathrm{A},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1\},\ \{2\},\ \{3\},\ \emptyset\}.$$

Esempio 1.9.2

Sia A $= \emptyset$. Allora

$$\mathcal{P}(\mathrm{A}) = \{\emptyset\}.$$

Esempio 1.9.3

Sia A $= \{a, b, x, y, z\}$. Allora

$$\mathcal{P}(\mathrm{A}) = \{\mathrm{A}, \{a,b,x,y\}, \{a,b,x,z\}, \{a,b,y,z\}, \{a,x,y,z\}, \{b,x,y,z\}, \{x,y,z\}, \{b,y,z\},$$
$$\{b,x,z\}, \{b,x,y\}, \{a,y,z\}, \{a,x,z\}, \{a,x,y\}, \{a,b,z\}, \{a,b,y\}, \{a,b,x\}, \{a,b\}, \{a,x\},$$
$$\{a,y\}, \{a,z\}, \{b,x\}, \{b,y\}, \{b,z\}, \{x,y\}, \{x,z\}, \{y,z\}, \{a\}, \{b\}, \{x\}, \{y\}, \{z\}, \emptyset\}.$$

1.10 - Unione, intersezione, differenza.

Siano A, B insiemi.

Si dice *unione* di A e B, e si indica con

$$\mathrm{A} \cup \mathrm{B},$$

l'insieme i cui elementi sono tutti e soli gli elementi di A e gli elementi di B. Con la notazione introdotta in 1.8: $\mathrm{A} \cup \mathrm{B} = \cup\{\mathrm{A}, \mathrm{B}\}$.

Si dice *intersezione* di A e B, e si indica con $\mathrm{A} \cap \mathrm{B}$, l'insieme degli elementi di A che appartengono anche a B. Con la notazione introdotta in 1.7: $\mathrm{A} \cap \mathrm{B} = \{x \in \mathrm{A} \,/\, x \in \mathrm{B}\}$.

Se $\mathrm{A} \cap \mathrm{B} = \emptyset$, A e B si dicono *disgiunti*.

Si dice *differenza* di A e B, e si indica con $\mathrm{A}\backslash\mathrm{B}$, l'insieme degli elementi di A che non appartengono a B. Con la notazione introdotta in 1.7: $\mathrm{A}\backslash\mathrm{B} = \{x \in \mathrm{A} \,/\, x \notin \mathrm{B}\}$.

Se $\mathrm{B} \subset \mathrm{A}$, l'insieme $\mathrm{A}\backslash\mathrm{B}$ viene detto anche *complementare* di B in A, ed è indicato (purché tale notazione non dia luogo ad equivoci) con B^c.

Esempio 1.10.1

Siano $A = \{1, 2, 3\}$, $B = \{2, 4, 6, 8\}$. Allora $A \cup B = \{1, 2, 3, 4, 6, 8\}$, $A \cap B = \{2\}$ e $A \setminus B = \{1, 3\}$.

Esempio 1.10.2

Siano A l'insieme dei triangoli e B l'insieme dei rettangoli (entrambi sottoinsiemi del piano euclideo). Allora $A \cap B = \emptyset$.

Esercizi

Siano A, B, C sottoinsiemi dell'insieme I. Si dimostrino le seguenti uguaglianze:

1.10.3 $A \cap B = B \cap A$;

1.10.4 $(A \cap B) \cap C = A \cap (B \cap C)$;

1.10.5 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

1.10.6 $A \cap (A \cup B) = A$;

1.10.7 $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$;

1.10.8 $(A \cap B)^c = A^c \cup B^c$.

Valgono le uguaglianze che si ottengono dalle precedenti scambiando $\cap$ con $\cup$?

Esercizi

Siano X, Y, Z sottoinsiemi dell'insieme I. Si dimostrino le seguenti uguaglianze:

1.10.9 $X \cap Y^c = X \setminus Y$;

1.10.10 $X \setminus (X \setminus Y) = X \cap Y$;

1.10.11 $X \cap (Y \setminus Z) = (X \cap Y) \setminus (X \cap Z)$.

Valgono le uguaglianza che si ottengono dalle precedenti scambiando $\cap$ con $\cup$?

1.11 - Unione e intersezione di una famiglia di insiemi. Partizioni.

Un insieme di insiemi si dice anche *una famiglia* di insiemi. Abbiamo definito in 1.8 l'*unione* di una famiglia di insiemi; in modo analogo si definisce l'*intersezione* di una famiglia *non vuota* di insiemi (l'esistenza dell'insieme intersezione è garantita dal fatto che esso si può definire secondo la regola fissata in 1.7 come l'insieme degli elementi di un insieme della famiglia che appartengono anche a tutti gli altri insiemi della famiglia).

Sia A un insieme. Una famiglia di sottoinsiemi non vuoti di A si dice una *partizione* di A se tali sottoinsiemi sono a due a due disgiunti e la loro unione è A.

Esempio 1.11.1

Un fascio di rette parallele è una partizione del piano.

1.12 - Prodotto cartesiano.

Siano A, B insiemi.

L'insieme di tutte le coppie ordinate (a, b) con $a \in$ A e $b \in$ B si dice *prodotto cartesiano* [7] di A per B e si indica con A $\times$ B.

Esempio 1.12.1

Sia A $= \{1, 2, 3\}$ e B $= \{0, 1\}$. Si ha A $\times$ B $= \{(1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}$.

[7] Tenendo conto della definizione rigorosa di "coppia ordinata" (nota 5), il lettore attento potrà osservare che $\mathbf{A} \times \mathbf{B}$ è un sottoinsieme di $\mathcal{P}(\mathcal{P}(\mathbf{A} \cup \mathbf{B}))$, e quindi può essere definito come in 1.7; ciò ne garantisce l'esistenza.

2.- IL PRINCIPIO DI INDUZIONE

2.1 - Gli assiomi di Peano per i numeri naturali.

Anche se, come si è detto, noi diamo per conosciuto dagli studi della Scuola Secondaria (se non addirittura della Scuola Primaria) l'insieme $\mathbb{N}$ dei numeri naturali [8], vale la pena di accennare alla sua bella e semplice costruzione assiomatica proposta dal matematico italiano Giuseppe Peano (1858 – 1932).

Riportiamo, con qualche irrilevante aggiornamento nei termini [9], la formulazione di [4]; la prima esposizione del sistema di assiomi è in un lavoro scientifico pubblicato nel 1891. I concetti primitivi sono indicati con la locuzione "*numero naturale*" e le parole "*zero*", "*successivo*", "*insieme*" e "*appartiene*". Gli assiomi sono i seguenti:

(P1) – Zero è un numero naturale.

(P2) – Ogni numero naturale ha un successivo, che è anch'esso un numero naturale.

(P3) – Sia **A** un insieme di numeri naturali. Supponiamo che zero appartenga ad **A** e che per ogni numero naturale che appartiene ad **A** anche il suo successivo appartenga ad **A**; allora ogni numero naturale appartiene ad **A**.

(P4) – Se due numeri naturali hanno lo stesso successivo, essi sono lo stesso numero.

(P5) – Zero non è il successivo di alcun numero naturale.

Questi concetti primitivi e questi assiomi sono sufficienti per definire tutte le usuali nozioni relative ai numeri naturali e per dimostrarne le proprietà. Ad esempio, si può definire il numero "uno" come il successivo di zero; il numero "due" come il successivo di "uno"; il risultato della somma $m + n$ come il successivo del successivo del successivo... (n volte) di m; il risultato del prodotto $m \cdot n$ come il risultato della somma di n numeri tutti uguali a m; ecc. ecc..

Noi, come si è detto, faremo invece riferimento ai numeri naturali come abbiamo imparato a conoscerli nella scuola dell'obbligo: interpretando il concetto di "successivo" come "ciò che si ottiene sommando uno" (cosicché il successivo del numero naturale n è il numero naturale $n + 1$), il contenuto degli assiomi di Peano risulterà allora banale conseguenza di fatti ben noti.

---

[8] assieme alle nozioni di somma, differenza, prodotto, elevamento a potenza, "minore o uguale" e alle relative proprietà.

[9] ad esempio, Peano scrive "classe" anziché "insieme", e scrive "numero" *tout-court* anziché "numero naturale".

2.2 - Dimostrazioni per induzione: il teorema fondamentale.

L'assioma (P3) è detto anche *principio di induzione*. Esso fornisce il sostegno teorico a un'importante tecnica di dimostrazione, detta appunto *dimostrazione per induzione*, sulla quale adesso ci soffermeremo.

Teorema 2.2.1

Sia X un insieme, e sia **P**(n) un predicato in X con variabile libera n su $\mathbb{N}$. Se

– **P**(0) è vero in X

e per ogni $n \in \mathbb{N}$

– se **P**(n) è vero in X allora anche **P**($n+1$) è vero in X

allora **P**(n) è vero in X per ogni $n \in \mathbb{N}$.

Dimostrazione – Sia $A = \{n \in \mathbb{N} \,/\, \mathbf{P}(n) \text{ è vero in X}\}$.

Le ipotesi del teorema ci dicono che 0 appartiene ad A e che per ogni numero naturale che appartiene ad A anche il suo successivo (cioè $n+1$) appartiene ad A.

Ma allora, per il "principio di induzione" (cioè per il postulato (P3) di Peano) A coincide con $\mathbb{N}$, e dunque in X l'enunciato **P**(n) è vero per ogni $n \in \mathbb{N}$, come si voleva dimostrare.

Il teorema 2.2.1 fornisce un'utilissima strategia per dimostrare teoremi il cui enunciato dipende da un numero naturale n. Se (in un certo ambiente) si deve provare che

P(n) è vero in $\mathbb{N}$ per ogni $n \in \mathbb{N}$

per una dato predicato **P**(n) con variabile libera n su $\mathbb{N}$, si può procedere come segue:

(i) si verifica che sia vero **P**(0);

(ii) supposto vero **P**(n) (ciò si esprime dicendo che si usa **P**(n) come *ipotesi di induzione*), si dimostra che è vero **P**($n+1$).

Ciò fatto, il teorema 2.2.1 garantisce che **P**(n) è vero in $\mathbb{N}$ per ogni $n \in \mathbb{N}$.

Esempio 2.2.2

Dimostriamo per induzione su n che

per ogni numero naturale n, esiste $k_n \in \mathbb{N}$ tale che $\quad n^3 + 2n = 3k_n$ ([10]).

Dimostrazione – Il predicato è vero per $n = 0$ (scegliendo $k := 0$): infatti

$$0^3 + 2 \cdot 0 = 0 = 3 \cdot 0 .$$

Adesso supponiamo che (ipotesi di induzione) esista k_n tale che

$$n^3 + 2n = 3k_n$$

e dimostriamo che esiste k_{n+1} tale che

$$(n+1)^3 + 2(n+1) = 3k_{n+1} .$$

In effetti,

$$\begin{aligned}(n+1)^3 + 2(n+1) &= (n^3 + 3n^2 + 3n + 1) + (2n + 2) = \\ &= (n^3 + 2n) + 3(n^2 + n + 1) = 3k_n + 3(n^2 + n + 1) = \\ &= 3(k_n + n^2 + n + 1)\end{aligned}$$

che è quanto si voleva dimostrare (con $k_{n+1} := k_n + n^2 + n + 1$).

Esempio 2.2.3

Dimostriamo per induzione su n che

per ogni numero naturale n, $\quad 9^{n+1} + 2^{6n+1} \quad$ è multiplo di 11

(ossia, esiste un numero naturale k tale che $\quad 9^{n+1} + 2^{6n+1} = 11k$).

Dimostrazione – Il predicato è vero per $n = 0$: infatti

$$9^{0+1} + 2^{6\cdot 0+1} = 9^1 + 2^1 = 9 + 2 = 11 = 11 \cdot 1 .$$

Adesso supponiamo che (ipotesi di induzione) esista un numero naturale k_0 tale che $9^{n+1} + 2^{6n+1} = 11k_0$ e dimostriamo che per un opportuno numero naturale k si ha

$$9^{(n+1)+1} + 2^{6(n+1)+1} = 11k .$$

In effetti,

$$9^{(n+1)+1} + 2^{6(n+1)+1} = 9^{n+2} + 2^{6n+7} = 9 \cdot 9^{n+1} + 2^6 \cdot 2^{6n+1} = 9 \cdot \left(11k_0 - 2^{6n+1}\right) + 2^6 \cdot 2^{6n+1} =$$

$$= 99k_0 - 9 \cdot 2^{6n+1} + 2^6 \cdot 2^{6n+1} = 99k_0 + 2^{6n+1}(2^6 - 9) = 99k_0 + 55 \cdot 2^{6n+1} = 11 \cdot \left(9k_0 + 5 \cdot 2^{6n+1}\right)$$

come si voleva ($k := 9k_0 + 5 \cdot 2^{6n+1}$).

[10] Esprimeremo questo fatto con l'espressione "3 divide $n^3 + 2n$"; cfr. es. 6.2.2 e oss. 6.2.4 .

Esercizio 2.2.4

Si dimostri, per induzione su n, che

per ogni numero naturale n, esiste $k_n \in \mathbb{N}$ tale che $\quad n^5 - n = 5k_n$.

Esempio 2.2.5

Sia x un numero reale maggiore di -1. Dimostriamo per induzione su n che

per ogni numero naturale n, $\quad (1+x)^n \geq 1 + nx$.

Dimostrazione – Il predicato è vero per $n = 0$: infatti

$$(1+x)^0 = 1 = 1 + 0 \cdot x\,.$$

Adesso supponiamo che (ipotesi di induzione) sia $(1+x)^n \geq 1 + nx$, e dimostriamo che

$$(1+x)^{n+1} \geq 1 + (n+1)x\,.$$

In effetti, poiché

$$x > -1$$

è

$$x + 1 > 0$$

e quindi dall'ipotesi di induzione (moltiplicando ambo i membri per $x+1$) segue che

$$(1+x)^n \cdot (1+x) \geq (1+nx)(1+x) = 1 + x + nx + nx^2 \geq 1 + x + nx = 1 + (n+1)x\,.$$

2.3 - Dimostrazioni per induzione: partire da $n_0 > 0$.

Talvolta ci si trova a considerare un predicato $\mathbf{P}(n)$ con variabile libera n su $\mathbb{N}$ che non ha senso per valori "piccoli" di n (tipicamente: valutare una somma di n addendi; che senso può infatti avere una somma di 0 addendi, o anche di un solo addendo?) o che è vero solo per $n \geq n_0$ (per un certo $n_0 \in \mathbb{N}$, $n_0 > 0$) mentre per $n = 0$ e per altri valori di n minori di n_0 risulta falso (cfr. esempio 2.3.6).

In questi casi si può applicare ugualmente il principio di induzione. Per maggiore chiarezza, riformuliamo opportunamente il teorema 2.2.1.

Teorema 2.3.1

Sia X un insieme, e sia **P**(n) un predicato in X con variabile libera n su $\mathbb{N}$. Se

– **P**(n_0) è vero in X

e per ogni $n \in \mathbb{N}$ con $n \geq n_0$

– se **P**(n) è vero in X allora anche **P**($n+1$) è vero in X

allora **P**(n) è vero in X per ogni numero naturale $n \geq n_0$.

Dimostrazione – Sia $\quad A = \{n \in \mathbb{N} \,/\, \mathbf{P}(n+n_0) \text{ è vero in X}\}$.

Le ipotesi del teorema ci dicono che 0 appartiene ad A e che per ogni numero naturale che appartiene ad A anche il suo successivo (cioè $n+1$) appartiene ad A.

Ma allora, per il "principio di induzione" (cioè per il postulato (P3) di Peano) A coincide con $\mathbb{N}$, e dunque **P**($n+n_0$) è vero in X per ogni $n \in \mathbb{N}$; in altre parole, **P**(n) è vero in X per ogni numero naturale n maggiore o uguale a n_0, come si voleva dimostrare.

Applicando il teorema 2.3.1, se (in un certo ambiente) si deve provare che il predicato **P**(n) con variabile libera n su $\mathbb{N}$ diventa un enunciato vero sostituendo a n un qualsiasi numero naturale maggiore o uguale a un fissato n_0, si può procedere come segue:

(i) si verifica che sia vero **P**(n_0);

(ii) supposto vero **P**(n) (ciò ancora una volta si esprime dicendo che si usa **P**(n) come *ipotesi di induzione*), si dimostra che è vero **P**($n+1$); in questa fase è lecito utilizzare (come ipotesi aggiuntiva) il fatto che $n \geq n_0$.

Esempio 2.3.2

Dimostriamo per induzione su n che la somma dei numeri naturali non superiori a n è

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

Dimostrazione – L'asserto ha senso se $n \geq 2$; pertanto procediamo per induzione partendo dal valore iniziale $n_0 := 2$. Si ha

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

dunque per $n := 2$ l'asserto è vero. Supponiamo ora (*ipotesi di induzione*) che sia

$$0+1+2+\ldots+n = \frac{n(n+1)}{2}$$

e dimostriamo che $\quad 0+1+2+\ldots+n+(n+1) = \frac{(n+1)(n+2)}{2}$.

In effetti,

$$0+1+2+\ldots+n+(n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\,.$$

Esempio 2.3.3

Dimostriamo per induzione su n che la somma dei quadrati dei numeri naturali non superiori a n è

$$\frac{n(n+1)(2n+1)}{6}.$$

Dimostrazione – L'asserto ha senso se $n \geq 2$; pertanto procediamo per induzione partendo dal valore iniziale $n_0 := 2$. Si ha

$$1^2 + 2^2 = 5 = \frac{2(2+1)(2\cdot 2+1)}{6}$$

dunque per $n := 2$ l'asserto è vero. Supponiamo ora (*ipotesi di induzione*) che sia

$$0^2 + 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

e dimostriamo che

$$0^2 + 1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

In effetti,

$$0^2 + 1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$= \frac{n(n+1)(2n+1)+6(n+1)^2}{6} = \frac{(n+1)(2n^2+n+6n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}.$$

Esercizio 2.3.4

Si dimostri che la somma dei cubi dei numeri naturali non superiori a n è $\frac{n^2(n+1)^2}{4}$.

Esercizio 2.3.5

Si dimostri che la somma dei primi n numeri dispari è n^2.

Esempio 2.3.6

Dimostriamo per induzione su n che

$$n^3 < 2^n \qquad \text{se } n \geq 10.$$

Dimostrazione – Notiamo che per $n < 10$ può invece essere $n^3 > 2^n$; ad esempio, $9^3 = 729 > 512 = 2^9$.

Procediamo per induzione partendo dal valore iniziale $n_0 := 10$. Si ha

$$10^3 = 1\,000 < 1\,024 = 2^{10}$$

dunque per $n := 10$ l'asserto è vero.

Supponiamo ora (*ipotesi di induzione*) che sia

$$n^3 < 2^n$$

e dimostriamo che

$$(n+1)^3 < 2^{n+1}$$

In effetti,

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1 < n^3 + 3n^2 + 3n^2 + n^2 = n^3 + 7n^2$$

e ricordando che $7 < 10 \leq n$

$$n^3 + 7n^2 \leq n^3 + n \cdot n^2 = n^3 + n^3 = 2n^3 .$$

D'altro lato, per l'ipotesi di induzione, $2n^3 < 2 \cdot 2^n = 2^{n+1}$ e quindi

$$(n+1)^3 < n^3 + 10n^2 \leq 2n^3 < 2^{n+1}$$

come si voleva dimostrare.

2.4 - Il simbolo di "sommatoria".

Sia $n \in \mathbb{N}$.

Nelle dimostrazioni sviluppate all'interno degli esempi 2.3.2 e 2.3.3, abbiamo indicato la somma dei numeri naturali non superiori a n con

$$0 + 1 + 2 + \ldots + n$$

e la somma dei loro quadrati con

$$0^2 + 1^2 + 2^2 + \ldots + n^2 .$$

Benché tali scritture siano sufficientemente espressive e risultino comprensibili senza ambiguità, in matematica (ma anche nelle altre scienze) di regola si preferisce evitare l'uso dei "puntini di sospensione" e si adotta una diversa notazione, che adesso introduciamo.

Se $(a_1, a_2, a_3, \ldots, a_n)$ è una $n-$pla ordinata di numeri reali, la somma dei suoi elementi si indica con la scrittura

$$\sum_{k=1}^{n} a_k$$

che si legge "somma degli a_k per k che va da 1 a n".

Il simbolo "$\sum$" si dice *simbolo di sommatoria*, la lettera k si dice *indice della sommatoria*. È importante capire che con questa scrittura la lettera k viene "dedicata" alla somma così indicata e quindi: da un lato, k non può venire ad assumere altri significati nel contesto in cui compare come indice di sommatoria; dall'altro, come indice di sommatoria si può di fatto usare, anziché k, qualsiasi lettera di qualsiasi alfabeto (o addirittura qualsiasi simbolo, anche se usualmente è preferibile evitare scelte estreme).

Esempio 2.4.1

Le scritture

$$\sum_{k=1}^{n} a_k, \quad \sum_{i=1}^{n} a_i, \quad \sum_{\beta=1}^{n} a_\beta \quad \text{e} \quad \sum_{*=1}^{n} a_*$$

indicano tutte la stessa somma.

Esempio 2.4.2

Le scritture

$$k + \sum_{k=1}^{n} a_k, \quad \left(\sum_{k=1}^{n} a_k\right)^k, \quad \text{e} \quad k \cdot \left(\sum_{k=1}^{n} a_k\right)$$

sono da evitare: come indice di sommatoria va utilizzata una lettera diversa da k.

Esempio 2.4.3

Utilizzando il simbolo di sommatoria, la somma dei numeri naturali non superiori a n si indica con la scrittura $\sum_{k=1}^{n} k$ e la somma dei loro quadrati con $\sum_{k=1}^{n} k^2$.

La notazione col simbolo di "sommatoria" si può utilizzare anche per somme parziali fra gli elementi di una assegnata $n-$pla ordinata $(a_1, a_2, a_3, \ldots, a_n)$ di numeri reali: ad esempio, con la scrittura $\sum_{k=k_0}^{k_1} a_k$ si indica la somma degli elementi il cui indice è compreso fra k_0 (incluso) e k_1 (incluso); con la scrittura $\sum_{\substack{k \text{ dispari} \\ k \leq n}} a_k$ si indica la somma degli elementi il cui indice è dispari e non superiore a n.

Esempio 2.4.4

Dimostriamo per induzione su n che $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

Dimostrazione – L'asserto ha senso se $n \geq 1$; pertanto procediamo per induzione partendo dal valore iniziale $n_0 := 1$. Si ha $2^0 + 2^1 = 1 + 2 = 3 = 2^{1+1} - 1$, dunque per $n := 1$ l'asserto è vero.

Supponiamo ora (*ipotesi di induzione*) che sia $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$ e dimostriamo che

$$\sum_{k=0}^{n+1} 2^k = 2^{n+2} - 1\,.$$

In effetti, $\sum_{k=0}^{n+1} 2^k = \sum_{k=0}^{n} 2^k + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1\,.$

In modo del tutto analogo si introduce un simbolo $\prod_{k=1}^{n} a_k$ (che si legge "prodotto degli a_k per k che va da 1 a n") per indicare il prodotto fra tutti gli elementi di una assegnata $n-$pla ordinata $(a_1, a_2, a_3, \ldots, a_n)$ di numeri reali, o anche (con le opportune modifiche di scrittura) fra alcuni di essi.

Valgono per il simbolo $\prod$ e per la lettera k le stesse considerazioni svolte sopra per la sommatoria: non si parla però di (agh!) "produttoria", ma semplicemente di "prodotto".

2.5 - Dimostrazioni per induzione: altre formulazioni.

Riportiamo in questa sezione altre strategie di dimostrazione basate sul principio di induzione che ci saranno utili più avanti.

Teorema 2.5.1

Sia X un insieme, e sia **P**(n) un predicato in X con variabile libera n su $\mathbb{N}$. Se

– **P**(0) e **P**(1) sono veri in X

e per ogni $n \in \mathbb{N}$

– se **P**(n) e **P**$(n+1)$ sono entrambi veri in X allora anche **P**$(n+2)$ è vero in X

allora **P**(n) è vero in X per ogni $n \in \mathbb{N}$.

Dimostrazione – Sia A $= \{n \in \mathbb{N}$ / **P**(n) e **P**$(n+1)\}$.

Le ipotesi del teorema ci dicono che $0 \in$ A e che per ogni numero naturale n che appartiene ad A anche il suo successivo (cioè $n+1$) appartiene ad A.

Ma allora, per il "principio di induzione" (cioè per il postulato (P3) di Peano) A coincide con $\mathbb{N}$, e in particolare **P**(n) è vera per ogni $n \in \mathbb{N}$, come si voleva dimostrare.

Siano $k_0, k \in \mathbb{N}$. Poniamo

$$\mathrm{J}_{k_0}^{k} := \{n \in \mathbb{N} \,/\, k_0 \leq n < k\}$$

cosicché, ad esempio: $\mathrm{J}_h^k = \emptyset$ tutte le volte che $k \leq h$, $\mathrm{J}_0^1 = \{0\}$, $\mathrm{J}_3^4 := \{3\}$, $\mathrm{J}_3^7 := \{3,4,5,6\}$.

Teorema 2.5.2

Siano X un insieme, **P**(n) un predicato in X con variabile libera n su $\mathbb{N}$ e $k_0 \in \mathbb{N}$. Se per ogni numero naturale $\overline{n} \in \mathbb{N} \setminus \mathrm{J}_0^{k_0}$ si ha che

se per ogni $k \in \mathrm{J}_{k_0}^{\overline{n}}$ **P**(k) è vero in X allora anche **P**$(\overline{n})$ è vero in X

allora **P**(n) è vero in X per ogni numero naturale $n \geq k_0$.

Dimostrazione – Sia

$$\mathrm{A} = \{n \in \mathbb{N} \,/\, \textbf{P}(k_0 + k) \text{ è vero in X per ogni } k \leq n\}.$$

Dimostriamo che $\mathrm{A} = \mathbb{N}$ (da cui l'asserto) applicando il "principio di induzione" (cioè il postulato (P3) di Peano).

Mostriamo in primo luogo che $0 \in \mathrm{A}$. A tale scopo dobbiamo soltanto provare che è vero **P**(k_0). Osserviamo che $\mathrm{J}_{k_0}^{k_0} = \emptyset$, quindi **P**$(k)$ è certamente vero in X per ogni $k \in \mathrm{J}_{k_0}^{k_0}$; l'ipotesi del teorema per $\overline{n} := k_0$ ci dice che **P**(k_0) deve essere vero, ossia che $0 \in \mathrm{A}$.

Ora supponiamo che sia $n \in \mathrm{A}$. Per definizione di A, deve essere vero **P**$(k_0 + k)$ per ogni $k \leq n$, cioè per ogni $k \in \mathrm{J}_{k_0}^{n+1}$; dall'ipotesi del teorema segue che anche **P**$(n+1)$ deve essere vera, ossia che $n + 1 \in \mathrm{A}$, come si voleva dimostrare.

Osservazione 2.5.3

A una prima, superficiale, lettura può sembrare che l'ipotesi del teorema 2.5.2 differisca da quelle dei teoremi 2.2.1, 2.3.1 e 2.5.1 in un punto chiave: il "passo iniziale", quello in cui si chiede che sia vero **P**(0) (nel teorema 2.2.1) o che sia vero **P**(n_0) (nel teorema 2.3.1) o che siano veri **P**(0) e **P**(1) (nel teorema 2.5.1).
In realtà, il "passo iniziale", cioè la verifica che sia vero l'enunciato **P**(k_0), è presente anche nell'ipotesi del teorema 2.5.2. Si chiede infatti che valga l'implicazione

se per ogni $k \in \mathrm{J}_{k_0}^{\overline{n}}$ **P**(k) è vero in X allora anche **P**$(\overline{n})$ è vero in X

per ogni $\overline{n} \in \mathbb{N} \setminus \mathrm{J}_0^{k_0}$. Ma si valuti tale implicazione per $\overline{n} := k_0$: poiché $\mathrm{J}_{k_0}^{k_0}$ è l'insieme vuoto, è certamente vera la premessa (cioè **P**(k) è vero in X per ogni $k \in \mathrm{J}_{k_0}^{k_0}$); dunque, affinché l'implicazione stessa risulti vera, si deve dimostrare che è vero **P**(k_0) (senza disporre, per questo valore di n, di alcuna "ipotesi di induzione", visto che la verità di $(\forall k \in \mathrm{J}_{k_0}^{k_0})$**P**$(k)$ non ci fornisce alcuna informazione).

Esempio 2.5.4

Dimostriamo che per ogni $n \in \mathbb{N}$ si ha

$$\sum_{k=1}^{n}(-1)^{k-1}\tfrac{1}{k} \geq 0\,.$$

Dimostrazione – L'asserto ha senso se $n \geq 2$; pertanto procediamo per induzione partendo dal valore iniziale $n_0 := 2$. Si ha

$$\sum_{k=1}^{n}(-1)^{k-1}\tfrac{1}{k} = (-1)^0\tfrac{1}{1} + (-1)^1\tfrac{1}{2} = 1 - \tfrac{1}{2} = \tfrac{1}{2} \geq 0\,.$$

dunque per $n := 2$ l'asserto è vero.

Supponiamo ora (*ipotesi di induzione*) che sia

$$\sum_{k=1}^{m}(-1)^{k-1}\tfrac{1}{k} \geq 0 \qquad \text{per ogni } m \in \mathbb{N} \text{ tale che } \; 2 \leq m < n$$

e dimostriamo che

$$\sum_{k=1}^{m}(-1)^{k-1}\tfrac{1}{k} \geq 0\,.$$

Se n è dispari, utilizzando l'ipotesi di induzione per $m := n-1$, si trova che

$$\sum_{k=1}^{n}(-1)^{k-1}\tfrac{1}{k} = \sum_{k=1}^{n-1}(-1)^{k-1}\tfrac{1}{k} + (-1)^{n-1}\tfrac{1}{n} \geq 0$$

perché è la somma di due addendi non negativi: il primo non è negativo per l'ipotesi di induzione, il secondo non è negativo perché $n-1$ è pari.

Se n è pari, utilizzando l'ipotesi di induzione per $m := n-2$, si trova che

$$\sum_{k=1}^{n}(-1)^{k-1}\tfrac{1}{k} = \sum_{k=1}^{n-2}(-1)^{k-1}\tfrac{1}{k} + \big((-1)^{n-2}\tfrac{1}{n-1} + (-1)^{n-1}\tfrac{1}{n}\big) \geq 0$$

perché è la somma di due addendi non negativi: il primo non è negativo per l'ipotesi di induzuone, il secondo non è negativo perché (essendo n è pari) vale

$$\tfrac{1}{n-1} - \tfrac{1}{n} = \tfrac{n-(n-1)}{n(n-1)} = \tfrac{n-n+1}{n(n-1)} = \tfrac{1}{n(n-1)} > 0\,.$$

3.- FUNZIONI

3.1 - Relazioni.

Siano A, B insiemi.

Si dice *relazione* tra A e B un sottoinsieme del prodotto cartesiano A $\times$ B.

Sia ϱ una relazione tra A e B, cioè sia $\varrho \subset$ A $\times$ B; se $(a, b) \in \varrho$, si dice che gli elementi a (di A) e b (di B) *sono in relazione*, e si scrive $a\varrho b$. In pratica si usa sempre la notazione $a\varrho b$ anziché $(a, b) \in \varrho$.

Intuitivamente, una relazione tra A e B è una "legge" che a ogni elemento di A associa qualche elemento di B (eventualmente nessuno).

Esempio 3.1.1

Siano

$$\mathrm{A} := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101\};$$
$$\mathrm{B} := \{n \in \mathbb{N} / \ 1 \leq n \leq 100\}.$$

Si ponga per $p \in$ A e $n \in$ B

$$p\varrho n \quad \text{se e solo se} \quad \text{esiste } q \in \mathbb{N} \text{ tale che } n = pq \quad (^{11}).$$

Si è così definita una relazione ϱ tra A e B; si noti che alcuni elementi di A sono in relazione con un solo elemento di B (è quanto accade considerando $p := 53, 59, \ldots, 97$), altri ($p := 37, 41, 43, 47$) con due, altri ($p := 29, 31$) con tre, ecc.. L'elemento 2 di A è in relazione con 50 elementi di B; l'elemento 101 di A non è in relazione con alcun elemento di B. Inoltre: più elementi di A possono essere in relazione con gli stessi elementi di B (2, 3, 5 sono tutti in relazione con 30, 60 e 90).

Esempio 3.1.2

Sia A un insieme, e si ponga per $a \in$ A e X $\subseteq$ A

$$a\varrho \mathrm{X} \quad \text{se e solo se} \quad a \in \mathrm{X}.$$

Si è così definita una relazione ϱ tra A e $\mathcal{P}$(A).

---

[11] Esprimeremo questo fatto con l'espressione "p divide n"; cfr. esempio 6.2.2 e osservazione 6.2.4 .

Esempio 3.1.3

Sia A un insieme, e si ponga per $X, Y \subseteq A$

$$X \varrho Y \quad \text{se e solo se} \quad X \subset Y .$$

Si è così definita una relazione ϱ tra $\mathcal{P}(A)$ e $\mathcal{P}(A)$ (detta."inclusione").

Esempio 3.1.4

Per $m, n \in \mathbb{N}$ si ponga

$$m \leq n \quad \text{se e solo se esiste } d \in \mathbb{N} \text{ tale che} \quad n = m + d .$$

Si è così definita una relazione $\leq$ tra $\mathbb{N}$ e $\mathbb{N}$ (detta."minore o uguale").

3.2 - Relazione inversa.

Siano A, B insiemi e sia ϱ una relazione tra A e B. Si dice *relazione inversa* di ϱ la relazione ϱ^{-1} tra B e A così definita:

$$b \varrho^{-1} a \quad \text{se e soltanto se} \quad a \varrho b.$$

Esempio 3.2.1

La relazione inversa della relazione "minore o uguale" tra $\mathbb{N}$ e $\mathbb{N}$ definita in 3.1.4 si dice "maggiore o uguale" e si indica con il simbolo $\geq$. Per definizione,

$$n \geq m \quad \text{se e solo se} \quad m \leq n .$$

3.3 - Restrizione a un sottoinsieme.

Siano A, B insiemi e sia ϱ una relazione tra A e B. Se $A_1 \subset A$, si dice *restrizione* di ϱ ad A_1 la relazione $\varrho|_{A_1}$ tra A_1 e B così definita:

$$\varrho|_{A_1} := \varrho \cap (A_1 \times B)$$

(si ricordi che ϱ è un sottoinsieme di $A \times B$).

Questa definizione è molto "tecnica", perché l'unica differenza tra ϱ e $\varrho|_{A_1}$ è che quest'ultima "coinvolge" solo gli elementi di A_1); certe proprietà possono però essere verificate da $\varrho|_{A_1}$ e non da ϱ, e viceversa.

3.4 - Funzioni.

Siano A, B insiemi.

Una relazione **f** tra A e B si dice una *funzione* (o *applicazione*) da A in B se per ogni $a \in$ A esiste esattamente un $b \in$ B tale che $a\,\mathbf{f}\,b$, cioè se ogni elemento di A è in relazione (secondo **f**) con esattamente un elemento di B. Ciò si esprime scrivendo

$$\mathbf{f}: \mathrm{A} \to \mathrm{B}.$$

Intuitivamente, una funzione da A in B è una "legge" che a ogni elemento di A associa uno e un solo elemento di B .

Esempio 3.4.1

Sia A l'insieme $\mathbb{Q}^+$dei numeri razionali positivi, e sia B l'insieme $\mathbb{N}$ dei numeri naturali. La "legge" che al numero razionale $\frac{m}{n}$ associa il numero naturale $m+n$ non è una funzione $\mathbb{Q}^+ \to \mathbb{N}$ (si dice anche, impropriamente, che non è ben definita come funzione). Infatti, ad esempio, al numero razionale $\frac{2}{3}$ (che si può scrivere anche $\frac{4}{6}$, $\frac{6}{9}$, $\frac{8}{12}$, ecc.) vengono associati non solo il numero naturale $5\ (=2+3)$ ma anche i numeri naturali $10\ (=4+6)$, $15\ (=6+9)$, $20\ (=8+12)$, ecc.. La legge considerata fornisce invece un esempio significativo di relazione tra $\mathbb{Q}$ e $\mathbb{N}$; oppure individua una funzione dall'insieme delle frazioni in $\mathbb{N}$.

3.5 - Dominio. Immagine, immagine inversa.

Sia **f** una funzione da A in B .

L'insieme A si dice *dominio* di **f**, e si indica con $\mathcal{D}$(**f**).

Per ogni $a \in \mathcal{D}$(**f**), l'(unico) elemento b di B tale che $a\,\mathbf{f}\,b$ si indica con $\mathbf{f}(a)$; si dice che b *proviene* da a (o anche che b è l'*immagine* di a) mediante **f**. Si scrive sempre

$$\mathbf{f}(a) = b$$

anziché $a\,\mathbf{f}\,b$.

Se $\mathrm{A}_1 \subset$ A, si dice *immagine* di A_1 (mediante **f**) il sottoinsieme $\mathbf{f}(\mathrm{A}_1)$ di B formato dalle immagini (mediante **f**) degli elementi di A_1; con la notazione di 1.7,

$$\mathbf{f}(\mathrm{A}_1) = \{b \in \mathrm{B} \,/\, b = \mathbf{f}(a) \text{ per qualche } a \in \mathrm{A}_1\}.$$

L'immagine $\mathbf{f}(\mathrm{A})$ di A si dice anche *immagine di* **f**.

Se $\mathrm{B}_1 \subset$ B, si dice *immagine inversa* di B_1 (mediante **f**) il sottoinsieme $\mathbf{f}^{-1}(\mathrm{B}_1)$ di A formato dagli elementi le cui immagini (mediante **f**) appartengono a $\mathbf{B}_1$; con la notazione di 1.7,

$$\mathbf{f}^{-1}(\mathrm{B}_1) = \{a \in \mathrm{A} \,/\, \mathbf{f}(a) \in \mathrm{B}_1\}.$$

Sia B = A, cioè sia **f** una funzione da A in A . Un elemento a di A si dice un *punto fisso* per **f** se $\mathbf{f}(a) = a$.

Esempio 3.5.1

Sia $\mathbf{f}: \mathbb{N} \to \mathbb{N}$ la funzione che a ogni numero naturale n associa il suo doppio.
Ciò si indica con l'espressione $\mathbf{f}(n) := 2n$.
Si ha che:

(i) l'immagine di **f** è l'insieme dei numeri pari ;

(ii) posto $A_1 := \{5, 7, 10\}$, si ha $\mathbf{f}(A_1) = \{10, 14, 20\}$;

(iii) posto $B_1 := \{10, 11, 12, 13, 14, 15\}$, si ha $\mathbf{f}^{-1}(B_1) = \{5, 6, 7\}$;

(iv) 0 è l'unico punto fisso di **f** .

Esercizi

Sia **f**:A $\to$ B, e siano A_1, $A_2 \subset A$. Si dimostri che:

3.5.2 $(A_1 \subset A_2) \Rightarrow (\mathbf{f}(A_1) \subset \mathbf{f}(A_2))$;

3.5.3 $\mathbf{f}(A_1 \cup A_2) = \mathbf{f}(A_1) \cup \mathbf{f}(A_2)$;

3.5.4 $\mathbf{f}(A_1 \cap A_2) \subset \mathbf{f}(A_1) \cap \mathbf{f}(A_2)$.

Si mostri inoltre con un esempio che può essere $\mathbf{f}(A_1 \cap A_2) \subsetneq \mathbf{f}(A_1) \cap \mathbf{f}(A_2)$.

3.6 - Iniettività e suriettività.

Siano A, B insiemi, e sia **f**:A $\to$ B.

Se per ogni $b \in$ B esiste almeno un $a \in$ A tale che $\mathbf{f}(a) = b$ (cioè se ogni elemento di B proviene mediante **f** da almeno un elemento di A; ossia se $\mathbf{f}(A) = B$), **f** si dice *suriettiva*. In tal caso, si dice che **f** è una funzione da A su B.

Se comunque presi a, a' $\in$ A con $a \neq a'$ è $\mathbf{f}(a) \neq \mathbf{f}(a')$ (ossia se comunque presi a, a' $\in$ A da $\mathbf{f}(a) = \mathbf{f}(a')$ segue a = a'; cioè se ogni elemento di B proviene da al più un elemento di A), **f** si dice *iniettiva*.

Se **f** è iniettiva e suriettiva si dice che **f** è *biiettiva* (o anche che **f** è una *biiezione*, oppure che **f** è una *corrispondenza biunivoca* tra A e B). Una funzione iniettiva è sempre una corrispondenza biunivoca tra il suo dominio e la sua immagine.

Esempi

3.6.1 La funzione $\mathbb{N} \to \mathbb{N}$ che ad ogni numero associa il suo triplo è iniettiva ma non suriettiva: $\mathbf{f}(\mathbb{N})$ è l'insieme dei numeri naturali multipli di 3.

3.6.2 La funzione $\mathbf{f}: \mathbb{N} \to \mathbb{N}$ definita da

$$\mathbf{f}(n) := \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ \\ \frac{3n+1}{2} & \text{se } n \text{ è dispari} \end{cases}$$

è suriettiva ma non iniettiva.

3.6.3 La funzione $\mathbf{f}: \mathbb{N} \to \mathbb{N}$ definita da

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

è biiettiva (e dunque è una corrispondenza biunivoca tra $\mathbb{N}$ e $\mathbb{N}$).

3.6.4 Per ogni insieme A, la funzione $\mathbf{id}_{\mathrm{A}}: \mathrm{A} \to \mathrm{A}$ che ad ogni elemento associa se stesso è una corrispondenza biunivoca detta *funzione identica* o anche *identità* di **A**. Ogni elemento di A è un punto fisso per $\mathbf{id}_{\mathrm{A}}$.

3.7 - La funzione inversa.

Siano A, B insiemi, e sia $\mathbf{f}: \mathrm{A} \to \mathrm{B}$ una funzione. In generale, l'inversa di **f** (nel senso di 3.2) non è una funzione, perché il generico $b \in \mathrm{B}$ potrebbe non essere immagine di alcun elemento di A (cfr. $b := 4$ nell'esempio 3.6.1) oppure potrebbe essere immagine di più di un elemento di A (cfr. $b := 5$ nell'esempio 3.6.2).

Siano A, B insiemi, e sia $\mathbf{f}: \mathrm{A} \to \mathrm{B}$ iniettiva. Per ogni $b \in \mathbf{f}(\mathrm{A})$, $\mathbf{f}^{-1}(\{b\})$ non è vuoto (per definizione di $\mathbf{f}(\mathrm{A})$) ed è formato da al più un elemento (perché per ipotesi **f** è iniettiva), quindi è formato da esattamente un elemento; dunque la relazione inversa di **f** (nel senso di 3.2) è una funzione $\mathbf{f}(\mathrm{A}) \to \mathrm{A}$ che si dice *funzione inversa* della **f** e si indica con $\mathbf{f}^{-1}$.

In altri termini, $\mathbf{f}^{-1}$ si definisce ponendo, per ogni $b \in \mathbf{f}(\mathrm{A})$,

$$\mathbf{f}^{-1}(b) := \text{l'unico elemento di } \mathbf{f}^{-1}(\{b\})$$

(il significato del simbolo $\mathbf{f}^{-1}$ nell'espressione a destra è quello fissato in 3.5).

È facile vedere che $\mathbf{f}^{-1}$ è una corrispondenza biunivoca tra l'immagine di **f** e A; ne segue che, in particolare, l'inversa di una corrispondenza biunivoca $A \to B$ è una corrispondenza biunivoca $B \to A$.

Esempio 3.7.1

Sia $\mathbf{f}: \mathbb{Q}\backslash\{-\frac{5}{3}\} \to \mathbb{Q}$ definita da $\mathbf{f}(x) := \frac{1}{3x+5}$.

È facile verificare che **f** è iniettiva (non è invece suriettiva: $0 \notin \mathbf{f}(\mathbb{Q})$). La funzione inversa si può esprimere scrivendo $\mathbf{f}^{-1}(x) := \frac{1-5x}{3x}$ e si ha $\mathcal{D}(\mathbf{f}^{-1}) = \mathbb{Q}\backslash\{0\}$.

3.8 - Composizione di funzioni.

Siano A, B, C insiemi, e siano $\mathbf{f}: A \to B$, $\mathbf{g}: B \to C$ funzioni.

Si dice *composizione* di **f** con **g** e si indica con $\mathbf{g} \circ \mathbf{f}$ (attenzione all'ordine in cui si scrivono **f** e **g**!) la funzione $A \to C$ definita ponendo

$$(\mathbf{g} \circ \mathbf{f})(a) := \mathbf{g}(\mathbf{f}(a)) \qquad \forall a \in A.$$

Esempi

3.8.1 Sia $\mathbf{f}: \mathbb{N} \to \mathbb{Q}$ definita da $\mathbf{f}(n) := \frac{1}{n+1}$, e sia $\mathbf{g}: \mathbb{Q} \to \mathbb{Q}$ definita da $\mathbf{g}(x) := x + 2$. Si ha

$$(\mathbf{g} \circ \mathbf{f})(n) := \frac{2n+3}{n+1}.$$

3.8.2 Sia $\mathbf{f}: \mathbb{N} \to \mathbb{N}$ definita da $\mathbf{f}(n) := n^2$, e sia $\mathbf{g}: \mathbb{N} \to \mathbb{N}$ definita da $\mathbf{g}(x) := x + 1$. Si ha

$$(\mathbf{g} \circ \mathbf{f})(n) := n^2 + 1, \qquad (\mathbf{f} \circ \mathbf{g})(n) := n^2 + 2n + 1.$$

Teorema 3.8.3

Siano A, B insiemi, e sia $\mathbf{f}: \mathrm{A} \to \mathrm{B}$ iniettiva. Sia $\mathbf{f}^{-1}: \mathbf{f}(\mathrm{A}) \to \mathrm{A}$ la funzione inversa di **f** definita in 3.7. Si ha

$$\mathbf{f}^{-1} \circ \mathbf{f} = \mathbf{id}_{\mathrm{A}} \qquad \text{e} \qquad \mathbf{f} \circ \mathbf{f}^{-1} = \mathbf{id}_{\mathbf{f}(\mathrm{A})}.$$

Dimostrazione – Sia $a \in \mathrm{A}$, e sia $\mathbf{f}(a) = b$ con $b \in \mathrm{B}$.

Allora $\mathbf{f}^{-1}(b) = a$, e dunque

$$(\mathbf{f}^{-1} \circ \mathbf{f})(a) = \mathbf{f}^{-1}(\mathbf{f}(a)) = \mathbf{f}^{-1}(b) = a = \mathbf{id}_{\mathrm{A}}(a).$$

Per l'arbitrarietà di a in A, si è così provato [12] che $\mathbf{f}^{-1} \circ \mathbf{f} = \mathbf{id}_{\mathrm{A}}$.

Sia ora $b \in \mathbf{f}(\mathrm{A})$, e sia a l'elemento di A per il quale si ha $\mathbf{f}(a) = b$. Allora $\mathbf{f}^{-1}(b) = a$, e dunque

$$(\mathbf{f} \circ \mathbf{f}^{-1})(b) = \mathbf{f}(\mathbf{f}^{-1}(b)) = \mathbf{f}(a) = b = \mathbf{id}_{\mathbf{f}(\mathrm{A})}(b)$$

cosicché l'asserto è completamente provato.

Teorema 3.8.4

Siano A, B, C, D insiemi, e siano $\mathbf{f}: \mathrm{A} \to \mathrm{B}$, $\mathbf{g}: \mathrm{B} \to \mathrm{C}$, $\mathbf{h}: \mathrm{C} \to \mathrm{D}$ funzioni. Si ha

$$(\mathbf{h} \circ \mathbf{g}) \circ \mathbf{f} = \mathbf{h} \circ (\mathbf{g} \circ \mathbf{f}).$$

Dimostrazione – Sia $a \in \mathrm{A}$. Allora

$$((\mathbf{h} \circ \mathbf{g}) \circ \mathbf{f})(a) = (\mathbf{h} \circ \mathbf{g})(\mathbf{f}(a)) = \mathbf{h}(\mathbf{g}(\mathbf{f}(a))) = \mathbf{h}((\mathbf{g} \circ \mathbf{f})(a)) = (\mathbf{h} \circ (\mathbf{g} \circ \mathbf{f}))(a)$$

e l'asserto è completamente provato.

Esercizio 3.8.5

Siano **A**, **B**, **C** insiemi, e siano $\mathbf{f}: \mathrm{A} \to \mathrm{B}$, $\mathbf{g}: \mathrm{B} \to \mathrm{C}$ funzioni biiettive. Si provi che $\mathbf{g} \circ \mathbf{f}$ è biiettiva.

---

[12] Che cosa significa per due funzioni "essere uguali"? Ricordiamo le definizioni date in 3.1 e 3.4: una "funzione" è un particolare insieme di coppie ordinate. Poiché (cfr. 1.3) due insiemi "sono uguali" (cioè coincidono) se e solo se hanno gli stessi elementi, due funzioni -in particolare- sono uguali se e solo se sono costituite dalle stesse coppie ordinate, ossia "operano allo stesso modo" su ogni elemento dell'insieme di partenza.

È importante avere ben chiaro che questa non è una definizione *ad hoc* di uguaglianza tra funzioni, ma solo un modo "specialistico" di esprimere la nozione di uguaglianza tra insiemi.

3.9 - Successioni definite per recursione.

Sia A un insieme.

Una funzione $\mathbf{s}:\mathbb{N}\to \mathrm{A}$ si dice *successione in* A; quando non sorgono ambiguità, l'immagine $\mathbf{s}(n)$ del generico numero naturale n si indica con a_n e si dice $n-$*simo termine della successione*, mentre la successione **s** si indica con la scrittura (a_n).

Il principio di induzione fornisce alcune strategie molto importanti per definire successioni in un insieme qualsiasi. Non ci soffermeremo sulle dimostrazioni dei teoremi che saranno enunciati in questa sezione, ma cercheremo di presentarne qualche applicazione significativa.

Teorema 3.9.1

Sia A un insieme. Sia $\alpha\in \mathrm{A}$, e sia $\mathbf{w}:\mathbb{N}\times \mathrm{A}\to \mathrm{A}$ una funzione. Esiste una e una sola successione (a_n) in A tale che

– $a_0=\alpha$;

– $a_{n+1}=\mathbf{w}(n,a_n)$.

Dimostrazione – Omettiamo la dimostrazione di questo teorema.

Esempio 3.9.2

Per il teorema 3.9.1 (con $\mathbf{w}(n,a):=\sqrt{1+a}$) esiste (ed è unica) la successione (a_n) in $\mathbb{R}^+$ tale che

– $a_0=0$;

– $a_{n+1}=\sqrt{1+a_n}$.

L'$n-$simo termine di tale successione è

$$a_n:=\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{\dots}}}}$$

convenendo che in tale espressione il numero 1 compare esattamente n volte.

Esercizio 3.9.3

Si dimostri che nella successione dell'esempio 3.9.2 tutti i termini (tranne i primi due) sono irrazionali.

Esempio 3.9.4

Sia $\alpha \in \mathbb{R}$. Per il teorema 3.9.1 (con $\mathbf{w}(n, a) \coloneqq \alpha a$), esiste (ed è unica) la successione (a_n) in $\mathbb{R}$ tale che

– $a_0 = 1$;

– $a_{n+1} = \alpha \cdot a_n$.

Se $\alpha \neq 0$, l'$n-$simo termine di tale successione si indica con α^n e si dice *potenza di base* α *ed esponente* n.

Esempio 3.9.5

Per il teorema 3.9.1 (con $\mathbf{w}(n, a) \coloneqq (n+1)a$) esiste (ed è unica) la successione (a_n) in $\mathbb{N}$ tale che

– $a_0 = 1$;

– $a_{n+1} = (n+1) \cdot a_n$.

Per ogni $n \in \mathbb{N}$, il termine a_n di questa successione si dice "*fattoriale di* n" (o anche "n *fattoriale*") e si indica con la scrittura

$$n!\,.$$

Esercizio 3.9.6

Si provi che, se $n \geq 2$, $n!$ (cfr. esempio 3.9.5) è il prodotto di tutti i numeri naturali compresi fra 1 e n.

Teorema 3.9.7

Sia A un insieme. Siano $\alpha, \beta \in$ A, e sia $\mathbf{w} : \mathbb{N} \times \mathrm{A} \times \mathrm{A} \to \mathrm{A}$ una funzione. Esiste una e una sola successione (a_n) in A tale che

– $a_0 = \alpha$;

– $a_1 = \beta$;

– $a_{n+1} = \mathbf{w}(n, a_{n-1}, a_n)$.

Le successioni di cui ai teoremi 3.9.1 e 3.9.7 si dicono *definite ricorsivamente* (o anche *definite per recursione*) *dai valori iniziali e dalle condizioni* espresse negli enunciati di quei teoremi.

3.10 - Recursione lineare omogenea di primo grado sugli ultimi due termini.

Teorema 3.10.1

Siano $a_0, a_1, b, c \in \mathbb{R}$ con $(b, c) \neq (0, 0)$, e sia (a_n) la successione in $\mathbb{R}$ definita ricorsivamente dai valori iniziali a_0 e a_1 e dalla condizione

$$a_{n+1} := ba_n + ca_{n-1}\,.$$

Se l'equazione

(*) $$x^2 - bx - c = 0$$

ha due soluzioni distinte α e β, il termine generico della successione (a_n) si può esprimere come

(°) $$a_n = h\alpha^n + k\beta^n$$

dove h e k verificano il sistema

$$\begin{cases} h + k = a_0 \\ \alpha h + \beta k = a_1 \end{cases}.$$

Se invece l'equazione (*) ha una sola soluzione α, il termine generico della successione (a_n) si può esprimere come

(°°) $$a_n = (h + nk)\alpha^n$$

dove h e k verificano il sistema

$$\begin{cases} h = a_0 \\ (h + k)\alpha = a_1 \end{cases}.$$

Dimostrazione – Il teorema si prova, in entrambi i casi, per induzione su n.

Supponiamo in primo luogo che l'equazione (*) abbia due soluzioni α e β. Per esse si ha che

$$\alpha^2 = b\alpha + c \qquad \text{e} \qquad \beta^2 = b\beta + c\,.$$

Per $n := 0$ e $n := 1$, a_0 e a_1 sono espressi dalla (°) per come sono stati scelti h e k ([13]). Possiamo dunque supporre, per l'ipotesi d'induzione, che sia

$$a_n = h\alpha^n + k\beta^n \qquad \text{e} \qquad a_{n-1} = h\alpha^{n-1} + k\beta^{n-1}\,.$$

Per come è definita la successione,

$$a_{n+1} = ba_n + ca_{n-1} = b(h\alpha^n + k\beta^n) + c(h\alpha^{n-1} + k\beta^{n-1}) =$$
$$= h\alpha^{n-1}(b\alpha + c) + k\beta^{n-1}(b\beta + c) = h\alpha^{n-1}\alpha^2 + k\beta^{n-1}\beta^2 = h\alpha^{n+1} + k\beta^{n+1}$$

come si voleva dimostrare.

[13] Osserviamo che il sistema lineare dal quale cerchiamo di ricavare h e k ha esattamente una soluzione perché $\alpha - \beta \neq 0$.

Ora supponiamo che l'equazione (*) abbia una sola soluzione α; ciò significa che

$$b^2 + 4c = 0 \qquad \text{e} \quad \alpha = \tfrac{b}{2}$$

da cui $b = 2\alpha$ e infine $4\alpha^2 + 4c = 0$, ossia

$$\alpha^2 + c = 0\,.$$

Inoltre, come nel caso precedente,

$$\alpha^2 = b\alpha + c\,.$$

Per $n := 0$ e $n := 1$, a_0 e a_1 sono espressi dalla (°°) per come sono stati scelti h e k ([14]). Possiamo dunque supporre, per l'ipotesi d'induzione, che sia

$$a_n = (h + nk)\alpha^n \qquad \text{e} \qquad a_{n-1} = (h + (n-1)k)\alpha^{n-1}\,.$$

Per come è definita la successione,

$$\begin{aligned} a_{n+1} &= ba_n + ca_{n-1} = b(h+nk)\alpha^n + c(h+(n-1)k)\alpha^{n-1} = \\ &= b(h+nk)\alpha^n + c(h+nk)\alpha^{n-1} - ck\alpha^{n-1} = \\ &= (h+nk)\alpha^{n-1}(b\alpha + c) + k\alpha^{n+1} - k\alpha^{n+1} - ck\alpha^{n-1} = \\ &= (h+nk)\alpha^{n-1}\alpha^2 + k\alpha^{n+1} - k\alpha^{n-1}(\alpha^2 + c) = \\ &= (h+nk)\alpha^{n+1} + k\alpha^{n+1} = (h+(n+1)k)\alpha^{n+1} \end{aligned}$$

come si voleva dimostrare.

[14] Questa volta il sistema lineare dal quale cerchiamo di ricavare h e k ha esattamente una soluzione perché $\alpha \neq 0$ (altrimenti sarebbe $b = c = 0$ contro le ipotesi del teorema).

Esempio 3.10.2

Utilizzando il teorema 3.10.1, determiniamo il termine generico della successione (a_n) definita ricorsivamente dai valori iniziali $a_0 := 3$, $a_1 := 5$ e dalla condizione

$$a_{n+1} := a_n + 6a_{n-1}\,.$$

Si deve considerare l'equazione

$$x^2 - x - 6 = 0$$

che ha le due soluzioni distinte $\alpha = -2$ e $\beta = 3$. Il termine generico della successione (a_n) si può esprimere come

$$a_n = h(-2)^n + k3^n$$

dove h e k verificano il sistema

$$\begin{cases} h + k = 3 \\ -2h + 3k = 5 \end{cases}$$

cosicché $h = \frac{4}{5}$ e $k = \frac{11}{5}$. Dunque si ha

$$a_n = \tfrac{4}{5}(-2)^n + \tfrac{11}{5}3^n\,.$$

Esempio 3.10.3

Determiniamo il termine generico della successione (a_n) definita ricorsivamente dai valori iniziali $a_0 := 1$, $a_1 := 3$ e dalla condizione

$$a_{n+1} := 2a_n - a_{n-1}\,.$$

L'equazione

$$x^2 - 2x + 1 = 0$$

ha come unica soluzione $\alpha = 1$. Dal sistema

$$\begin{cases} h = 1 \\ h + k = 3 \end{cases}$$

si ricava che deve essere $h = 1$ e $k = 2$. Dunque il termine generico della successione (a_n) si può esprimere come $a_n = (1 + 2n)1^n$ ossia come

$$a_n = 1 + 2n\,.$$

Se avessimo cercato di applicare la formula trovata per il caso in cui l'equazione di secondo grado considerata ha due soluzioni distinte, ci saremmo imbattuti nel sistema

$$\begin{cases} h + k = 1 \\ h + k = 3 \end{cases}$$

che non ha soluzione.

Esempio 3.10.4

Determiniamo il termine generico della successione (a_n) definita ricorsivamente dai valori iniziali

$$a_0 := 1, \quad a_1 := 2$$

e dalla condizione

$$a_{n+1} := 4a_n - 4a_{n-1}\,.$$

L'equazione

$$x^2 - 4x + 4 = 0$$

ha come unica soluzione $\alpha = 2$. Dal sistema

$$\begin{cases} h = 1 \\ 2(h+k) = 2 \end{cases}$$

si ricava che deve essere $h = 1$ e $k = 0$. Dunque il termine generico della successione (a_n) si può esprimere come

$$a_n = (1 + 0 \cdot n)2^n$$

ossia come

$$a_n = 2^n\,.$$

Notiamo esplicitamente che in questo caso avremmo potuto anche applicare la formula trovata per il caso in cui l'equazione di secondo grado considerata ha due soluzioni distinte.

Infatti il sistema

$$\begin{cases} h + k = 1 \\ 2h + 2k = 2 \end{cases}$$

questa volta ha soluzione: precisamente, ammette le infinite soluzioni che si possono esprimere nella forma

$$h \text{ qualsiasi}, \quad k = 1 - h\,.$$

Si ottiene dunque

$$a_n = h2^n + (1-h)2^n = h2^n + 2^n - h2^n = 2^n$$

cioè (inevitabilmente) la stessa espressione ricavata applicando la formula *ad hoc*.

3.11 - Le successioni "tipo Fibonacci".

Si dice *successione di Fibonacci con valori iniziali* a_0 *e* a_1 la successione definita ricorsivamente dai valori iniziali a_0 e a_1 e dalla condizione

$$a_{n+1} := a_n + a_{n-1}\,.$$

Poiché l'equazione

(*) $$x^2 - x - 1 = 0$$

ha le due soluzioni distinte $\varphi = \frac{1+\sqrt{5}}{2}$ e $1-\varphi = \frac{1-\sqrt{5}}{2}$, il termine generico della successione di Fibonacci con valori iniziali a_0 e a_1 si può esprimere come

(°) $$a_n = h\varphi^n + k(1-\varphi)^n$$

dove h e k verificano il sistema lineare

$$\begin{cases} h + k = a_0 \\ h\varphi + k(1-\varphi) = a_1 \end{cases}.$$

La successione di Fibonacci classica (F_n) è quella con valori iniziali 0 e 1. Per lei deve essere

$$\begin{cases} h + k = 0 \\ h\varphi + k(1-\varphi) = 1 \end{cases}.$$

Per risolvere questo sistema conviene ricavare sia h che k dalla seconda equazione sommandovi un opportuno multiplo della prima. Precisamente, sommando alla seconda equazione la prima moltiplicata per $\varphi - 1$ si trova che

$$h(\varphi - 1) + h\varphi = 1$$

da cui

$$h = \frac{1}{2\varphi - 1} = \frac{1}{\sqrt{5}}$$

mentre sommando alla seconda equazione la prima moltiplicata per $-\varphi$ si trova che

$$k(-\varphi) + k(1-\varphi) = 1$$

da cui

$$k = \frac{1}{-2\varphi + 1} = \frac{-1}{2\varphi - 1} = \frac{-1}{\sqrt{5}}$$

cosicché

$$\mathrm{F}_n = \frac{\varphi^n}{\sqrt{5}} - \frac{(1-\varphi)^n}{\sqrt{5}}\,.$$

Osservando che

$$-\varphi^{-1} = -\frac{1}{\varphi} = -\frac{2}{\sqrt{5}+1} = -\frac{2\left(\sqrt{5}-1\right)}{4} = \frac{1-\sqrt{5}}{2} = 1-\varphi$$

si ottiene l'espressione alternativa

$$\mathrm{F}_n = \frac{\varphi^n}{\sqrt{5}} - \frac{(1-\varphi)^n}{\sqrt{5}} = \frac{\varphi^n}{\sqrt{5}} - \frac{(-\varphi)^{-n}}{\sqrt{5}} = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}\,.$$

Teorema 3.11.1

Sia (F_n) la successione di Fibonacci con valori iniziali 0 e 1. Si ha

$$\lim_{n \to +\infty} \frac{F_{n+1}}{F_n} = \varphi$$

Dimostrazione – Ricordiamo che, come si è visto sopra,

$$F_n = \frac{\varphi^n}{\sqrt{5}} - \frac{(1-\varphi)^n}{\sqrt{5}} = \frac{\varphi^n-(1-\varphi)^n}{\sqrt{5}}$$

e

$$F_{n+1} = \frac{\varphi^{n+1}}{\sqrt{5}} - \frac{(1-\varphi)^{n+1}}{\sqrt{5}} = \frac{\varphi^{n+1}-(1-\varphi)^{n+1}}{\sqrt{5}}$$

cosicché

$$\frac{F_{n+1}}{F_n} = \frac{\varphi^{n+1}-(1-\varphi)^{n+1}}{\varphi^n-(1-\varphi)^n} = \frac{\varphi^{n+1}-\varphi(1-\varphi)^n+\varphi(1-\varphi)^n-(1-\varphi)^{n+1}}{\varphi^n-(1-\varphi)^n} =$$

$$= \frac{\varphi(\varphi^n-(1-\varphi)^n)+(1-\varphi)^n(\varphi-(1-\varphi))}{\varphi^n-(1-\varphi)^n} = \varphi + \frac{(1-\varphi)^n(2\varphi-1)}{\varphi^n-(1-\varphi)^n} =$$

$$= \varphi + \frac{2\varphi-1}{\left(\frac{\varphi}{1-\varphi}\right)^n-1} = \varphi + \frac{\sqrt{5}}{(-\varphi^2)^n-1}$$

ricordando che $\frac{\varphi}{1-\varphi} = \frac{\varphi}{-\varphi^{-1}} = -\varphi^2$.

Poiché $\varphi > 1$, il valore assoluto di $-\varphi^2$ è maggiore di 1 cosicché

$$\lim_{n \to +\infty} \frac{\sqrt{5}}{(-\varphi^2)^n-1} = 0$$

e possiamo concludere che

$$\lim_{n \to +\infty} \frac{F_{n+1}}{F_n} = \lim_{n \to +\infty} \left(\varphi + \frac{\sqrt{5}}{(-\varphi^2)^n-1}\right) = \varphi\,.$$

Vale la pena di soffermarsi un po' sul numero φ, detto *rapporto aureo*. Esso risponde a un classico problema: *in che rapporto devono stare le due parti nelle quali si suddivide un segmento se vogliamo che una delle due parti sia media proporzionale fra l'intero segmento e l'altra*?

Se indichiamo con ℓ la lunghezza di una delle due parti e con x il loro rapporto, l'altra parte ha lunghezza $x\ell$ e l'intero segmento ha lunghezza $x\ell + \ell$. Dunque deve valere la proporzione

$$(x\ell + \ell):x\ell = x\ell:\ell$$

ossia

$$(x+1):x = x:1$$

da cui l'equazione $x^2 = x + 1$ ossia $x^2 - x - 1 = 0$, che (come abbiamo visto) ha come unica soluzione positiva φ.

Esercizio 3.11.2

Sia (F_n) la successione di Fibonacci con valori iniziali 0 e 1. Si dimostri che per ogni n dispari si ha

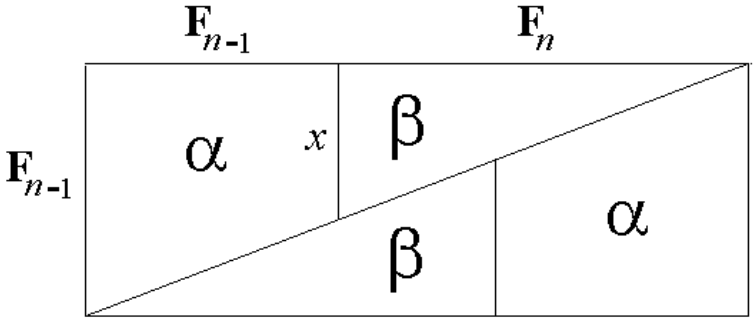
$$F_n^2 = F_{n-1} \cdot F_{n+1} + 1$$

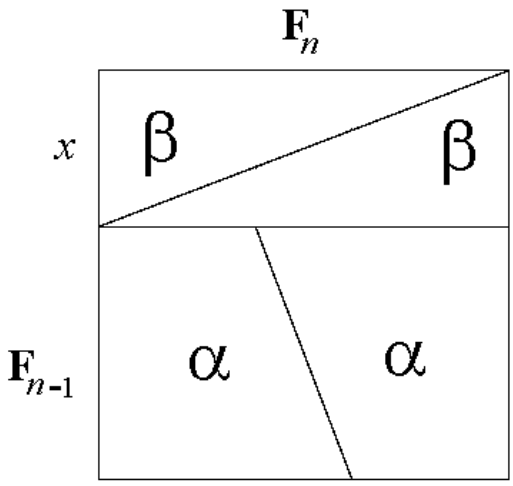
e per ogni n pari si ha

$$F_n^2 = F_{n-1} \cdot F_{n+1} - 1 .$$

Osservazione 3.11.3

Le uguaglianze viste nell'esercizio 3.11.2 sono alla base di un classico apparente paradosso geometrico, nel quale un rettangolo di dimensioni F_{n-1} e F_{n+1} viene scomposto in due trapezi congruenti ("α" nella figura qui sotto) e due triangoli congruenti ("β" nella figura qui sotto) con i quali poi si ricompone quello che sembra un quadrato di lato F_n.
È chiaro però che se quello ricomposto fosse un quadrato allora x dovrebbe essere F_{n-2}, cioè (impostando la similitudine fra gli opportuni triangoli rettangoli) dovrebbe essere $\frac{F_{n-2}}{F_{n-1}} = \frac{F_n}{F_{n+1}}$ mentre abbiamo visto sopra che il rapporto fra due numeri di Fibonacci consecutivi non è costante.





4.- OPERAZIONI IN UN INSIEME

4.1 - Operazioni in un insieme.

Sia A un insieme non vuoto.

Si dice *operazione* (*binaria*, *interna*) in A una funzione da $A \times A$ in A (cioè, intuitivamente, una "legge" che ad ogni coppia ordinata di elementi di A associa un elemento di A).

Se $\bigstar$ è un'operazione in A e $a, b \in A$, scriviamo $a \bigstar b$ anziché $\bigstar(a, b)$: così $a \bigstar b = c$ significa che c è l'immagine di (a, b) mediante $\bigstar$, ossia che $\bigstar$ associa alla coppia ordinata (a, b) di elementi di A l'elemento c di A (risalendo alla definizione formale di funzione come caso particolare di relazione: $((a, b), c) \in \bigstar$).

Esempi

4.1.1 Le ordinarie operazioni di somma e prodotto sono operazioni in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$.

4.1.2 Per ogni insieme A, la composizione definita in 3.8 è un'operazione nell'insieme di tutte le funzioni $A \to A$.

4.1.3 Nell'insieme $\mathbb{Z}$, la sottrazione è un'operazione, la divisione non lo è.

4.1.4 Nell'insieme $\mathbb{N}$ è un'operazione la $\bigstar$ definita come segue:

$$a \bigstar b = a(b+1) \qquad \forall a, b \in \mathbb{N}.$$

4.1.5 Nell'insieme $\{a, b, c\}$ è un'operazione la $\bigstar$ definita come segue [15]:

$$\boldsymbol{a \bigstar a = a, a \bigstar b = b, a \bigstar c = c, b \bigstar a = b, b \bigstar b = a, b \bigstar c = a, c \bigstar a = c, c \bigstar b = a, c \bigstar c = b.}$$

4.1.6 Sia A un insieme. Le operazioni (definite in 1.10) che a due sottoinsiemi di A associano la loro unione e la loro intersezione sono operazioni in $\mathcal{P}(A)$ (nel senso definito in 4.1) che si indicano rispettivamente con $\cup$ e $\cap$.

---

[15] Come si definisce un'operazione? Ricordiamo che "operazione in **A**" è una particolare funzione $\mathbf{A} \times \mathbf{A} \to \mathbf{A}$, cioè una particolare relazione tra $\mathbf{A} \times \mathbf{A}$ e **A**, cioè un particolare sottoinsieme di $(\mathbf{A} \times \mathbf{A}) \times \mathbf{A}$; i criteri per definire un'operazione sono dunque gli stessi che abbiamo stabilito nel capitolo 1 per definire un insieme.

In particolare, l'operazione dell'esempio 3.1.5 è definita come in 1.4; quella dell'esempio 3.1.4 come in 1.7.

4.2 - Chiusura rispetto a un'operazione.

Sia A un insieme nel quale è definita un'operazione ★.

Un sottoinsieme B di A si dice *chiuso* rispetto a ★ se comunque presi $b, b' \in \mathrm{B}$ è anche $b \bigstar b' \in \mathrm{B}$.

Esempi

4.2.1 $\mathbb{Q}^+$ è chiuso rispetto alla somma e al prodotto.

4.2.2 Il sottoinsieme di $\mathbb{N}$ formato dai numeri dispari è chiuso rispetto al prodotto ma non rispetto alla somma.

4.2.3 Siano I un insieme e A l'insieme di tutte le funzioni da I in I. Il sottoinsieme di A costituito dalle corrispondenze biunivoche (cfr. sez. 3.6) è chiuso rispetto alla composizione.

4.3 - Associatività e commutatività.

Sia A un insieme.

Un'operazione ★ in A si dice *associativa* se

$$a \bigstar (b \bigstar c) = (a \bigstar b) \bigstar c \quad \forall a, b, c \in \mathrm{A}.$$

Un'operazione ★ in A si dice *commutativa* se

$$a \bigstar b = b \bigstar a \quad \forall a, b \in \mathrm{A}.$$

Esempi

Le operazioni considerate in 4.1.1 e 4.1.6 sono associative e commutative (cfr. anche 4.6.3 e 4.6.4); quella considerata in 4.1.2 è associativa ma in generale non commutativa; quella considerata in 4.1.5 è commutativa ma non associativa (infatti $(b \bigstar b) \bigstar c \neq b \bigstar (b \bigstar c)$); quella considerata in 4.1.4 non è né associativa né commutativa.

4.4 - Elemento neutro.

Siano A un insieme e ★ un'operazione definita in A.

Un elemento n di **A** si dice *elemento neutro* per ★ se $a★n = n★a = a \quad \forall a \in A$.

Se l'operazione ★ è detta *somma*, l'elemento neutro si indica con "0" e si chiama "*zero*"; se è detta *prodotto*, si indica con "1" e si chiama "*uno*" oppure "*unità*".

Teorema 4.4.1

Siano A un insieme e ★ un'operazione definita in A. Se esiste un elemento neutro per ★, questo è unico.

Dimostrazione – Siano n, n' elementi neutri per ★. Allora $n = n★n' = n'$, come si voleva.

Esempi

4.4.2 L'operazione ★ considerata in 4.1.4 non ha elemento neutro. Si noti che $a★0 = a$ per ogni $a \in \mathbb{N}$, ma in generale $0★a \neq a$.

4.4.3 L'operazione "somma" in $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ ha come elemento neutro il numero 0.

4.4.4 L'operazione "prodotto" in $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ ha come elemento neutro il numero 1.

4.4.5 L'operazione ★ considerata in 4.1.5 ha come elemento neutro l'elemento a.

4.4.6 Le operazioni "unione" e "intersezione" considerate in 4.1.6 hanno come elemento neutro rispettivamente $\emptyset$ e A.

4.4.7 L'operazione "composizione" considerata in 4.1.2 ha come elemento neutro la funzione $\mathbf{id}_A$ definita in 3.6.4.

4.5 - Il simmetrico di un elemento.

Siano A un insieme e ★ un'operazione definita in A per la quale esiste l'elemento neutro n.

Per ogni $a \in A$, si dice *simmetrico di* a (rispetto a ★) un elemento $\overline{a} \in \mathbf{A}$ tale che sia

$$a★\overline{a} = \overline{a}★a = n\,.$$

Se l'operazione ★ è detta *somma*, il simmetrico di a si dice *opposto* di a, e si indica con $-a$; se è detta *prodotto*, si dice *inverso* di a, e si indica con a^{-1}.

Teorema 4.5.1

Siano A un insieme e ★ un'operazione associativa definita in A per la quale esiste l'elemento neutro n. Per ogni $a \in$ A, se esiste un simmetrico questo è unico.

Dimostrazione – Siano $\overline{a}$, $\overline{\overline{a}}$ simmetrici di a . Allora

$$\overline{a} = \overline{a} \bigstar n = \overline{a} \bigstar (a \bigstar \overline{\overline{a}}) = (\overline{a} \bigstar a) \bigstar \overline{\overline{a}} = n \bigstar \overline{\overline{a}} = \overline{\overline{a}} .$$

Esempi

4.5.2 Rispetto all'operazione ★ definita in 4.1.5 (che non è associativa), l'elemento b ha due distinti simmetrici: se stesso e l'elemento c.

4.5.3 In $\mathbb{Z}$, per ogni elemento esiste l'opposto (cioè, il simmetrico rispetto alla somma) ma solo per +1 e -1 esiste l'inverso (cioè, il simmetrico rispetto al prodotto).

4.5.4 Rispetto alle operazioni di "unione" e "intersezione" considerate in 4.1.6, non esiste in generale il simmetrico di un elemento di $\mathcal{P}$(A).

4.5.5 Rispetto all'operazione di "composizione" considerata in 4.1.2 non esiste in generale il simmetrico di una funzione. Tuttavia, se **f** è una corrispondenza biunivoca di **A** in sé la funzione $\mathbf{f}^{-1}$ definita in 3.7 è il simmetrico di **f** rispetto alla composizione.

4.6 - La proprietà distributiva.

Siano A un insieme e ★, ∘ due operazioni definite in A .

Si dice che ∘ è *distributiva* rispetto a ★ se

$$a \circ (b \bigstar c) = (a \circ b) \bigstar (a \circ c) \quad \text{e} \quad (a \bigstar b) \circ c = (a \circ c) \bigstar (b \circ c) \qquad \forall\, a, b, c \in \text{A} .$$

Esempi

4.6.1 Negli esempi 4.1.1, il prodotto è distributivo rispetto alla somma ma la somma non è distributiva rispetto al prodotto.

4.6.2 Ciascuna delle due operazioni considerate in 4.1.6 è distributiva rispetto all'altra (cfr. anche 1.10.5).

4.7 - Gruppi.

Siano G un insieme e $\bigstar$ un'operazione in G.

Si dice che G è un *gruppo* rispetto a $\bigstar$, oppure (più correttamente!) che la coppia $(\mathrm{G}, \bigstar)$ è un gruppo, se valgono le seguenti proprietà:

G.1 l'operazione $\bigstar$ è associativa;

G.2 esiste in G l'elemento neutro per $\bigstar$;

G.3 per ogni $g \in \mathrm{G}$ esiste il [16] simmetrico di g rispetto a $\bigstar$.

Se inoltre

G.4 l'operazione $\bigstar$ è commutativa

il gruppo si dice *commutativo* (o *abeliano*).

Esempi

4.7.1 $\mathbb{Z}$ e $\mathbb{Q}$ sono gruppi commutativi rispetto alla somma.

4.7.2 $\mathbb{N}$ non è un gruppo rispetto alla somma (non esiste in generale l'opposto di un elemento).

4.7.3 $\mathbb{Z}$ e $\mathbb{Q}$ non sono gruppi rispetto al prodotto (non esiste l'inverso di 0).

4.7.4 $\mathbb{Q}\backslash\{0\}$ e $\mathbb{Q}^+$ sono gruppi commutativi rispetto al prodotto.

4.7.5 Per ogni insieme A, l'insieme delle corrispondenze biunivoche tra A e A (cfr. sez. 3.6) è un gruppo (in generale non commutativo) rispetto alla composizione di funzioni definita in 4.7.

Siano $(\mathrm{G}, \bigstar)$ e $(\mathrm{H}, \circ)$ gruppi.

Una funzione $\mathbf{f}: \mathrm{G} \to \mathrm{H}$ si dice un *omomorfismo* tra $(\mathrm{G}, \bigstar)$ e $(\mathrm{H}, \circ)$ (o anche, più semplicemente, tra G e H) se

$$\mathbf{f}(x \bigstar y) = \mathbf{f}(x) \circ \mathbf{f}(y) \qquad \forall x, y \in \mathrm{G}.$$

Un omomorfismo che sia anche una corrispondenza biunivoca si dice *isomorfismo*.

---

[16] cfr. G.1 e il teorema 4.5.1.

4.8 - Anelli.

Sia A un insieme con almeno due elementi, e siano $+, \cdot$ due operazioni in A (che chiameremo rispettivamente *somma* e *prodotto*).

Si dice che A è un *anello* rispetto a $+$ e $\cdot$, oppure (più correttamente!) che la terna $(\mathrm{A}, +, \cdot)$ è un anello, se

A.1 $(\mathrm{A}, +)$ è un gruppo commutativo;

A.2 il prodotto è associativo;

A.3 il prodotto è distributivo rispetto alla somma.

Se inoltre

A.4 esiste in A un elemento neutro per il prodotto

oppure

A.5 il prodotto è commutativo

si dice rispettivamente che A è un *anello con unità* (e l'elemento neutro si dice l'*unità* di A) oppure che A è un *anello commutativo*. Naturalmente, se valgono sia la A.4 che la A.5 si dice che A è un *anello commutativo con unità*.

Ricordiamo che, come convenuto in 4.4, gli elementi neutri per la somma e il prodotto si indicano rispettivamente con "0" e "1"; qualora possa esservi confusione con i numeri naturali 0 e 1, si usano le notazioni "0_{A}" e "1_{A}". Inoltre, secondo quanto stabilito in 4.5, l'opposto di un elemento x si indica con $-x$, l'inverso di un elemento x si indica con x^{-1}.

Gli elementi diversi da 0 si dicono *non nulli*.

Sia $(\mathrm{A}, +, \cdot)$ un anello con unità. Un elemento a di A si dice *invertibile* se esiste in A l'inverso di a, cioè il suo simmetrico rispetto al prodotto, cioè (cfr. sez. 4.5) un elemento a^{-1} tale che $a \cdot a^{-1} = a^{-1} \cdot a = 1_{\mathrm{A}}$.

Vale la pena di osservare che, qualora il prodotto in $(\mathrm{A}, +, \cdot)$ sia commutativo, per controllare che a^{-1} è l'inverso di A basta verificare una sola delle due uguaglianze

$$a \cdot a^{-1} = 1_{\mathrm{A}} \qquad \text{e} \qquad a^{-1} \cdot a = 1_{\mathrm{A}}\,.$$

Esempi

4.8.1 $\mathbb{Z}$ e $\mathbb{Q}$ sono anelli commutativi con unità rispetto alle ordinarie operazioni di somma e prodotto. In $\mathbb{Z}$ gli unici elementi invertibili sono $+1$ e -1, in $\mathbb{Q}$ tuttti gli elementi diversi da 0 sono invertibili.

4.8.2 L'insieme dei polinomi a coefficienti in $\mathbb{Z}$ (oppure in $\mathbb{Q}$) nell'indeterminata x è un anello commutativo con unità rispetto alle usuali operazioni di somma e prodotto.

4.8.3 L'insieme dei numeri interi pari (cioè della forma $2k$ con $k \in \mathbb{Z}$) è un anello commutativo senza unità rispetto alle ordinarie operazioni di somma e prodotto.

Osservazione 4.8.4

Sia $(\mathrm{A},\ +\ ,\ \cdot\ )$ un anello. Per ogni $a \in \mathrm{A}$, si ha $a \cdot 0 = 0 \cdot a = 0$.

Dimostrazione – Ricordiamo che abbiamo convenuto in 4.4 di indicare con 0 l'elemento neutro di A rispetto alla somma. Si ha

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

da cui (sommando ad ambo i membri l'opposto di $a \cdot 0$) si ricava che $0 = a \cdot 0$. Allo stesso modo si trova che $0 \cdot a = 0$.

Sia $(\mathrm{A},\ +\ ,\ \cdot\ )$ un anello, e siano $a, b \in \mathrm{A}$. Se $a = 0$ oppure $b = 0$, allora $ab = 0$ per l'oss. 4.8.4; ma può essere $ab = 0$ anche se $a \neq 0$ e $b \neq 0$ (vedremo degli esempi in 4.9.6, 10.5.3, 10.5.4 e soprattutto nella sez. 11.2).

Sia $(\mathrm{A},\ +\ ,\ \cdot\ )$ un anello. Un elemento $a \in \mathrm{A}$ si dice un *divisore dello zero* se

(i) $a \neq 0$

e

(ii) esiste $b \in \mathrm{A}$ tale che $b \neq 0$ e $ab = 0$ oppure $ba = 0$.

Il fatto che in $\mathbb{N}$, $\mathbb{Z}$ o $\mathbb{Q}$ non ci siano divisori dello zero (ossia, come siamo abituati a dire: se un prodotto è zero, almeno uno dei fattori deve essere zero) esprime una proprietà del tutto particolare generalmente nota col nome di "*legge di annullamento del prodotto*".

Osservazione 4.8.5

Sia $(\mathrm{A},\ +\ ,\ \cdot\ )$ un anello con unità. Si ha $\quad 1 \neq 0$

ossia, l'elemento neutro per il prodotto è necessariamente distinto dall'elemento neutro per la somma.

Dimostrazione – Se fosse $1 = 0$, per ogni $a \in \mathrm{A}$ sarebbe

$$a = a \cdot 1 = a \cdot 0 = 0$$

e dunque in A esisterebbe solo l'elemento 0, contro l'ipotesi che A sia un anello (e che dunque appartengano ad A almeno due elementi).

Osservazione 4.8.6

Sia $(\mathrm{A},\ +\ ,\ \cdot\ )$ un anello con unità. Non esiste in A l'inverso di 0.

Dimostrazione – Se $a \in \mathrm{A}$, è $a \cdot 0 = 0$ per l'osservazione 4.8.4, e dunque (per l'osservazione 4.8.5) non può essere $a \cdot 0 = 1$.

Osservazione 4.8.7

Sia $(\mathrm{A},\ +\ ,\ \cdot\ )$ un anello con unità. Si ha

$$(-1) \cdot (-1) = 1;$$

inoltre, per ogni $a \in \mathrm{A}$, si ha

$$(-1) \cdot a = -a.$$

Dimostrazione – Per l'osservazione 4.8.4 si ha (applicando la proprietà distributiva)

$$0 = 0 \cdot (-1) = (1 + (-1)) \cdot (-1) = 1 \cdot (-1) + (-1) \cdot (-1) = -1 + (-1) \cdot (-1)$$

e dunque, sommando 1 ad ambo i membri, la prima parte dell'asserto. Inoltre, sempre applicando l'osservazione 4.8.4 e la proprietà distributiva,

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1+1) \cdot a = 0 \cdot a = 0$$

e, analogamente, $\ a + (-1) \cdot a = 0$, cosicché $\ (-1) \cdot a\ $ è l'opposto di a .

Siano $(\mathrm{A},\ +\ ,\ \cdot\ )$ e $(\mathrm{B},\ \oplus\ ,\ \odot\ )$ anelli.

Una funzione $\mathbf{f}\colon \mathrm{A} \to \mathrm{B}$ si dice un *omomorfismo* tra $(\mathrm{A}, +, \cdot\ )$ e $(\mathrm{B}, \oplus, \odot\ )$ (o anche, più semplicemente, tra A e B) se

$$\mathbf{f}(x+y) = \mathbf{f}(x) \oplus \mathbf{f}(y) \qquad \text{e} \qquad \mathbf{f}(x \cdot y) = \mathbf{f}(x) \odot \mathbf{f}(y) \qquad\qquad \forall x, y \in \mathrm{A}\,.$$

Un omomorfismo che sia anche una corrispondenza biunivoca si dice *isomorfismo*.

Vedremo nella sez. 10.5 un importante esempio di omomorfismo fra anelli.

4.9 - Anelli di matrici.

Sia A un insieme nel quale è definita un'operazione " $+$ " detta "somma", e sia n un numero intero positivo. Se $\mathrm{X} := (x_{i,j})$ e $\mathrm{Y} := (y_{i,j})$ sono due matrici $n \times n$ a elementi in A, si dice *somma di* X *e* Y e si indica con $\mathrm{X} + \mathrm{Y}$ la matrice $n \times n$ a elementi in A $(z_{i,j})$ per la quale si ha

$$z_{i,j} := x_{i,j} + y_{i,j}\,.$$

Esempio 4.9.1

Sia $\mathrm{A} := \mathbb{N}$, $n := 3$,

$$\mathrm{X} := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \qquad \mathrm{Y} := \begin{pmatrix} 15 & 16 & 17 \\ 18 & 19 & 20 \\ 21 & 22 & 23 \end{pmatrix}.$$

Allora

$$\mathrm{X} + \mathrm{Y} = \begin{pmatrix} 1+15 & 2+16 & 3+17 \\ 4+18 & 5+19 & 6+20 \\ 7+21 & 8+22 & 9+23 \end{pmatrix} = \begin{pmatrix} 16 & 18 & 20 \\ 22 & 24 & 26 \\ 28 & 30 & 32 \end{pmatrix}.$$

Esempio 4.9.2

Sia $\mathrm{A} := \mathbb{N}$, $n := 3$,

$$\mathrm{X} := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \qquad \mathrm{Y} := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Allora

$$\mathrm{X} + \mathrm{Y} = \begin{pmatrix} 1+0 & 2+0 & 3+0 \\ 4+0 & 5+0 & 6+0 \\ 7+0 & 8+0 & 9+0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \mathrm{X}$$

e

$$\mathrm{Y} + \mathrm{X} = \begin{pmatrix} 0+1 & 0+2 & 0+3 \\ 0+4 & 0+5 & 0+6 \\ 0+7 & 0+8 & 0+9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \mathrm{X}.$$

Sia ora $(\mathrm{A}, +, \cdot)$ un anello. Sia ancora n un numero intero positivo, e siano $\mathrm{X} := (x_{i,j})$ e $\mathrm{Y} := (y_{j,k})$ due matrici $n \times n$ a elementi in A. Si dice *prodotto righe per colonne di* X *per* Y e si indica con XY la matrice $n \times n$ a elementi in A $(z_{i,k})$ per la quale si ha

$$z_{i,k} := \sum_{j=1}^{n} x_{i,j} \cdot y_{j,k} .$$

Esempio 4.9.3

Sia $\mathrm{A} := \mathbb{Z}$, $n := 3$,

$$\mathrm{X} := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \qquad \mathrm{Y} := \begin{pmatrix} 15 & 16 & 17 \\ 18 & 19 & 20 \\ 21 & 22 & 23 \end{pmatrix}.$$

Allora

$$\mathrm{XY} = \begin{pmatrix} 1\cdot 15 + 2\cdot 18 + 3\cdot 21 & 1\cdot 16 + 2\cdot 19 + 3\cdot 22 & 1\cdot 17 + 2\cdot 20 + 3\cdot 23 \\ 4\cdot 15 + 5\cdot 18 + 6\cdot 21 & 4\cdot 16 + 5\cdot 19 + 6\cdot 22 & 4\cdot 17 + 5\cdot 20 + 6\cdot 23 \\ 7\cdot 15 + 8\cdot 18 + 9\cdot 21 & 7\cdot 16 + 8\cdot 19 + 9\cdot 22 & 7\cdot 17 + 8\cdot 20 + 9\cdot 23 \end{pmatrix} =$$

$$= \begin{pmatrix} 114 & 120 & 126 \\ 276 & 291 & 306 \\ 438 & 462 & 486 \end{pmatrix}$$

Esempio 4.9.4

Sia $\mathrm{A} := \mathbb{Z}$, $n := 3$,

$$\mathrm{X} := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \qquad \mathrm{Y} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Allora

$$\mathrm{XY} = \begin{pmatrix} 1\cdot 1 + 2\cdot 0 + 3\cdot 0 & 1\cdot 0 + 2\cdot 1 + 3\cdot 0 & 1\cdot 0 + 2\cdot 0 + 3\cdot 1 \\ 4\cdot 1 + 5\cdot 0 + 6\cdot 0 & 4\cdot 0 + 5\cdot 1 + 6\cdot 0 & 4\cdot 0 + 5\cdot 0 + 6\cdot 1 \\ 7\cdot 1 + 8\cdot 0 + 9\cdot 0 & 7\cdot 0 + 8\cdot 1 + 9\cdot 0 & 7\cdot 0 + 8\cdot 0 + 9\cdot 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \mathrm{X}$$

e

$$\mathrm{YX} = \begin{pmatrix} 1\cdot 1+0\cdot 4+0\cdot 7 & 1\cdot 2+0\cdot 5+0\cdot 8 & 1\cdot 3+0\cdot 6+0\cdot 9 \\ 0\cdot 1+1\cdot 4+0\cdot 7 & 0\cdot 2+1\cdot 5+0\cdot 8 & 0\cdot 3+1\cdot 6+0\cdot 9 \\ 0\cdot 1+0\cdot 4+1\cdot 7 & 0\cdot 2+0\cdot 5+1\cdot 8 & 0\cdot 3+0\cdot 6+1\cdot 9 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \mathrm{X}.$$

Esempio 4.9.5

Sia $\mathrm{A} := \mathbb{Z}$, $n := 3$,

$$\mathrm{X} := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Allora

$$\mathrm{XX} = \begin{pmatrix} 0\cdot 0+1\cdot 1+0\cdot 0 & 0\cdot 1+1\cdot 0+0\cdot 0 & 0\cdot 0+1\cdot 0+0\cdot 1 \\ 1\cdot 0+0\cdot 1+0\cdot 0 & 1\cdot 1+0\cdot 0+0\cdot 0 & 1\cdot 0+0\cdot 0+0\cdot 1 \\ 0\cdot 0+0\cdot 1+1\cdot 0 & 0\cdot 1+0\cdot 0+1\cdot 0 & 0\cdot 0+0\cdot 0+1\cdot 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Esempio 4.9.6

Sia $\mathrm{A} := \mathbb{Z}$, $n := 3$,

$$\mathrm{X} := \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 1 & -1 \end{pmatrix}, \qquad \mathrm{Y} := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Allora

$$\mathrm{XY} = \begin{pmatrix} 1\cdot 1+0\cdot 0+(-1)\cdot 1 & 1\cdot 1+0\cdot 0+(-1)\cdot 1 & 1\cdot 1+0\cdot 0+(-1)\cdot 1 \\ 0\cdot 1+1\cdot 0+0\cdot 1 & 0\cdot 1+1\cdot 0+0\cdot 1 & 0\cdot 1+1\cdot 0+0\cdot 1 \\ 1\cdot 1+1\cdot 0+(-1)\cdot 1 & 1\cdot 1+1\cdot 0+(-1)\cdot 1 & 1\cdot 1+1\cdot 0+(-1)\cdot 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

e

$$YX = \begin{pmatrix} 1\cdot 1+1\cdot 0+1\cdot 1 & 1\cdot 1+1\cdot 0+1\cdot 1 & 1\cdot 1+1\cdot 0+1\cdot 1 \\ 0\cdot 1+0\cdot 0+0\cdot 1 & 0\cdot 1+1\cdot 0+0\cdot 1 & 0\cdot 1+0\cdot 0+0\cdot 1 \\ 1\cdot 1+1\cdot 0+1\cdot 1 & 1\cdot 1+1\cdot 0+1\cdot 1 & 1\cdot 1+1\cdot 0+1\cdot 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 2 & 2 & 2 \\ 0 & 0 & 0 \\ 2 & 2 & 2 \end{pmatrix}.$$

Osservazione 4.9.7

Si può dimostrare che per ogni anello A e per ogni numero intero positivo n l'insieme $A^{n,n}$ delle matrici $n \times n$ a elementi in A è un anello (se $n > 1$ non commutativo) rispetto alle operazioni di somma e prodotto (righe per colonne) definite in questa sezione; l'elemento neutro rispetto alla somma è la matrice che ha tutti gli elementi uguali a zero. L'esempio 4.9.6 mostra che nell'anello $A^{3,3}$ ci sono sempre divisori dello zero.

5.- PERMUTAZIONI

5.1 - Il gruppo simmetrico.

Sia A un insieme. Una corrispondenza biunivoca $A \to A$ (cfr. sez. 3.6) si dice una *permutazione* su A. L'insieme delle permutazioni su A si dice *gruppo simmetrico su* A e si indica con **Sym**(A).

Teorema 5.1.1

Sia A un insieme, e sia $\circ$ la composizione di funzioni definita in 3.8. (**Sym**(A), $\circ$) è un gruppo.

Dimostrazione – Lo si è già osservato in 4.7.5. La composizione di funzioni è associativa in generale (teorema 3.8.4); la funzione identica definita in 3.6.4 è l'elemento neutro per $\circ$ (lo si è già osservato in 4.4.7); la "funzione inversa" $\mathbf{f}^{-1}$ definita in 3.7 è il simmetrico di $\mathbf{f} \in$ **Sym**(A) rispetto a $\circ$ (teorema 3.8.3, cfr. oss. 4.5.5).

Sia A un insieme, e sia $\sigma \in$ **Sym**(A). Si dice *supporto* (o *sostegno*) di σ l'insieme

$$supp(\sigma) := \{a \in A \,/\, \sigma(a) \neq a\}$$

cioè il sottoinsieme di A formato dagli elementi che non sono punti fissi per σ (cfr. sez. 3.5).

Due permutazioni σ, τ si dicono *disgiunte* se sono disgiunti i loro supporti (cfr. sez. 1.10), cioè se

$$supp(\sigma) \cap supp(\tau) = \emptyset .$$

Teorema 5.1.2

Due permutazioni disgiunte commutano.

Dimostrazione – Sia A un insieme, e siano $\sigma, \tau \in$ **Sym**(A) con

$$supp(\sigma) \cap supp(\tau) = \emptyset .$$

Sia $a \in A$, e proviamo che $\sigma(\tau(a)) = \tau(\sigma(a))$.

Per ipotesi, si verifica una e una sola delle tre seguenti situazioni:

(i) $a \in$ *supp*(σ);

(ii) $a \in$ *supp*(τ);

(iii) $a \notin$ *supp*(σ) e $a \notin$ *supp*(τ).

Nel caso (i), osserviamo che deve essere anche $\sigma(a) \in$ *supp*(σ); infatti, se fosse $\sigma(\sigma(a)) = \sigma(a)$, gli elementi a e $\sigma(a)$ (per ipotesi distinti, perché siamo nel caso (i)) avrebbero la stessa immagine $\sigma(a)$, contro l'iniettività di σ. Allora, poiché σ e τ sono disgiunte, $a \notin$ *supp*(τ) e $\sigma(a) \notin$ *supp*(τ), cioè $\tau(a) = a$ e $\tau(\sigma(a)) = \sigma(a)$, da cui infine

$$\sigma(\tau(a)) = \sigma(a) = \tau(\sigma(a))$$

come si voleva.

Nel caso (ii), ragionando esattamente allo stesso modo si trova che $\tau(a) \in$ *supp*(τ) e quindi che $a \notin$ *supp*(σ) e $\tau(a) \notin$ *supp*(σ), cioè $\sigma(a) = a$ e $\sigma(\tau(a)) = \tau(a)$, da cui infine

$$\sigma(\tau(a)) = \tau(a) = \tau(\sigma(a))$$

come si voleva.

Infine, nel caso (iii) si ha che $\sigma(a) = a = \tau(a)$ cosicché

$$\sigma(\tau(a)) = \sigma(a) = a \qquad \text{e} \qquad \tau(\sigma(a)) = \tau(a) = a$$

cioè ancora una volta $\sigma(\tau(a)) = \tau(\sigma(a))$ e l'asserto è completamente provato.

Nel seguito chiameremo *prodotto* la composizione di due permutazioni, e non seguiremo la particolare notazione introdotta nella sez. 3.8 per la composizione di funzioni ma useremo la semplice giustapposizione che indica abitualmente il prodotto: dunque, se σ, $\tau \in$ **Sym**(A) scriveremo $\sigma\tau$ anziché $\tau \circ \sigma$ per indicare la permutazione ottenuta applicando prima σ e poi τ.

5.2 - Il gruppo Sym(n).

Se A $:= \{1, 2, \ldots, n\}$ con $n \in \mathbb{N}$ ($n > 0$), il gruppo simmetrico su A si indica con **Sym**(n) (o anche con $\mathbf{S}_n$).

Sia $n \in \mathbb{N}$, $n > 0$. Se $\sigma \in$ **Sym**(n), σ si può rappresentare con una matrice $(m_{i,j})$ $2 \times n$ (cfr. sez. 1.5) (che si denota ancora con σ) in cui:

- nella prima riga compaiono tutti i numeri naturali da 1 a n;
- nella seconda riga compaiono in corrispondenza le loro immagini mediante σ, cioè
$$m_{2,j} = \sigma(m_{1,j}).$$

Generalmente, si preferisce che nella prima riga i numeri naturali da 1 a n compaiano in ordine crescente, cioè che sia $m_{1,j} = j$ per $j := 1, \ldots, n$; se non è così, è comunque sempre possibile riordinare le colonne della matrice in modo che questa condizione resti verificata.

Esempio 5.2.1

Sia $n = 9$. La permutazione $\sigma \in$ **Sym**(9) tale che

$$\sigma(1) = 3\,; \qquad \sigma(2) = 4\,; \qquad \sigma(3) = 7\,; \qquad \sigma(4) = 2\,; \qquad \sigma(5) = 6\,;$$
$$\sigma(6) = 9\,; \qquad \sigma(7) = 1\,; \qquad \sigma(8) = 8\,; \qquad \sigma(9) = 5$$

si rappresenta scrivendo

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

ma si potrebbe rappresentare anche (ad esempio) scrivendo

$$\sigma = \begin{pmatrix} 2 & 7 & 6 & 1 & 3 & 5 & 8 & 9 & 4 \\ 4 & 1 & 9 & 3 & 7 & 6 & 8 & 5 & 2 \end{pmatrix}.$$

La permutazione $\tau \in$ **Sym**(9) tale che

$$\tau(1) = 5\,; \qquad \tau(2) = 1\,; \qquad \tau(3) = 4\,; \qquad \tau(4) = 3\,; \qquad \tau(5) = 9\,;$$
$$\tau(6) = 8\,; \qquad \tau(7) = 7\,; \qquad \tau(8) = 6\,; \qquad \tau(9) = 2$$

si rappresenta scrivendo

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

ma si potrebbe rappresentare anche (ad esempio) scrivendo

$$\tau = \begin{pmatrix} 6 & 3 & 1 & 2 & 5 & 9 & 4 & 8 & 7 \\ 8 & 4 & 5 & 1 & 9 & 2 & 3 & 6 & 7 \end{pmatrix}.$$

Si ha

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 7 & 1 & 8 & 2 & 5 & 6 & 9 \end{pmatrix}$$

e

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 2 & 7 & 5 & 8 & 1 & 9 & 4 \end{pmatrix}$$

cosicché, in particolare, il gruppo **Sym**(9) non è commutativo.

Osservazione 5.2.2

Se la matrice $(m_{i,j})$ rappresenta la permutazione σ, la permutazione σ^{-1} (cioè l'inversa di σ) si rappresenta con la matrice che si ottiene da $(m_{i,j})$ scambiando le due righe.

Esempio 5.2.3

Per indicare la permutazione inversa della σ considerata nell'esempio 5.2.1 si può scrivere

$$\sigma^{-1} = \begin{pmatrix} 3 & 4 & 7 & 2 & 6 & 9 & 1 & 8 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

ma anche (riordinando le colonne)

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 2 & 9 & 5 & 3 & 8 & 6 \end{pmatrix}.$$

Per indicare la permutazione inversa della τ considerata nell'esempio 5.2.1 si può scrivere

$$\tau^{-1} = \begin{pmatrix} 5 & 1 & 4 & 3 & 9 & 8 & 7 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

ma anche (riordinando le colonne)

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 4 & 3 & 1 & 8 & 7 & 6 & 5 \end{pmatrix}.$$

Esempio 5.2.4

Gli elementi del gruppo simmetrico **Sym**(3) sono:

$$\mathbf{id} := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \qquad \alpha := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \qquad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$$

$$\beta := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \qquad \alpha\beta := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \qquad \alpha^2\beta := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

La struttura del gruppo **Sym**(3) si può esprimere con la sua *tavola moltiplicativa*, che all'incrocio tra la riga contrassegnata con l'elemento x e la colonna contrassegnata con l'elemento y riporta il risultato del prodotto xy:

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	**id**	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	**id**	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	**id**	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	**id**	α^2	α
αb	$\alpha\beta$	β	$\alpha^2\beta$	α	**id**	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	**id**

Il fatto che la tabella non sia simmetrica rispetto alla diagonale che va dalla casella in alto a sinistra alla casella in basso a destra esprime il fatto che il gruppo Sym(3) non è commutativo.

5.3 - Cicli.

Sia $n \in \mathbb{N}$, $n > 0$. Una permutazione σ su $\{1, 2, \ldots, n\}$ (cioè un elemento di **Sym**(n)) si dice un *ciclo* (di *lunghezza* k) se esistono $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ tali che:

- $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\sigma(i_3) = i_4$, $\ldots$, $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$;
- $\sigma(i_j) = i_j$ se $j > k$.

Per i cicli si usa una notazione più compatta ed efficiente di quella introdotta nella sez. 5.2 per le permutazioni. Il ciclo σ tale che $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\sigma(i_3) = i_4$, $\ldots$, $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$ e $\sigma(i_j) = i_j$ se $j > k$ si indica con la scrittura

$$(\, i_1 \quad i_2 \quad i_3 \quad \ldots \quad i_k \,).$$

Esempio 5.3.1

Sia $n = 9$. Il ciclo

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

si rappresenta con la scrittura

$$(1 \quad 3 \quad 5 \quad 2 \quad 7 \quad 6).$$

Teorema 5.3.2

Ogni permutazione si può scrivere come prodotto di cicli disgiunti.

Dimostrazione – Sia $\sigma \in$ **Sym**(n), e sia i_1 un elemento del supporto di σ (cfr. sez. 5.1). Sia $i_2 := \sigma(i_1)$, sia $i_3 := \sigma(i_2)$ e così via finché l'immagine di i_k mediante σ è uno degli elementi già considerati (questo avviene dopo al più n passaggi): tale elemento non può che essere i_1, perché se fosse i_j con $j \neq 1$ l'elemento i_j sarebbe immagine sia di i_{j-1} sia di i_k, contro l'iniettività di σ. Si è ottenuto così un ciclo $(\, i_1 \quad i_2 \quad i_3 \quad \ldots \quad i_k \,)$. Se $i_1, i_2, \ldots, i_k$ esauriscono il supporto di σ, σ è essa stessa un ciclo; altrimenti si considera un elemento del supporto di σ distinto da $i_1, i_2, \ldots, i_k$ e si procede allo stesso modo finché non si esaurisce il supporto di σ: a questo punto σ è espressa come prodotto di cicli disgiunti.

Esempio 5.3.3

Sia $n = 9$, e siano σ, τ le permutazioni considerate nell'esempio 5.2.1. Si ha

$\sigma = (1 \quad 3 \quad 7)(2 \quad 4)(5 \quad 6 \quad 9)$; $\qquad \tau = (1 \quad 5 \quad 9 \quad 2)(3 \quad 4)(6 \quad 8)$;

$\sigma\tau = (1 \quad 4)(2 \quad 3 \quad 7 \quad 5 \quad 8 \quad 6)$; $\qquad \tau\sigma = (1 \quad 6 \quad 8 \quad 9 \quad 4 \quad 7)(2 \quad 3)$;

$\sigma^{-1} = (1 \quad 7 \quad 3)(2 \quad 4)(5 \quad 9 \quad 6)$; $\qquad \tau^{-1} = (1 \quad 2 \quad 9 \quad 5)(3 \quad 4)(6 \quad 8)$.

Un ciclo di lunghezza 2 si dice una *trasposizione* (o, anche: uno *scambio*).

Teorema 5.3.4

Ogni permutazione si può scrivere come prodotto di trasposizioni.

Dimostrazione – Per il teorema 5.3.2, basta verificare che ogni ciclo si può scrivere come prodotto di trasposizioni; e in effetti

$$(i_1 \quad i_2 \quad i_3 \quad i_4 \quad \dots \quad i_k) = (i_1 \quad i_2)(i_1 \quad i_3)(i_1 \quad i_4)\dots(i_1 \quad i_k).$$

Esempio 5.3.5

Sia $n = 9$, e siano σ, τ le permutazioni considerate nell'esempio 5.2.1. Si ha

$$\sigma = (1 \quad 3)(1 \quad 7)(2 \quad 4)(5 \quad 6)(5 \quad 9); \quad \tau = (1 \quad 5)(1 \quad 9)(1 \quad 2)(3 \quad 4)(6 \quad 8);$$
$$\sigma\tau = (1 \quad 4)(2 \quad 3)(2 \quad 7)(2 \quad 5)(2 \quad 8)(2 \quad 6);$$
$$\tau\sigma = (1 \quad 6)(1 \quad 8)(1 \quad 9)(1 \quad 4)(1 \quad 7)(2 \quad 3);$$
$$\sigma^{-1} = (1 \quad 7)(1 \quad 3)(2 \quad 4)(5 \quad 9)(5 \quad 6); \ \tau^{-1} = (1 \quad 2)(1 \quad 9)(1 \quad 5)(3 \quad 4)(6 \quad 8).$$

Teorema 5.3.6

Se una permutazione si può scrivere come prodotto di un numero pari di trasposizioni, ogni sua espressione come prodotto di trasposizioni consta di un numero pari di trasposizioni. Se una permutazione si può scrivere come prodotto di un numero dispari di trasposizioni, ogni sua espressione come prodotto di trasposizioni consta di un numero dispari di trasposizioni.

Dimostrazione – Omettiamo la dimostrazione di questo teorema.

Una permutazione si dice pari se si può esprimere (in almeno un modo) come prodotto di un numero pari di trasposizioni. Per il teorema 5.3.6, se una permutazione è pari ogni sua espressione come prodotto di trasposizioni consta di un numero pari di trasposizioni.

Una permutazione si dice dispari se non è pari. Ancora per il teorema 5.3.6, se una permutazione è dispari ogni sua espressione come prodotto di trasposizioni consta di un numero dispari di trasposizioni.

6.- RELAZIONI DI ORDINE

6.1 - Definizioni.

Sia A un insieme.

Si dice *relazione in* A una relazione tra A e A (cioè un sottoinsieme del prodotto cartesiano A $\times$ A).

Sia ϱ una relazione in A. Essa si dice

- *riflessiva* sse $a \varrho a \quad \forall a \in \mathrm{A}$;
- *simmetrica* sse $a \varrho b \Rightarrow b \varrho a \quad \forall a, b \in \mathrm{A}$;
- *antisimmetrica* sse $(a \varrho b \text{ e } b \varrho a) \Rightarrow (a = b) \quad \forall a, b \in \mathrm{A}$;
- *transitiva* sse $(a \varrho b \text{ e } b \varrho c) \Rightarrow (a \varrho c) \quad \forall a, b, c \in \mathrm{A}$.

Sia ϱ una relazione in A. Due elementi $a, b \in$ A si dicono *confrontabili* (secondo ϱ) se si verifica almeno una delle seguenti situazioni: $a \varrho b$, $b \varrho a$. La relazione ϱ si dice *totale* sse comunque presi a, b $\in$ A essi sono confrontabili.

Esempi

6.1.1 Per ogni insieme A, la relazione "vuota" (secondo la quale nessun elemento è in relazione con alcun elemento: si tratta di $\emptyset$ pensato come sottoinsieme di A $\times$ A) è simmetrica, antisimmetrica e transitiva (ma non riflessiva).

6.1.2 La relazione ϱ in $\mathbb{Q}$ definita ponendo $a \varrho b$ sse $|\, a - b \,| < 1$ è riflessiva e simmetrica ma non transitiva.

6.1.3 La relazione ϱ nell'insieme dei cerchi del piano definita ponendo

$\mathcal{C}_1 \varrho \mathcal{C}_2$ sse l'area di $\mathcal{C}_1$ è minore o uguale all'area di $\mathcal{C}_2$

è riflessiva, transitiva e totale ma non simmetrica né antisimmetrica. Per quest'ultima affermazione, si osservi che se $\mathcal{C}_1$ e $\mathcal{C}_2$ hanno la stessa area essi sono *congruenti* ma non è in generale $\mathcal{C}_1 = \mathcal{C}_2$, cioè non sono in generale uguali!.

6.1.4 La relazione ϱ in $\mathbb{N}$ definita ponendo

$a \varrho b$ sse a, b sono entrambi pari

è simmetrica e transitiva ma non riflessiva (non è infatti, ad es., $1 \varrho 1$).

6.2 - Relazioni di ordine.

Sia A un insieme.

Una relazione in A si dice una *relazione di ordine* in A se è riflessiva, antisimmetrica e transitiva. Una relazione di ordine in A si indica spesso con $\preceq$ oppure con $\leq$ (quest'ultimo simbolo, in caso di ambiguità, è riservato all'usuale relazione di "minore o uguale" in $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$).

Sia $\preceq$ una relazione di ordine in A, e siano $a, b \in$ A. Se $a \preceq b$, si dice che a *precede* b (secondo $\preceq$); si usa anche la scrittura $b \succeq a$, che si considera equivalente.

Se una relazione di ordine in A non è totale e si vuol mettere in rilievo questo fatto, si dice che è *parziale*. In tal caso, esistono in A almeno due elementi che non sono confrontabili.

Esempi

6.2.1 L'usuale relazione $\leq$ (detta "minore o uguale") è una relazione di ordine totale in $\mathbb{N}$ e in $\mathbb{Z}$.

6.2.2 Sia A un insieme con una operazione $\cdot$ (detta "prodotto"). Se $a, b \in$ A, si dice che

$$a \textit{ divide } b \quad \text{(e si scrive } a|b)$$

se esiste $q \in$ A tale che $b = a \cdot q$. La "|" è una relazione in A; essa è una relazione di ordine (parziale) in $\mathbb{N}$ ma non in $\mathbb{Z}$ (cfr. le osservazioni 6.2.4 e 6.2.5; si veda anche la sez. 8.6).

Se a divide b, si dice anche che "a *è un divisore di* b" oppure che "b *è multiplo di* a". Se A è un anello nel quale 0 ("zero") indica l'elemento neutro per la somma, per l'oss. 4.8.4 ogni elemento di A divide 0 e quindi è un divisore ***di*** zero; si faccia attenzione a non confondere questo fatto col concetto di "divisore ***dello*** zero" introdotto nella sez. 4.8, notando in particolare che ogni divisore dello zero è un divisore di zero ma non viceversa.

6.2.3 La relazione di "inclusione" tra sottoinsiemi di un dato insieme A (cfr. esempio 3.1.3) è una relazione di ordine (parziale) nell'insieme $\mathcal{P}$(A) definito nella sez. 1.9.

Osservazione 6.2.4

La relazione "|" ("*divide*") definita in $\mathbb{N}$ ponendo

$$a|b \text{ se e soltanto se esiste } q \in \mathbb{N} \text{ tale che } b = a \cdot q$$

è una relazione di ordine parziale in $\mathbb{N}$. Infatti essa è riflessiva (per ogni $a \in \mathbb{N}$ si ha $a = a \cdot 1$), antisimmetrica (per ogni $a, b \in \mathbb{N}$, se $a|b$ e $b|a$ esistono $q_1, q_2 \in \mathbb{N}$ tali che $b = a \cdot q_1$ e $a = b \cdot q_2$; allora $b = (b \cdot q_2) \cdot q_1 = b \cdot (q_2 \cdot q_1)$ da cui $q_2 \cdot q_1 = 1$ cosicché $q_2 = 1 = q_1$ e infine $a = b$) e transitiva (per ogni $a, b, c \in \mathbb{N}$, se $a|b$ e $b|c$ esistono $q_1, q_2 \in \mathbb{N}$ tali che $b = a \cdot q_1$ e $c = b \cdot q_2$; allora $c = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$ con $q_1 \cdot q_2 \in \mathbb{N}$, e dunque $a|c$).

Osservazione 6.2.5

La relazione "|" ("*divide*") definita in $\mathbb{Z}$ ponendo

$$a|b \text{ se e soltanto se esiste } q \in \mathbb{Z} \text{ tale che } b = a \cdot q$$

non è una relazione di ordine in $\mathbb{Z}$ perché non è antisimmetrica: infatti, ad esempio, $3|(-3)$ e $(-3)|3$ ma $3 \neq -3$.

Una relazione ϱ in A si dice una *relazione di ordine stretto* in A se è transitiva e inoltre comunque presi $a, b \in$ A si verifica al più una delle seguenti due situazioni: $a \varrho b$, oppure $b \varrho a$.

Se $\preceq$ è una relazione di ordine in A, la relazione $\prec$ in A definita ponendo

$$a \prec b \quad \text{sse} \quad a \preceq b \text{ e } a \neq b$$

è una relazione di ordine stretto, che si dice *associata* a $\preceq$.

Analogamente, se $\prec$ è una relazione di ordine stretto in A, la relazione $\preceq$ in A definita ponendo

$$a \preceq b \quad \text{sse} \quad a \prec b \text{ oppure } a = b$$

è una relazione di ordine, che si dice *associata* a $\prec$.

Sia $\preceq$ una relazione di ordine in A, e sia $\prec$ la relazione di ordine stretto associata a $\preceq$: la relazione di ordine associata a $\prec$ coincide con $\preceq$. Viceversa, sia $\prec$ una relazione di ordine stretto in A, e sia $\preceq$ la relazione di ordine associata a $\prec$: la relazione di ordine stretto associata a $\preceq$ coincide con $\prec$. Ciò si potrebbe esprimere dicendo che il concetto di "relazione di ordine" e il concetto di "relazione di ordine stretto" sono equivalenti.

6.3 - Intervalli.

Siano A un insieme e $\leq$ una relazione di ordine in A. Introduciamo qui una notazione che sarà molto utile in diverse occasioni.

Siano a, b elementi di A tali che $a < b$. Si dicono *intervalli* (*limitati*) *di estremi* a, b i seguenti sottoinsiemi di A :

$(a, b) := \{x \in \text{A} \,/\, a < x < b\}$ (*intervallo aperto*)

$(a, b] := \{x \in \text{A} \,/\, a < x \leq b\}$ (*intervallo chiuso a destra*)

$[a, b) := \{x \in \text{A} \,/\, a \leq x < b\}$ (*intervallo chiuso a sinistra*)

$[a, b] := \{x \in \text{A} \,/\, a \leq x \leq b\}$ (*intervallo chiuso*)

Si dicono *intervalli illimitati* i seguenti sottoinsiemi di A :

$(-\infty, b) := \{x \in \mathrm{A} \,/\, x < b\}$ (*intervallo aperto, illimitato a sinistra*)

$(-\infty, b] := \{x \in \mathrm{A} \,/\, x \leq b\}$ (*intervallo chiuso, illimitato a sinistra*)

$(a, +\infty) := \{x \in \mathrm{A} \,/\, a < x\}$ (*intervallo aperto, illimitato a destra*)

$[a, +\infty) := \{x \in \mathrm{A} \,/\, a \leq x\}$ (*intervallo chiuso, illimitato a destra*)

$(-\infty, +\infty) := \mathrm{A}$ (*intervallo aperto, illimitato a sinistra e a destra*)

6.4 - Minimo e massimo.

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme di A.

Un elemento *m* di X si dice *il minimo* di X, e si indica con *min* X, se

$$m \leq x \quad \forall x \in \mathrm{X}\,.$$

Analogamente, un elemento *M* di X si dice *il massimo* di X, e si indica con *max* X, se

$$x \leq M \quad \forall x \in \mathrm{X}\,.$$

Teorema 6.4.1

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme di A. Se X ha un minimo [un massimo], questo è unico.

Dimostrazione – Siano *m*, *m*' minimi di X. Poiché *m* è minimo e *m*' $\in$ X, $m \leq m'$; poiché *m*' è minimo e *m* $\in$ X, $m' \leq m$. Per la proprietà antisimmetrica, $m = m'$ come si voleva.

Analogamente si prova che se X ha un massimo questo è unico.

Esempi

6.4.2 Nell'insieme $\mathbb{N}$ dotato dell'ordinaria relazione di "minore o uguale", l'insieme

$$\mathrm{X} = \{20, 30, 60, 80, 100\}$$

ha per minimo 20 e per massimo 100.

6.4.3 Nell'insieme $\mathbb{N}$ dotato della relazione di "divisibilità" (cfr. osservazione 6.2.4), l'insieme

$$\mathrm{X} = \{20, 30, 60, 80, 100\}$$

non ha minimo né massimo.

6.4.4 Nell'insieme $\mathbb{Q}$ dotato dell'ordinaria relazione di "minore o uguale", l'insieme

$$\mathbf{X} = \{x \in \mathbb{Q} \,/\, x = \tfrac{1}{n}, \text{ con } n \in \mathbb{N}\backslash\{0\}\}$$

non ha minimo; il suo massimo è 1.

6.5 - Elementi minimali ed elementi massimali.

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme di A.

Un elemento *m* di X si dice *minimale* in X se

$$(x \leq m) \Rightarrow x = m \quad \forall x \in \mathrm{X}$$

cioè se in X non esiste alcun elemento che precede strettamente *m*.

Analogamente, un elemento *M* di X si dice *massimale* in X se

$$(M \leq x) \Rightarrow x = M \quad \forall x \in \mathrm{X}$$

cioè se in X non esiste alcun elemento preceduto strettamente da *M*.

Teorema 6.5.1

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme di A. Se X ha un minimo [un massimo], questo è l'unico elemento minimale [massimale] di X.

Dimostrazione – Sia m il minimo di X, e sia m_0 un elemento minimale di X; proveremo che $m_0 = m$, da cui l'asserto.

Poiché m è il minimo di X, deve essere $m \leq m_0$; poiché m_0 è minimale in X, ne segue che $m = m_0$, come si voleva.

Analogamente si prova che se X ha un massimo questo è l'unico elemento massimale di X.

Esempio 6.5.2

Nell'insieme $\mathbb{N}$ dotato della relazione di "divisibilità" (cfr. oss. 6.2.4), l'insieme

$$\mathrm{X} = \{20, 30, 60, 80, 100, 120\}$$

ha come elementi minimali 20 e 30 e come elementi massimali 80, 100 e 120.

6.6 - Limitazioni inferiori e limitazioni superiori.

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme non vuoto di A.

Un elemento a di A si dice *limitazione inferiore* (o *minorante*) di X se

$$a \leq x \quad \forall x \in \mathrm{X};$$

si dice invece *limitazione superiore* (o *maggiorante*) di X se

$$x \leq \mathbf{a} \quad \forall x \in \mathrm{X}.$$

Il sottoinsieme non vuoto X di A si dice *inferiormente* [*superiormente*] *limitato* se esiste in A una limitazione inferiore [superiore] per X.

Esempi

6.6.1 Nell'insieme $\mathbb{N}$ dotato dell'ordinaria relazione di "minore o uguale", il sottoinsieme formato dai multipli di 57 non è superiormente limitato.

6.6.2 Nell'insieme $\mathbb{Q}^+$ dotato dell'ordinaria relazione di "minore o uguale", ogni sottoinsieme è inferiormente limitato (da 0).

6.7 - Estremo superiore.

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme non vuoto di A superiormente limitato.

Se l'insieme delle limitazioni superiori di **X** ha minimo, tale minimo si dice *estremo superiore* di **X**, e si indica con *sup* X. Dal teorema 6.4.1 segue subito che l'estremo superiore, qualora esista, è unico.

Teorema 6.7.1

Siano A un insieme, $\leq$ una relazione di ordine in A, e X un sottoinsieme non vuoto di A. Se X ha un massimo, questo è anche estremo superiore per X.

Dimostrazione – Sia m il massimo di X. Per definizione di massimo, m è una limitazione superiore per X; dobbiamo provare che per ogni limitazione superiore a di X si ha $m \leq a$: ma ciò è ovvio (poiché $m \in$ X) per definizione di limitazione superiore.

Teorema 6.7.2

Siano **A** un insieme, $\leq$ una relazione di ordine in **A**, e **X** un sottoinsieme non vuoto di **A** dotato di estremo superiore. Se **sup X** appartiene a **X**, esso è il massimo di **X**.

Dimostrazione – Sia $\mathbf{x_0}$ l'estremo superiore di **X**. Poiché $\mathbf{x_0}$ è una limitazione superiore per **X**, si ha che $\mathbf{x} \leq \mathbf{x_0}$ per ogni $\mathbf{x} \in \mathbf{X}$; poiché per ipotesi $\mathbf{x_0} \in \mathbf{X}$, si ha l'asserto.

I teoremi 6.7.1 e 6.7.2 suggeriscono che l'estremo superiore di **X** può essere assunto come "surrogato" del massimo di **X** quando tale massimo manca.

6.8 - Estremo inferiore.

Siano **A** un insieme, $\leq$ una relazione di ordine in **A**, e **X** un sottoinsieme non vuoto di **A** inferiormente limitato.

Se l'insieme delle limitazioni inferiori di **X** ha massimo, tale massimo si dice *estremo inferiore* di **X**, e si indica con **inf X**. Ancora dal teorema 6.4.1 segue che l'estremo inferiore, qualora esista, è unico.

Teorema 6.8.1

Siano **A** un insieme, $\leq$ una relazione di ordine in **A**, e **X** un sottoinsieme non vuoto di **A**. Se **X** ha un minimo, questo è anche estremo inferiore per **X**.

Dimostrazione – La dimostrazione è analoga a quella del teorema 6.7.1, e si lascia al lettore come esercizio.

Teorema 6.8.2

Siano **A** un insieme, $\leq$ una relazione di ordine in **A**, e **X** un sottoinsieme non vuoto di **A** dotato di estremo inferiore. Se **inf X** appartiene a **X**, esso è il minimo di **X**.

Dimostrazione – La dimostrazione è analoga a quella del teorema 6.7.2, e si lascia al lettore come esercizio.

Esempio 6.8.3

Nell'insieme $\mathbb{Q}$ dotato dell'ordinaria relazione di "minore o uguale", l'insieme

$$\mathrm{X} = \{x \in \mathbb{Q} \,/\, x = \tfrac{1}{n}, \text{ con } n \in \mathbb{N}\backslash\{0\}\}$$

ha per estremo inferiore il numero 0. (Cfr. esempio 6.4.4).

Dimostrazione – È chiaro che 0 è una limitazione inferiore per X; resta da provare che ogni limitazione inferiore per X è minore o uguale a 0, ossia che nessun numero razionale positivo y è limitazione inferiore per X.
Sia dunque $y \in \mathbb{Q}^+$. Possiamo scrivere $y = \frac{m}{n}$, con $m, n \in \mathbb{N}\backslash\{0\}$; allora

$$y = \frac{m}{n} = \frac{2m}{2n} = 2m\frac{1}{2n} > \frac{1}{2n}$$

con $\frac{1}{2n} \in \mathbf{X}$, come si voleva.

Esercizio 6.8.4

Nell'insieme $\mathbb{N}$ dotato della relazione di "divisibilità" (cfr. oss. 6.2.4), si consideri l' insieme

$$\mathrm{X} = \{20, 30, 60, 80, 100, 120\} \qquad \text{(cfr. esempio 6.4.2).}$$

Determinare (qualora esistano) estremo inferiore ed estremo superiore per X.

7.- L'ALGORITMO DI EUCLIDE IN $\mathbb{N}$

7.1 - Ancora su ($\mathbb{N}$, $\leq$).

Teorema 7.1.1

Ogni insieme non vuoto superiormente limitato di numeri naturali ha massimo.

Dimostrazione – Proviamo (per induzione su n) che:

se $\emptyset \neq \mathrm{A} \subset \mathbb{N}$ e $a \leq n$ per ogni $a \in \mathrm{A}$, allora A ha massimo.

Se $n = 0$, deve essere $\mathrm{A} = \{0\}$ e quindi A ha per massimo lo zero. Supponiamo dunque che l'asserto sia vero per n.

Sia $\emptyset \neq \mathrm{A} \subset \mathbb{N}$ tale che $a \leq n+1$ per ogni $a \in \mathrm{A}$, e proviamo che A ha massimo. Distinguiamo due casi:

(i) $n+1 \in \mathrm{A}$; in questo caso, è immediato che $n+1$ è il massimo di A;

(ii) $n+1 \notin \mathrm{A}$; in questo caso $a < n+1$ (e dunque $a \leq n$) per ogni $a \in \mathrm{A}$, quindi otteniamo che A ha massimo per l'ipotesi di induzione.

Teorema 7.1.2

Ogni insieme non vuoto di numeri naturali ha minimo.

Dimostrazione – Sia $\emptyset \neq \mathrm{A} \subset \mathbb{N}$. Se $0 \in \mathrm{A}$, 0 è il minimo di A (infatti $0 \leq x$ per ogni $x \in \mathbb{N}$, dunque in particolare $0 \leq x$ per ogni $x \in \mathrm{A}$). Se $0 \notin \mathrm{A}$, poniamo

$$\mathrm{S} := \{n \in \mathbb{N} \,/\, n \notin \mathrm{A} \text{ e } (n \leq a \text{ per ogni } a \in \mathrm{A})\}.$$

L'insieme S non è vuoto (infatti $0 \in \mathrm{S}$) e (per come è definito) è superiormente limitato (da ogni $a \in \mathrm{A}$): per il teorema 7.1.1, S ha un massimo m. Poiché $m \in \mathrm{S}$,

$$m \notin \mathrm{A} \quad \text{e} \quad m \leq a \text{ per ogni } a \in \mathrm{A}.$$

In effetti, poiché $m \notin \mathrm{A}$, è addirittura $m < a$ per ogni $a \in \mathrm{A}$, cosicché

$$m+1 \leq a \text{ per ogni } a \in \mathrm{A}.$$

Dunque $m+1 \in \mathrm{A}$, (altrimenti sarebbe $m+1 \in \mathrm{S}$, assurdo perché è m il massimo di S) e quindi m+1 è il minimo di A.

7.2 - La divisione euclidea.

Teorema 7.2.1

Comunque presi $a, b \in \mathbb{N}$ con $b \neq 0$ esiste un'unica coppia ordinata (q, r) di numeri naturali tale che

(i) $a = bq + r$;

e

(ii) $0 \leq r < b$.

Dimostrazione – Sia

$$\mathrm{S} := \{x \in \mathbb{N} \,/\, x = bn \text{ con } n \in \mathbb{N} \text{ e } x \leq a\}.$$

L'insieme S non è vuoto (perché $0 \in$ S, essendo $0 = b \cdot 0$ e $0 \leq a$) ed è superiormente limitato da a, dunque per il teorema 7.1.1 ha massimo x_0 (che, per definizione di S, è della forma bq con $q \in \mathbb{N}$). Poiché $bq \leq a$, possiamo calcolare $r := a - bq$ e ottenere la (i). Se fosse $r \geq b$, potremmo calcolare $r_1 := r - b$, da cui $r = b + r_1$ e quindi

$$a = bq + r = bq + b + r_1 = b(q + 1) + r_1$$

assurdo perché $b(q + 1)$ sarebbe un elemento di S strettamente maggiore di x_0 (essendo per ipotesi $b \neq 0$).

Dunque per ogni scelta di a e b in $\mathbb{N}$ (con $b \neq 0$) esiste una coppia ordinata (q, r) di numeri interi che verifica sia la (i) che la (ii). Resta da provare che tale coppia è unica.

Supponiamo che sia

$$a = bq_1 + r_1 = bq_2 + r_2$$

(con $0 \leq r_1 < b$, $0 \leq r_2 < b$) e proviamo che $q_1 = q_2$ e $r_1 = r_2$. Poniamo, per fissare le idee, $q_1 \geq q_2$ (altrimenti nel ragionamento che segue si scambia il ruolo di q_1 con quello di q_2 e il ruolo di r_1 con quello di r_2). Non può essere $r_1 > r_2$ (altrimenti non varrebbe la seconda uguaglianza) dunque possiamo scrivere

$$b(q_1 - q_2) = r_2 - r_1.$$

Se fosse $q_1 \neq q_2$, sarebbe $q_1 - q_2 \geq 1$ e dunque il primo membro sarebbe $\geq b$; ma allora sarebbe anche

$$r_2 = b(q_1 - q_2) + r_1 \geq b + r_1 \geq b$$

contro la (ii). Dunque $q_1 = q_2$ e di conseguenza anche $r_1 = r_2$, e l'asserto è completamente provato.

Siano $a, b \in \mathbb{N}$, con $b \neq 0$. I due numeri naturali q e r di cui al teorema 7.2.1 si dicono rispettivamente *quoziente* e *resto* della *divisione euclidea di a per b* (e i numeri naturali a e b si dicono rispettivamente *dividendo* e *divisore* di tale divisione euclidea).

Osservazione 7.2.2

Siano $a, b \in \mathbb{N}$. Condizione necessaria e sufficiente affinché b divida a (nel senso dell'esempio 6.2.2) è che il resto della divisione euclidea di a per b sia 0.

Osservazione 7.2.3

La divisione euclidea realizza l'idea intuitiva di "spartizione in parti uguali", ma è vincolata dalla scelta che il resto debba essere positivo. È vero che nel classico problema della maestra che deve dividere 30 caramelle fra 7 bambini la soluzione "pratica" è proprio quella fornita in via teorica dalla divisione euclidea: poiché $30 = 7 \cdot 4 + 2$, a ogni bambino spettano 4 caramelle e ne avanzano 2 (e le mangia la maestra?). Ma si pensi a un altro problema formalmente analogo: se 30 studenti devono partire per una gita scolastica, e sono disponibili pullmini da 7 posti l'uno, quanti pullmini bisognerà prenotare? Questa volta la risposta "teorica" (si prenotano 4 pullmini e 2 bambini restano a casa) non è accettabile come soluzione pratica; si dovrebbe scegliere il resto r negativo, $0 \geq r > -b$, e così, poiché $30 = 7 \cdot 5 + (-5)$, si avrebbe la conferma teorica della soluzione "pratica": si prenotano 5 pullmini, sui quali complessivamente 5 posti resteranno vuoti. Ma, d'altro lato, la scelta di un resto negativo non avrebbe alcuna interpretazione sensata nel problema delle caramelle…

Osservazione 7.2.4

Non è difficile estendere la definizione di "divisione euclidea" (e il teorema 7.2.1) a due numeri interi relativi a, b; ma è chiaro che la condizione

$$0 \leq r < b$$

sul resto r non è ipotizzabile quando $b < 0$. Bisognerà dunque scegliere se imporre che il resto r sia positivo ($0 \leq r < |b|$) oppure imporre che il resto r sia compreso tra 0 e b (escluso b), e a seconda di come daremo la definizione si otterrà un quoziente diverso: infatti (ad esempio) 7 diviso -2 potrebbe avere quoziente -3 e resto 1 (se si definisce la divisione euclidea in modo che il resto sia sempre positivo) oppure potrebbe avere quoziente -4 e resto -1 (se si definisce la divisione euclidea in modo che il resto sia sempre compreso fra 0 e il divisore).

Per fortuna non c'è ambiguità di scelta nell'estendere la definizione di divisione euclidea al caso in cui il dividendo è un qualsiasi numero intero relativo e il divisore è un numero intero positivo, e noi ci limiteremo a questo caso perché è l'unico che ci servirà.

Teorema 7.2.5

Comunque presi a in $\mathbb{Z}$ e b in $\mathbb{Z}^+$, esiste un'unica coppia ordinata $(q,\ r)$ di numeri interi relativi tale che

(i) $\quad a = bq + r$;

e

(ii) $\quad 0 \leq r < b$.

Dimostrazione – Se $a \in \mathbb{Z}^+$ (oppure $a = 0$), poiché identifichiamo i numeri naturali con gli interi non negativi (cfr. sez. 1.3) possiamo applicare direttamente il teorema 7.2.1 per ottenere l'asserto.

Se $a \in \mathbb{Z}^-$, è $-a \in \mathbb{Z}^+$, dunque (per il teorema 7.2.1 e la già citata identificazione di $\mathbb{N}$ coi numeri interi non negativi) esiste una coppia ordinata $(q,\ r)$ di numeri interi non negativi tale che

(j) $\quad -a = bq_0 + r_0$;

e

(jj) $\quad 0 \leq r_0 < b$.

Dalla (i) segue che

$$a = -(-a) = -bq_0 - r_0 = b(-q_0) - r_0 = b(-q_0 - 1) + (b - r_0)$$

cioè le (i) e (ii) per $\quad q := -q_0 - 1 \quad$ e $\quad r := b - r_0$.

Dunque per ogni scelta di a in $\mathbb{Z}$ e b in $\mathbb{Z}^+$ esiste una coppia ordinata $(q,\ r)$ di numeri interi che verifica sia la (i) che la (ii). Resta da provare che tale coppia è unica, e a tale scopo si può ripetere esattamente il ragionamento visto nella dimostrazione del teorema 7.2.1.

Supponiamo che sia

$$a = bq_1 + r_1 = bq_2 + r_2$$

(con $0 \leq r_1 < b$, $0 \leq r_2 < b$) e proviamo che $\quad q_1 = q_2 \quad$ e $\quad r_1 = r_2$. Poniamo, per fissare le idee, $\quad q_1 \geq q_2 \quad$ (altrimenti nel ragionamento che segue si scambia il ruolo di q_1 con quello di q_2 e il ruolo di r_1 con quello di r_2). Non può essere $r_1 > r_2$ (altrimenti non varrebbe la seconda uguaglianza) dunque possiamo scrivere

$$b(q_1 - q_2) = r_2 - r_1 .$$

Se fosse $q_1 \neq q_2$, sarebbe $q_1 - q_2 \geq 1$ e dunque il primo membro sarebbe $\geq b$; ma allora sarebbe anche

$$r_2 = b(q_1 - q_2) + r_1 \geq b + r_1 \geq b$$

contro la (ii). Dunque $q_1 = q_2$ e di conseguenza anche $r_1 = r_2$, e l'asserto è completamente provato.

7.3 - Massimo comun divisore in $\mathbb{N}$. L'algoritmo di Euclide.

Siano $a, b \in \mathbb{N}$. Si dice *massimo comun divisore di a e b* e si indica con MCD(a,b) l'estremo inferiore di $\{a,b\}$ rispetto alla relazione di ordine (parziale) $|$ ("divide", cfr. oss. 6.2.4), cioè un $\delta \in \mathbb{N}$ tale che $\delta|a$, $\delta|b$ e per ogni $d \in \mathbb{N}$ tale che $d|a$ e $d|b$ si ha anche $d|\delta$. Se MCD$(a,b) = 1$, si dice talvolta che *a è primo con b* oppure che a e b sono *primi fra loro*.

Se a e b sono confrontabili rispetto alla relazione "divide" (cioè $a|b$ oppure $b|a$), MCD(a,b) è il minimo di $\{a,b\}$ (rispetto alla relazione $|$), cioè quello dei due che divide l'altro.

Osservazione 7.3.1

Siano $a, b \in \mathbb{N}$ e sia r il resto della divisione euclidea di a per b. Sia $d \in \mathbb{N}$.

Sono fatti equivalenti:

(i) d divide sia a che b;

(ii) d divide sia b che r.

Dimostrazione – Poiché r è il resto della divisione euclidea di a per b, si ha che

$$a = bq + r\,.$$

Supponiamo che valga la (i); allora esistono $h, k \in \mathbb{N}$ tali che $a = dh$ e $b = dk$. Ne segue che $r = a - bq = dh - dkq = d(h - kq)$ cosicché d divide (sia b che) r, cioè vale la (ii).

Supponiamo ora che valga la (ii); allora esistono $k, t \in \mathbb{N}$ tali che $b = dk$ e $r = dt$. Ne segue che $a = bq + r = dkq + dt = d(kq + t)$ cosicché d divide (sia b che) a, cioè vale la (i).

L'osservazione 7.3.1 è la chiave di un veloce algoritmo (attribuito al matematico greco *Euclide*) per calcolare il massimo comun divisore fra due numeri naturali. L'esistenza di tale algoritmo costituisce anche una dimostrazione ("costruttiva") del fatto che il massimo comun divisore esista per ogni coppia di numeri naturali.

Teorema 7.3.2 ("algoritmo di Euclide" per calcolare il MCD in $\mathbb{N}$)

Siano $a, b \in \mathbb{N}$, con $b \neq 0$. Posto $r_0 := a$ e $r_1 := b$, definiamo induttivamente r_{i+1} come il resto della divisione euclidea di r_{i-1} per r_i finché $r_i \neq 0$, $r_{i+1} = 0$ se $r_i = 0$. Allora:

(1) esiste i_0 tale che $r_{i_0} \neq 0$ ma $r_i = 0$ per $i \geq i_0$;

(2) $r_{i_0} = \text{MCD}(a,b)$;

(3) per ogni $i \in \mathbb{N}$, esistono $\alpha_i, \beta_i \in \mathbb{Z}$ tali che $r_i = \alpha_i a + \beta_i b$.

Dimostrazione – Poiché per ipotesi r_1 ($= b$) è $\neq 0$, e poiché $r_{i+1} < r_i$ quando $r_i \neq 0$, (per il teor. 7.2.1), c'è un numero finito (≥ 1) di valori di i per i quali $r_i \neq 0$, da cui la (1).

Applicando ripetutamente l'osservazione 7.3.1, si trova che per ogni terna (r_{i-1}, r_i, r_{i+1}) la coppia di numeri $\{r_{i-1}, r_i\}$ ha esattamente gli stessi divisori comuni della coppia di numeri $\{r_i, r_{i+1}\}$ e quindi

$$\text{MCD}(r_{i-1}, r_i) = \text{MCD}(r_i, r_{i+1}) \quad \text{per ogni } i < i_0 \,.$$

In particolare, $\text{MCD}(a, b) = \text{MCD}(r_0, r_1) = \text{MCD}(r_{i-1}, r_i)$ per ogni $i \leq i_0$. D'altro lato, $\text{MCD}(r_{i_0-1}, r_{i_0}) = r_{i_0}$ perché r_{i_0} divide r_{i_0-1} (essendo $r_{i_0+1} = 0$), da cui la (2).

Proviamo infine la (3) procedendo per induzione su i . Per $i := 0$,

$$r_0 = b = 0 \cdot a + 1 \cdot b$$

cioè la (3) con $\alpha_0 := 0$ e $\beta_0 := 1$. Dalla $a = bq_0 + r_1$ si deduce subito che

$$r_1 = a + (-q_0)b$$

cioè la (3) per $i = 1$ con $\alpha_1 := 1$ e $\beta_1 := (-q_0)$.

Supponiamo adesso di sapere che $r_{i-1} = \alpha_{i-1}a + \beta_{i-1}b$ con $\alpha_{i-1}, \beta_{i-1} \in \mathbb{Z}$ e $r_i = \alpha_i a + \beta_i b$ con $\alpha_i, \beta_i \in \mathbb{Z}$ e proviamo la (3) per $i + 1$. Poiché $r_{i-1} = r_i q_i + r_{i+1}$ si ha

$$r_{i+1} = r_{i-1} - r_i q_i = \alpha_{i-1}a + \beta_{i-1}b - (\alpha_i a + \beta_i b)q_i = (\alpha_{i-1} - \alpha_i q_i)a + (\beta_{i-1} - \beta_i q_i)b$$

con $\alpha_{i-1} - \alpha_i q_i$, $\beta_{i-1} - \beta_i q_i \in \mathbb{Z}$ e dunque anche la (3) è provata

La (3) del teorema 7.3.2 per $i = i_0$ si dice *identità di Bézout*.

Esempio 7.3.3

Sia $a := 1794, b := 1938$. Si ha

$1938 = 1 \cdot 1794 + 144$; $1794 = 12 \cdot 144 + 66$; $144 = 2 \cdot 66 + 12$;
$66 = 5 \cdot 12 + 6$; $12 = 2 \cdot 6 + 0$.

Dunque $\text{MCD}(1794, 1938) = 6$. Inoltre:

$144 = 1938 - 1794$;
$66 = 1794 - 12 \cdot (1938 - 1794) = 13 \cdot 1794 - 12 \cdot 1938$;
$12 = 144 - 2 \cdot 66 = 1938 - 1794 - 2 \cdot (13 \cdot 1794 - 12 \cdot 1938) = 25 \cdot 1938 - 27 \cdot 1794$;
$6 = 66 - 5 \cdot 12 = 13 \cdot 1794 - 12 \cdot 1938 - 5 \cdot (25 \cdot 1938 - 27 \cdot 1794) = 148 \cdot 1794 - 137 \cdot 1938$.

Esempio 7.3.4

$a := 213\,443, b := 175\,477$. Si ha

$$213\,443 = 1 \cdot 175\,477 + 37\,966;$$
$$175\,477 = 4 \cdot 37\,966 + 23\,613;$$
$$37\,966 = 1 \cdot 23\,613 + 14\,353;$$
$$23\,613 = 1 \cdot 14\,353 + 9\,260;$$
$$14\,353 = 1 \cdot 9\,260 + 5\,093;$$
$$9\,260 = 1 \cdot 5\,093 + 4\,167;$$
$$5\,093 = 1 \cdot 4\,167 + 926;$$
$$4\,167 = 4 \cdot 926 + 463;$$
$$926 = 2 \cdot 463 + 0;$$

Dunque $\mathrm{MCD}(213\,443, 175\,477) = 463$. Inoltre:

$$37\,966 = 213\,443 - 175\,477;$$
$$23\,613 = 175\,477 - 4 \cdot (213\,443 - 175\,477) = 5 \cdot 175\,477 - 4 \cdot 213\,443;$$
$$14\,353 = 37\,966 - 23\,613 = 213\,443 - 175\,477 - (5 \cdot 175\,477 - 4 \cdot 213\,443) =$$
$$= 5 \cdot 213\,443 - 6 \cdot 175\,477;$$
$$9\,260 = 23\,613 - 14\,353 = 5 \cdot 175\,477 - 4 \cdot 213\,443 - (5 \cdot 213\,443 - 6 \cdot 175\,477) =$$
$$= 11 \cdot 175\,477 - 9 \cdot 213\,443.$$
$$5\,093 = 14\,353 - 9\,260 = 5 \cdot 213\,443 - 6 \cdot 175\,477 - (11 \cdot 175\,477 - 9 \cdot 213\,443) =$$
$$= 14 \cdot 213\,443 - 17 \cdot 175\,477.$$
$$4\,167 = 9\,260 - 5\,093 = 11 \cdot 175\,477 - 9 \cdot 213\,443 - (14 \cdot 213\,443 - 17 \cdot 175\,477) =$$
$$= 28 \cdot 175\,477 - 23 \cdot 213\,443.$$
$$926 = 5\,093 - 4\,167 = 14 \cdot 213\,443 - 17 \cdot 175\,477 - (28 \cdot 175\,477 - 23 \cdot 213\,443) =$$
$$= 37 \cdot 213\,443 - 45 \cdot 175\,477.$$
$$463 = 4\,167 - 4 \cdot 926 = 28 \cdot 175\,477 - 23 \cdot 213\,443 - 4 \cdot (37 \cdot 213\,443 - 45 \cdot 175\,477) =$$
$$= 208 \cdot 175\,477 - 171 \cdot 213\,443.$$

Osservazione 7.3.5

Siano $a, b \in \mathbb{N}$, e sia $\delta := \mathrm{MCD}(a, b)$. Allora

$$\mathrm{MCD}(\tfrac{a}{\delta}, \tfrac{b}{\delta}) = 1.$$

Dimostrazione – Dobbiamo provare che 1 è l'unico divisore comune di $\frac{a}{\delta}$ e $\frac{b}{\delta}$, cioè che: se il numero naturale k divide sia $\frac{a}{\delta}$ che $\frac{b}{\delta}$ allora $k = 1$. Sia dunque

$$\tfrac{a}{\delta} = kq_1 \quad (\text{ossia} \quad a = k\delta q_1) \qquad \text{e} \qquad \tfrac{b}{\delta} = kq_2 \quad (\text{ossia} \quad b = k\delta q_2).$$

Allora $k\delta$ divide sia a che b, quindi $k\delta$ deve dividere δ; ma certamente δ divide $k\delta$ e dunque per la proprietà antisimmetrica della relazione "divide" in $\mathbb{N}$ (cfr. oss. 6.2.4) deve essere $\delta = k\delta$ e quindi $k = 1$.

Teorema 7.3.6

Siano $a, b, c \in \mathbb{N}$. Se MCD$(a, b) = 1$, allora

$$a|bc \quad \text{se e soltanto se} \quad a|c\,.$$

Dimostrazione – Se $a|c$, poiché $c|bc$ è anche $a|bc$ per la transitività della relazione "|" (cfr. oss. 6.2.4) (qui la condizione MCD$(a, b) = 1$ non serve).

Supponiamo ora che a divida il prodotto bc; esisterà $\gamma \in \mathbb{N}$ tale che $bc = a\gamma$. Per l'identità di Bézout, esistono $\alpha, \beta \in \mathbb{Z}$ tali che

$$1 = \alpha a + \beta b$$

e quindi

$$c = \alpha ac + \beta bc = \alpha ac + \beta a\gamma = a(\alpha c + \beta\gamma)$$

cioè a divide c, come si voleva dimostrare.

7.4 - Una classe di equazioni diofantine.

Si parla di *equazioni diofantine* (o *diofantee*) (in onore del matematico greco $\Delta\iota\grave{o}\varphi\alpha\nu\tau o\varsigma$, vissuto probabilmente nel terzo secolo) quando si considera una uguaglianza fra polinomi (generalmente in più indeterminate) con coefficienti in $\mathbb{Z}$ e ci si chiede quali elementi di $\mathbb{N}$ (o di $\mathbb{Z}$) vadano sostituiti alle indeterminate dei polinomi affiché l'uguaglianza risulti vera. L'identità di Bezout vista nella sezione 7.2 consente di studiare e risolvere una importante classe di equazioni diofantine.

Teorema 7.4.1

Siano $a, b, c \in \mathbb{N}$ con $a \neq 0$ e $b \neq 0$. Esiste una soluzione in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione

$$ax + by = c$$

se e soltanto se c è multiplo di MCD(a, b).

Dimostrazione – Se esiste una soluzione $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ dell'equazione considerata, è $ax_0 + by_0 = c$. Posto $\delta := \text{MCD}(a, b)$, esistono $a_0, b_0 \in \mathbb{N}$ tali che $a = a_0\delta$ e $b = b_0\delta$, cosicché

$$c = ax_0 + by_0 = a_0\delta x_0 + b_0\delta y_0 = \delta(a_0x_0 + b_0y_0)\,;$$

poiché $c, \delta \in \mathbb{N}$, deve essere anche $a_0x_0 + b_0y_0 \in \mathbb{N}$ e quindi si è provato che c è multiplo di δ.

Viceversa, se c è multiplo di δ sarà $c = c_0\delta$ con $c_0 \in \mathbb{N}$; per l'identità di Bézout esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\delta = \alpha a + \beta b$, quindi

$$c = c_0\delta = c_0(\alpha a + \beta b) = c_0\alpha a + c_0\beta b$$

cioè $(c_0\alpha, c_0\beta)$ è soluzione in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione considerata.

Teorema 7.4.2

Siano $a, b, c \in \mathbb{N}$, e sia $\delta := \text{MCD}(a, b)$. Se (x_0, y_0) è soluzione in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione

$$ax + by = \delta\,,$$

allora (cx_0, cy_0) è soluzione in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione

$$ax + by = c\delta\,.$$

Dimostrazione – Infatti dall'uguaglianza

$$ax_0 + by_0 = \delta$$

segue la

$$a(cx_0) + b(cy_0) = c\delta\,.$$

Osservazione 7.4.3

Siano $a, b, c \in \mathbb{N}$, e sia $\delta := \text{MCD}(a, b)$. Non tutte le soluzioni in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione

$$ax + by = c\delta$$

sono della forma (cx_0, cy_0) con (x_0, y_0) soluzione soluzione in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione

$$ax + by = \delta\,.$$

Ad esempio, l'equazione $2x + 3y = 5$ ha la soluzione $(1, 1)$ oltre a tutte le soluzioni della forma $(5(3h - 1), 5(1 - 2h))$ con $h \in \mathbb{Z}$ (come vedremo col teorema 7.4.4, le coppie della forma $(3h - 1,\ 1 - 2h)$ con $h \in \mathbb{Z}$ sono tutte le soluzioni dell'equazione $2x + 3y = 1$).

Teorema 7.4.4

Siano $a, b, c \in \mathbb{N}$, con $a \neq 0$, $b \neq 0$ e c multiplo di $\delta := \text{MCD}(a, b)$. Se (x_0, y_0) è una soluzione in $\mathbb{Z} \times \mathbb{Z}$ dell'equazione

$$ax + by = c\,,$$

tutte le soluzioni di tale equazione in $\mathbb{Z} \times \mathbb{Z}$ sono della forma $x = x_0 + h\frac{b}{\delta}$, $y = y_0 - h\frac{a}{\delta}$ al variare di $h \in \mathbb{Z}$.

Dimostrazione – Se

$$ax_0 + by_0 = c,$$

è anche

$$a\big(x_0 + h\tfrac{b}{\delta}\big) + b\big(y_0 - h\tfrac{a}{\delta}\big) = ax_0 + h\tfrac{ab}{\delta} + by_0 - h\tfrac{ab}{\delta} = ax_0 + by_0 = c\,.$$

e dunque anche $(x_0 + h\frac{b}{\delta}, y_0 - h\frac{a}{\delta}) \in \mathbb{Z} \times \mathbb{Z}$ è soluzione dell'equazione considerata.

Viceversa, sia $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$ tale che $ax_1 + by_1 = c$. Sottraendo membro a membro dalla

$$ax_0 + by_0 = c$$

la

$$ax_1 + by_1 = c$$

si trova che

$$a(x_0 - x_1) + b(y_0 - y_1) = 0$$

ossia

$$a(x_0 - x_1) = b(y_1 - y_0)\,.$$

Ricordando che si è posto $\delta := \text{MCD}(a, b)$, possiamo scrivere $a = \overline{a}\delta$, $b = \overline{b}\delta$ con $\text{MCD}(\overline{a}, \overline{b}) = 1$ e dunque, dividendo per δ ambo i membri dell'ultima uguaglianza,

$$\overline{a}(x_0 - x_1) = \overline{b}(y_1 - y_0)\,.$$

Supponiamo per il momento che sia $x_0 \geq x_1$, cosicché anche $y_1 \geq y_0$ e stiamo lavorando in $\mathbb{N}$.

Poiché $\text{MCD}(\overline{a}, \overline{b}) = 1$, per il teorema 7.3.6 $\overline{a}$ divide $(y_1 - y_0)$ e $\overline{b}$ divide $(x_0 - x_1)$, ossia

$$y_1 - y_0 = h\overline{a}, \quad x_0 - x_1 = k\overline{b} \quad \text{per opportuni } h, k \in \mathbb{N}\,.$$

Ne segue che

$$y_1 = y_0 + h\overline{a} = y_0 + h\tfrac{a}{\delta} \quad \text{e} \quad x_1 = x_0 - k\overline{b} = x_0 - k\tfrac{b}{\delta}\,.$$

Poiché (x_1, y_1) è soluzione dell'equazione data, deve essere

$$c = ax_1 + by_1 = a\big(x_0 - k\tfrac{b}{\delta}\big) + b\big(y_0 + h\tfrac{a}{\delta}\big) = ax_0 + by_0 - k\tfrac{ab}{\delta} + h\tfrac{ab}{\delta} = c + (h - k)\tfrac{ab}{\delta}$$

da cui

$$(h - k)\tfrac{ab}{\delta} = 0$$

e quindi (poiché per ipotesi $a \neq 0$ e $b \neq 0$) $h = k$.

Se invece nella

$$\overline{a}(x_0 - x_1) = \overline{b}(y_1 - y_0)$$

è $x_1 > x_0$, cosicché anche $y_0 > y_1$, la scriviamo come

$$\overline{a}(x_1 - x_0) = \overline{b}(y_0 - y_1)$$

per lavorare ancora in $\mathbb{N}$. Ragionando esattamente come sopra, si trova che

$$x_1 = x_0 + h\tfrac{b}{\delta} \quad \text{e} \quad y_1 = y_0 - h\tfrac{a}{\delta} \quad \text{per un opportuno } h \text{ in } \mathbb{N}$$

e ciò completa la dimostrazione del teorema.

Esempio 7.4.5

Risolviamo in $\mathbb{Z}$ l'equazione

$$84x + 60y = 150\,.$$

Vediamo in primo luogo se ci sono soluzioni. Applichiamo l'algoritmo euclideo per trovare MCD$(84, 60)$; se l'equazione data risulterà avere soluzioni, i passaggi che facciamo adesso ci faranno comodo per calcolarle.

$84 = 60 \cdot 1 + 24\,;$
$60 = 24 \cdot 2 + 12\,;$
$24 = 12 \cdot 2 + 0\,.$

Quindi MCD$(84, 60) = 12\,.$

Poiché $150 = 12 \cdot 12 + 6$ (cioè 150 non è multiplo di 12) l'equazione data non ha soluzioni.

Esempio 7.4.6

Risolviamo in $\mathbb{Z}$ l'equazione

$$616x + 490y = 210\,.$$

Vediamo in primo luogo se ci sono soluzioni. Applichiamo l'algoritmo euclideo per trovare MCD$(616, 490)$; se l'equazione data risulterà avere soluzioni, i passaggi che facciamo adesso ci faranno comodo per calcolarle.

$616 = 490 \cdot 1 + 126\,;$
$490 = 126 \cdot 3 + 112\,;$
$126 = 112 \cdot 1 + 14\,;$
$112 = 14 \cdot 8 + 0\,.$

Quindi MCD$(616, 490) = 14\,.$ Poiché $210 = 14 \cdot 15$ (cioè 210 è multiplo di 14) l'equazione data ha soluzioni. Cerchiamo in primo luogo una soluzione dell'equazione

$$616x + 490y = 14\,.$$

Dai calcoli effettuati per trovare MCD$(616, 490)$ si ricava che:

$126 = 616 - 490\,;$
$112 = 490 - 126 \cdot 3 = 490 - (616 - 490) \cdot 3 = 4 \cdot 490 - 3 \cdot 616\,;$
$14 = 126 - 112 = 616 - 490 - (4 \cdot 490 - 3 \cdot 616) = 4 \cdot 616 - 5 \cdot 490\,.$

Quindi, $(4, -5)$ è una soluzione di $616x + 490y = 14\,;$ e di conseguenza $(60, -75)$ è una soluzione di $616x + 490y = 210\,.$ Le soluzioni dell'equazione sono, per il teorema 7.4.4, tutte e sole le coppie ordinate $(60 + 35h, -75 - 44h)\,.$

Esempio 7.4.7

Per risolvere in $\mathbb{Z}$ l'equazione

$$280x - 385y = 175\,.$$

andiamo a considerare l'equazione

$$280x + 385y = 175\,.$$

Vediamo in primo luogo se ci sono soluzioni. Applichiamo l'algoritmo euclideo per trovare MCD$(385, 280)$; se l'equazione data risulterà avere soluzioni, i passaggi che facciamo adesso ci faranno comodo per calcolarle.

$385 = 280 \cdot 1 + 105\,;$ $\quad 280 = 105 \cdot 2 + 70\,;$ $\quad 105 = 70 \cdot 1 + 35\,;$ $\quad 70 = 35 \cdot 2 + 0\,.$

Quindi MCD$(385, 280) = 35$. Poiché $175 = 35 \cdot 5$ (cioè 175 è multiplo di 35) l'equazione a cui ci siamo ricondotti ha soluzioni. Cerchiamo in primo luogo una soluzione dell'equazione

$$280x + 385y = 35\,.$$

Dai calcoli effettuati per trovare MCD$(385, 280)$ si ricava che:

$105 = 385 - 280\,;$
$70 = 280 - 2 \cdot 105 = 280 - 2 \cdot (385 - 280) = 3 \cdot 280 - 2 \cdot 385\,;$
$35 = 105 - 70 = 385 - 280 - (3 \cdot 280 - 2 \cdot 385) = 3 \cdot 385 - 4 \cdot 280\,.$

Dunque $(-4, 3)$ è una soluzione di $280x + 385y = 35$; e di conseguenza $(-20, 15)$ è una soluzione di $280x + 385y = 175$. Le soluzioni di tale equazione sono, per il teorema 7.4.4, tutte e sole le coppie ordinate $(-20 + 11h, 15 - 8h)$.

Pertanto, le soluzioni dell'equazione proposta sono tutte e sole le coppie ordinate $(-20 + 11h, 8h - 15)$.

Esercizi

Risolvere in $\mathbb{Z} \times \mathbb{Z}$ le seguenti equazioni diofantine:

7.4.8 $\quad 406x + 147y = 84\,;$

7.4.9 $\quad 122x - 305y = 183\,;$

7.4.10 $\quad 333x + 888y = 1111\,;$

7.4.11 $\quad 357x - 255y = 204\,;$

7.4.12 $\quad 102x + 174y = 150\,.$

7.5 - Minimo comune multiplo in $\mathbb{N}$.

Siano $a, b \in \mathbb{N}$. Si dice *minimo comune multiplo di a e b* e si indica con mcm(a, b) l'estremo superiore di $\{a, b\}$ rispetto alla relazione di ordine (parziale) "$|$" ("divide", cfr. oss. 6.2.4), cioè un $\mu \in \mathbb{N}$ tale che $a|\mu$, $b|\mu$ e per ogni $m \in \mathbb{N}$ tale che $a|m$ e $b|m$ si ha anche $\mu|m$.

Se a e b sono confrontabili rispetto alla relazione "$|$" (cioè $a|b$ oppure $b|a$), mcm(a, b) è il massimo di $\{a, b\}$ rispetto alla relazione "$|$", cioè quello dei due che è multiplo dell'altro.

Teorema 7.5.1

Siano $a, b \in \mathbb{N}$. Si ha $\quad \text{mcm}(a, b) = \frac{ab}{\text{MCD}(a,b)}$.

Dimostrazione – Sia $\delta := \text{MCD}(a, b)$; allora $a = \overline{a}\delta$ e $b = \overline{b}\delta$ per opportuni $\overline{a}$, $\overline{b} \in \mathbb{N}$, con $\text{MCD}(\overline{a}, \overline{b}) = 1$ per l'osservazione 7.3.5.

Poniamo $\mu := \frac{ab}{\text{MCD}(a,b)} = \frac{ab}{\delta} = a\overline{b} = \overline{a}b$. Come si è appena visto, sia a che b dividono μ. Resta da provare che se $m \in \mathbb{N}$ è tale che $a|m$ (cioè $m = am_1$ con $m_1 \in \mathbb{N}$) e $b|m$ (cioè $m = bm_2$ con $m_2 \in \mathbb{N}$) si ha anche $\mu|m$. Dalle uguaglianze

$$am_1 = m = bm_2$$

segue che $\quad \overline{a}\delta m_1 = \overline{b}\delta m_2 \quad$ e quindi $\quad \overline{a}m_1 = \overline{b}m_2$.

Poiché $\text{MCD}(\overline{a}, \overline{b}) = 1$, per il teorema 7.3.6 $\overline{b}$ divide m_1, cioè esiste $b_1 \in \mathbb{N}$ tale che $m_1 = \overline{b}b_1$; si può così concludere che

$$m = am_1 = a\overline{b}b_1 = \mu b_1$$

ossia $\mu|m$ come si voleva dimostrare.

8.- NUMERI PRIMI IN $\mathbb{N}$

8.1 - Numeri irriducibili e numeri primi in $\mathbb{N}$.

Sia $p \in \mathbb{N}\backslash\{0,1\}$. Si dice che p è *irriducibile* se

8.1.I gli unici numeri naturali che dividono p sono 1 e p .

Teorema 8.1.1

Sia $p \in \mathbb{N}\backslash\{0,1\}$. Se p è irriducibile, allora

comunque presi $a, b \in \mathbb{N}$, se p divide il prodotto ab e p non divide a allora p divide b .

Dimostrazione – Siano $a, b \in \mathbb{N}$. Supponiamo che p divida il prodotto ab ma non divida a. Allora MCD$(p, a) = 1$ (l'unico altro divisore di p, cioè p stesso, per ipotesi non divide a), e dunque per il teorema 7.3.6 p divide b , come si voleva.

La proprietà espressa dal teorema 8.1.1 è talmente importante da giustificare un'apposita definizione.

Sia $p \in \mathbb{N}\backslash\{0,1\}$. Si dice che p è *primo* se

8.1.P comunque presi $a, b \in \mathbb{N}$, se p divide il prodotto ab e p non divide a allora p divide b .

Esempio 8.1.2

Il numero naturale 6 non è primo, perché (scelti $a := 2$ e $b := 9$)

6 divide il prodotto $2 \cdot 9$ ($= 18$) e 6 non divide 2, ma 6 non divide nemmeno 9 .

Possiamo ora esprimere il contenuto del teorema 8.1.1 dicendo che: ogni numero naturale irriducibile è primo. Di fatto vale anche il viceversa, e quindi (per i numeri naturali!) i concetti di "primo" e "irriducibile" si equivalgono:

Teorema 8.1.3

Sia $p \in \mathbb{N}\backslash\{0, 1\}$. Sono fatti equivalenti:

(i) p è primo;

(ii) p è irriducibile.

Dimostrazione – (i) $\Rightarrow$ (ii).

Se p è un numero primo, vogliamo provare che gli unici divisori di p sono 1 e p. Sia dunque n un divisore di p e dimostriamo che $n = 1$ oppure $n = p$. Poiché n è divisore di p si ha che $p = nh$ con $h \in \mathbb{N}$ (e anche h è un divisore di p). Se p divide n allora $n = p$ (per la proprietà antisimmetrica della relazione "divide"); se invece p non divide n, poiché p divide il prodotto nh (e poiché p è primo) necessariamente p divide h, e quindi $p = h$ (ancora per la proprietà antisimmetrica della relazione "divide"); in questo caso $n = 1$, e l'asserto è comunque provato.

(ii) $\Rightarrow$ (i).

Questo è il contenuto del teorema 8.1.1 .

L'equivalenza fra il concetto di "primo" e "irriducibile" non vale però in contesti più generali: si rimanda alle sezioni 8.6, 8.7 e 8.8 il lettore interessato ad approfondire questo fatto.

8.2 - Il "teorema fondamentale dell'aritmetica".

Lemma 8.2.1

Siano p, $q_1, q_2, ..., q_s$ numeri primi. Se p divide il prodotto $q_1\, q_2 \ldots q_s$, esiste $i \in \{1, 2, ..., s\}$ tale che $p = q_i$.

Dimostrazione – Procediamo per induzione su s. Se $s = 1$, non c'è niente da dimostrare. Supponiamo vero il teorema per s e dimostriamolo per $s + 1$.

Supponiamo che p divida il prodotto $q_1\, q_2 \ldots q_{s+1}$.

Se p divide q_1, deve essere $p = q_1$; infatti q_1 è primo (e quindi irriducibile), dunque non ha altri divisori che 1 e q_1, ma $p \neq 1$ perché p è primo. Se p non divide q_1, poiché p divide il prodotto fra q_1 e $q_2\, q_3 \ldots q_{s+1}$, per definizione di numero primo deve dividere $q_2\, q_3 \ldots q_{s+1}$; ma questi sono s numeri primi, e per l'ipotesi di induzione p deve coincidere con uno di essi.

Teorema 8.2.2 ("Teorema fondamentale dell'aritmetica")

Ogni numero naturale (tranne 0 e 1) si può esprimere come prodotto di numeri primi (eventualmente uno solo), e tale espressione è unica (a meno dell'ordine).

Dimostrazione – Proviamo, procedendo per induzione su n, che

(*) ogni numero naturale ≥ 2 e $\leq n$ si può esprimere come prodotto di numeri primi (eventualmente uno solo).

Il primo valore di n per cui provare la (*) è 2. Se $n = 2$, l'unico numero naturale da considerare è 2; poiché 2 è primo (basta osservare che il prodotto di due numeri dispari è necessariamente dispari) la (*) è vera per $n = 2$.

Ora supponiamo di aver provato la (*) per n, e proviamola per $n + 1$. Tutti i numeri ≥ 2 e $\leq n$ si possono esprimere come prodotto di numeri primi (eventualmente uno solo) per l'ipotesi di induzione; resta da considerare $n + 1$. Se $n + 1$ è primo, non c'è altro da provare; se $n + 1$ non è primo, per il teorema 8.1.3 ha un divisore a diverso da 1 e da $n + 1$, cioè

$$n + 1 = ab$$

con $a \neq 1, n + 1$ e quindi necessariamente anche $b \neq 1, n + 1$. In particolare, sia a che b sono ≥ 2 e $\leq n$, quindi per l'ipotesi di induzione ciascuno di essi si può esprimere come prodotto di numeri primi (eventualmente uno solo); di conseguenza anche ab si può esprimere come prodotto di numeri primi.

Proviamo infine, procedendo per induzione su n, che

(°) ogni numero naturale ≥ 2 e $\leq n$ si può esprimere in un solo modo come prodotto di numeri primi.

Osserviamo preliminarmente che ogni numero primo (per il teorema 8.1.3) non si può esprimere come prodotto di numeri primi diversi da lui.

Il primo valore di n per cui provare la (°) è 2. Se $n = 2$, l'unico numero naturale da considerare è 2; poiché 2 è primo, la (°) è vera per $n = 2$.

Ora supponiamo di aver provato la (°) per n, e proviamola per $n + 1$. Tutti i numeri ≥ 2 e $\leq n$ si possono esprimere in un solo modo (a meno dell'ordine) come prodotto di numeri primi per l'ipotesi di induzione; resta da considerare $n + 1$. Se $n + 1$ è primo, non c'è altro da provare; sia allora $n + 1 = p_1 p_2 ... p_h = q_1 q_2 ... q_k$ con $h, k \geq 2$ e i p_i e i q_j numeri primi. Poiché il numero primo p_1 divide il prodotto $q_1\, q_2 \,...\, q_k$, p_1 deve coincidere con uno dei q_j; riordinandoli, possiamo supporre che sia $p_1 = q_1$. Allora $p_2 p_3 ... p_h = q_2 q_3 ... q_k \leq n$, quindi per l'ipotesi di induzione $h - 1 = k - 1$ e $p_2, p_3, ..., p_h$ coincidono con $q_2, q_3, ..., q_h$ a meno dell'ordine. Dunque la (°) è provata per $n + 1$ e con essa il teorema.

Esercizio 8.2.3

Esprimere come prodotto di numeri primi i seguenti numeri naturali:

$30\,031$; $305\,613$; $510\,511$; $223\,693$

Lemma 8.2.4

Sia $n \in \mathbb{N}\backslash\{0,1\}$. Se n non è irriducibile, n ha un divisore non superiore a $\sqrt{n}$.

Dimostrazione – Se n non è irriducibile si può scrivere

$$n = ab$$

con $a, b \neq 1, n$. Se a e b fossero entrambi strettamente maggiori di $\sqrt{n}$, si avrebbe la contraddizione

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n$$

dunque almeno uno dei divisori di n è $\leq \sqrt{n}$.

Osservazione 8.2.5 (il "crivello di Eratostene")

Sia $n \in \mathbb{N}$. Un efficiente algoritmo per ottenere tutti i numeri irriducibili compresi tra 2 e n è dovuto al matematico libico (ma di cultura greca) Eratostene (Cirene, 280 a.C. – Alessandria 195 a.C.).

(i) sia $\mathcal{L} := \{x \in \mathbb{N} \,/\, 2 \leq x \leq n\}$;
(ii) si ponga $p := 2$;
(iii) si ripeta
si cancellino da $\mathcal{L}$ tutti i multipli di p (eccetto p stesso), e sia $\overline{p}$ il primo numero rimasto in $\mathcal{L}$ dopo p (nell'usuale ordinamento $\leq$ di $\mathbb{N}$) ;
si ponga $p := \overline{p}$;
finché $p \geq \sqrt{n}$.

Ad ogni iterazione del ciclo descritto in (iii), $\overline{p}$ risulta irriducibile perché non è multiplo di nessun numero che lo precede nell'usuale ordinamento $\leq$ di $\mathbb{N}$. L'algoritmo termina quando $p \geq \sqrt{n}$ per il lemma 8.2.4 .

Teorema 8.2.6

Esistono infiniti numeri primi.

Dimostrazione – Procediamo per assurdo. Se esistessero soltanto s numeri primi p_1, p_2, ..., p_s, il numero

$$p_1 \cdot p_2 \cdot \ldots \cdot p_s + 1$$

non si potrebbe esprimere come prodotto di numeri primi, perché il resto della sua divisione euclidea per ciascuno dei numeri $p_1, p_2, ..., p_s$ è 1 . Ma ciò contraddirebbe il "teorema fondamentale dell'aritmetica" (teor. 8.2.2).

Osservazione 8.2.7

Se $p_1, p_2, ..., p_s$ sono numeri primi, il numero $p_1 p_2 ... p_s + 1$ non è in generale primo. Ad esempio, 5 e 7 sono numeri primi, ma $5 \cdot 7 + 1 = 36$ e 36 non è un numero primo.

Osservazione 8.2.8

Per ogni $n \in \mathbb{N}$, si possono facilmente trovare n numeri naturali consecutivi nessuno dei quali è primo: basta considerare $(n+1)! + 2$, $(n+1)! + 3$, $(n+1)! + 4$, $\ldots$, $(n+1)! + n + 1$ (cfr. esempio 3.9.5) . Il $j-$ simo di questi numeri è infatti divisibile per $j + 1$.

Osservazione 8.2.9

Sono numeri primi

- 11 ;
- $1\,111\,111\,111\,111\,111\,111$;
- $11\,111\,111\,111\,111\,111\,111\,111$;
- $\underbrace{111\ldots\ldots\ldots 111}_{317 \text{ cifre}}$;
- $\underbrace{111\ldots\ldots\ldots 111}_{1\,031 \text{ cifre}}$;

Non è noto se esistano altri numeri primi che si scrivano ([17]) usando soltanto la cifra 1.

Esercizio 8.2.10

Sia n un numero primo che si scrive ([18]) ripetendo k volte la cifra 1. Si dimostri che k è un numero primo.

[17] Naturalmente ci riferiamo a una scrittura "in base 10". Questo concetto sarà chiarito nella sez. 9.6.

[18] in qualunque base (si veda, ancora una volta, la sez. 9.6)

8.3 - Numeri primi "di Fermat".

Il giurista francese Pierre de Fermat (Beaumont-de-Lomagne, 17.8.1601 – Castres, 12.1.1665) era un grande appassionato di matematica, e fra le altre cose si dedicò allo studio dei numeri primi che si possono scrivere nella forma $2^k + 1$ con $k \in \mathbb{N}$.

Osserviamo preliminarmente che: se $2^k + 1$ (con $k \in \mathbb{N}$) è irriducibile, k non può avere divisori dispari maggiori di 1 (e quindi k deve essere della forma 2^n con $n \in \mathbb{N}$).

Lemma 8.3.1

Sia $k \in \mathbb{N}$. Se $k = dh$ con d numero naturale dispari maggiore di 1, $2^k + 1$ non è irriducibile.

Dimostrazione – Infatti se d è un numero naturale dispari maggiore di 1 si ha

$$2^{dh} + 1 = (2^h)^d + 1 = (2^h + 1)\left((2^h)^{d-1} - (2^h)^{d-2} + \ldots - 2^h + 1\right).$$

Sia $n \in \mathbb{N}$. Si dice *numero di Fermat relativo a* n il numero

$$\mathbf{F}_n := 2^{2^n} + 1 .$$

Avendo osservato che $\mathbf{F}_0$, $\mathbf{F}_1$, $\mathbf{F}_2$, $\mathbf{F}_3$ e $\mathbf{F}_4$ sono primi, Fermat congetturò che tutti gli $\mathbf{F}_n$ fossero primi. In realtà si ha che

$$\mathbf{F}_0 = 2^1 + 1 = 3,$$
$$\mathbf{F}_1 = 2^2 + 1 = 5,$$
$$\mathbf{F}_2 = 2^4 + 1 = 17,$$
$$\mathbf{F}_3 = 2^8 + 1 = 257$$

e $$\mathbf{F}_4 = 2^{16} + 1 = 65\,537$$

sono davvero tutti numeri primi, ma

$$\mathbf{F}_5 = 2^{32} + 1 = 4\,294\,967\,297$$

è divisibile per 641, e finora non si è trovato nessun altro numero di Fermat che risulti primo.

8.4 - Numeri primi "di Mersenne".

Il monaco francese Marin Mersenne (Oizé-in-Maine, 8.9.1588 – Parigi, 1.9.1648) si dedicò allo studio dei numeri primi della forma $2^k - 1$, che in suo onore sono detti "di Mersenne".

Osserviamo preliminarmente che: se $2^k - 1$ (con $k \in \mathbb{N}$) è irriducibile, k deve essere a sua volta irriducibile.

Lemma 8.4.1

Sia $k \in \mathbb{N}$. Se $k = ab$ con $1 < a < k$, il numero $2^k - 1$ non è irriducibile.

Dimostrazione – Infatti

$$2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\big((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 2^a + 1\big)$$

e se $1 < a < k$ è $1 < 2^a - 1 < 2^k - 1$. Dunque, se $k = ab$ con $1 < a < k$, il numero $2^k - 1$ ($= 2^{ab} - 1$) è divisibile per $2^a - 1$ con $1 < 2^a - 1 < 2^k - 1$.

Esistono numeri irriducibili p per i quali $2^p - 1$ non è irriducibile: ad esempio, per $p := 11$ si ha $2^{11} - 1 = 2047 = 23 \cdot 89$. È però nota una caratterizzazione dei numeri primi p per i quali $2^p - 1$ è un numero primo:

Teorema 8.4.2 (François Lucas – Derrick Lehmer)

Sia S_n la successione di numeri naturali definita ricorsivamente per $n \geq 2$ dalle condizioni

$S_2 := 4$;

$S_{n+1} := S_n^2 - 2$.

Per ogni numero primo $p > 2$, $2^p - 1$ è un numero primo se e soltanto se $2^p - 1$ divide S_p.

Dimostrazione – Omettiamo la dimostrazione di questo teorema. Si noti che $2^2 - 1 = 3$ è un numero primo ma non divide S_2.

Osservazione 8.4.3

Vale la pena di osservare che la successione S_n definita nel teorema 8.4.2 cresce molto velocemente, quindi il criterio espresso dal teorema non è di facile applicazione.

8.5 - Numeri perfetti.

Un numero naturale si dice *perfetto* se è uguale alla somma dei suoi divisori diversi da lui. Ad esempio, sono numeri perfetti: 6 ($= 1 + 2 + 3$) e 28 ($= 1 + 2 + 4 + 7 + 14$).

Si noti che 3 non è un numero perfetto.

Si ignora se esistano numeri perfetti dispari. I numeri perfetti pari sono invece completamente caratterizzati dal seguente risultato:

Teorema 8.5.1

I numeri perfetti pari sono tutti e soli i numeri naturali della forma

$$2^{n-1}(2^n-1) \quad \text{con} \quad 2^n-1 \text{ numero primo.}$$

Dimostrazione – Proviamo in primo luogo che ogni numero naturale α della forma

$$\alpha := 2^{n-1}(2^n-1) \quad \text{con} \quad 2^n-1 \text{ numero primo}$$

è un numero perfetto.

Posto $p := 2^n-1$, dalla definizione di "numero primo" (sez. 7.8) segue subito che gli unici divisori primi di α sono 2 e p; pertanto i divisori di α sono

$$1, 2, 2^2, 2^3, \dots, 2^{n-2}, 2^{n-1}, p, 2p, 2^2p, 2^3p, \dots, 2^{n-2}p, 2^{n-1}p$$

e, in particolare, i divisori di α diversi da α sono

$$1, 2, 2^2, 2^3, \dots, 2^{n-2}, 2^{n-1}, p, 2p, 2^2p, 2^3p, \dots, 2^{n-2}p\,.$$

La loro somma è

$$\sum_{k=0}^{n-1}2^k + \sum_{k=0}^{n-2}(2^kp) = \sum_{k=0}^{n-1}2^k + p\cdot\sum_{k=0}^{n-2}2^k \overset{\text{(esempio 2.4.4)}}{=}$$

$$= (2^n-1) + p\cdot\sum_{k=0}^{n-2}2^k = p + p\cdot\sum_{k=0}^{n-2}2^k = p\left(1+\sum_{k=0}^{n-2}2^k\right) \overset{\text{(esempio 2.4.4)}}{=} p\cdot 2^{n-1} = \alpha$$

quindi α è un numero perfetto.

Viceversa, sia α un numero perfetto pari; per il teorema fondamentale dell'aritmetica (teor. 8.2.2) sarà

$$\alpha = 2^{n-1}d$$

con d dispari.

Osserviamo subito che

– $n > 1$, perché α è pari;

e

– $d > 1$, perché 2^{n-1} non è un numero perfetto; infatti $2^{n-1} = 1 + \sum_{k=0}^{n-2}2^k$ (ancora in base all'esempio 2.4.4) e dunque 2^{n-1} non è un numero perfetto.

Se d è un numero primo, i divisori di α diversi da α sono

$$1, 2, 2^2, 2^3, \dots, 2^{n-2}, 2^{n-1}, d, 2d, 2^2d, 2^3d, \dots, 2^{n-2}d$$

e poiché per ipotesi α è un numero perfetto sarà

$$2^{n-1}d = \alpha = \sum_{k=0}^{n-1}2^k + d\left(\sum_{k=0}^{n-2}2^k\right) = 2^{n-1} + \sum_{k=0}^{n-2}2^k + d\left(\sum_{k=0}^{n-2}2^k\right) =$$

$$= 2^{n-1} + \left(\sum_{k=0}^{n-2} 2^k\right)(1+d) \overset{\text{(esempio 2.4.4)}}{=} 2^{n-1} + (2^{n-1}-1)(1+d) =$$

$$= 2^{n-1} + 2^{n-1} + 2^{n-1}d - 1 - d$$

da cui

$$0 = 2^{n-1} + 2^{n-1} - 1 - d = 2 \cdot 2^{n-1} - 1 - d = 2^n - 1 - d$$

e infine

$$d = 2^n - 1$$

cosicché α è della forma desiderata.

Resta da mostrare che se d non è un numero primo si giunge ad un assurdo.

Se d non è un numero primo, indichiamo con

$$d_1(=1), d_2, d_3, \ldots, d_t \quad (t \geq 2)$$

i divisori di d diversi da d; allora i divisori di α diversi da α sono

$$\begin{array}{lllllll}
1, & 2, & 2^2, & 2^3, & \ldots, & 2^{n-2}, & 2^{n-1}, \\
d_2, & 2d_2, & 2^2 d_2, & 2^3 d_2, & \ldots, & 2^{n-2} d_2, & 2^{n-1} d_2, \\
d_3, & 2d_3, & 2^2 d_3, & 2^3 d_3, & \ldots, & 2^{n-2} d_3, & 2^{n-1} d_3, \\
\ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\
d_t, & 2d_t, & 2^2 d_t, & 2^3 d_t, & \ldots, & 2^{n-2} d_t, & 2^{n-1} d_t, \\
d, & 2d, & 2^2 d, & 2^3 d, & \ldots, & 2^{n-2} d\,. &
\end{array}$$

La loro somma (raggruppando per colonne le prime t righe, e raggruppando a sé l'ultima riga) è

$$\sum_{k=1}^{t} d_k + 2 \cdot \left(\sum_{k=1}^{t} d_k\right) + 2^2 \cdot \left(\sum_{k=1}^{t} d_k\right) + 2^3 \cdot \left(\sum_{k=1}^{t} d_k\right) + \ldots + 2^{n-1} \cdot \left(\sum_{k=1}^{t} d_k\right) + d\left(\sum_{k=0}^{n-2} 2^k\right) =$$

$$= \left(\sum_{k=0}^{n-1} 2^k\right)\left(\sum_{k=1}^{t} d_k\right) + d\left(\sum_{k=0}^{n-2} 2^k\right)$$

Poiché per ipotesi α $(= 2^{n-1}d)$ è un numero perfetto, questa somma deve valere $2^{n-1}d$, cioè (tenendo ancora una volta conto dell'esempio 2.4.4)

$$\left(\sum_{k=0}^{n-1} 2^k\right)\left(\sum_{k=1}^{t} d_k\right) + d\left(\sum_{k=0}^{n-2} 2^k\right) = \left(\left(\sum_{k=0}^{n-2} 2^k\right) + 1\right)d = d\left(\sum_{k=0}^{n-2} 2^k\right) + d$$

da cui

$$\left(\sum_{k=0}^{n-1} 2^k\right)\left(\sum_{k=1}^{t} d_k\right) = d\,.$$

Ma questo (poiché $n > 1$) significa in particolare che

$$\sum_{k=1}^{t} d_k \quad \text{è un divisore di } d \text{ diverso da } \quad d$$

cioè è uno dei d_k: e questo è un assurdo, come si voleva.

Esercizio 8.5.2

Sia n un numero perfetto, e siano d_1, d_2, …, d_k tutti i divisori di n (incluso n). Si dimostri che

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} = 2\,.$$

8.6 - Divisibilità negli anelli commutativi con unità privi di divisori dello zero.

Sia A un anello commutativo con unità (cfr. sez. 4.8) privo di divisori dello zero; quest'ultimo fatto, come si è già detto nella sez. 4.8, si può esprimere dicendo che in A vale la "legge di annullamento del prodotto".

Se $a, b \in$ A, abbiamo già introdotto (esempio 6.2.2) l'espressione verbale

$$a \textit{ divide } b \quad \text{(e la notazione simbolica } a|b\text{)}$$

per esprimere il fatto che esiste $q \in$ A tale che $b = a \cdot q$.

Se $a, b \in$ A, sono espressioni equivalenti:

(i) a divide b ;

(ii) b è multiplo di a ;

(iii) a è un divisore di b (l'insieme dei divisori di b è $\{x \in \text{A} \,/\, x \text{ divide } b\}$) .

Si noti la differenza sostanziale (anche se apparentemente sottilissima) fra "divisore di 0" (per l'oss. 4.8.4, ogni elemento di A divide 0, e quindi è un divisore di 0) e "divisore dello 0" (concetto introdotto nella sez. 4.8).

La "|" è una relazione in A che adesso vogliamo studiare.

Osservazione 8.6.1

Sia A un anello con unità. La relazione "|" ("divide") definita in A ponendo

$$a|b \quad \text{sse} \quad \text{esiste } q \in \text{A tale che } b = a \cdot q$$

è riflessiva e transitiva.

Dimostrazione – Poiché per ipotesi A è un anello con unità $1_{\mathbf{A}}$, per ogni $a \in$ A è

$$a = a \cdot 1_{\mathbf{A}}$$

ossia $a|a$: dunque la relazione "|" è riflessiva.

Siano ora $a, b, c \in$ A tali che $a|b$ e $b|c$; ciò significa che esiste $q_1 \in$ A tale che $b = a \cdot q_1$ ed esiste $q_2 \in$ A tale che $c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$ con $q_1 \cdot q_2 \in$ A, cosicché $a|c$: dunque la relazione "|" è transitiva.

Osservazione 8.6.2

Sia A un anello commutativo con unità privo di divisori dello zero, e sia "|" la relazione "divide" definita in A ponendo

$$a|b \quad \text{sse} \quad \text{esiste } q \in \text{A tale che } b = a \cdot q\,.$$

Comunque presi $a, b \in$ A, sono fatti equivalenti:

(i) $\quad a|b$ e $b|a$;

(ii) $\quad b = a \cdot h \quad$ con $\quad h \in$ A $\quad$ invertibile;

(iii) $\quad a = b \cdot k \quad$ con $\quad k \in$ A $\quad$ invertibile.

In particolare, la relazione "|" non è in generale antisimmetrica.

Dimostrazione – Basterà provare che $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$ e $(iii) \Rightarrow (i)$.

$(i) \Rightarrow (ii)$.

Siano $a, b \in$ A. Se $a|b$ esiste $h \in$ A tale che $b = a \cdot h$ e se $b|a$ esiste $k \in$ A tale che $a = b \cdot k$, cosicché

$$b = a \cdot h = (b \cdot k) \cdot h = b \cdot (k \cdot h)$$

da cui

$$0 = b - b \cdot (k \cdot h) = b \cdot 1_{\mathbf{A}} - b \cdot (k \cdot h) = b(1_{\mathbf{A}} - (k \cdot h))\,.$$

Se $b = 0$, è anche $a = 0$ e dunque $b = a \cdot 1_{\mathbf{A}}$ con $1_{\mathbf{A}}$ invertibile. Se $b \neq 0$, poiché in A per ipotesi non ci sono divisori dello zero deve essere

$$1_{\mathbf{A}} - (k \cdot h) = 0$$

ossia

$$1_{\mathbf{A}} = k \cdot h \quad (= h \cdot k, \text{ perché per ipotesi A è un anello commutativo})$$

cosicché h e k sono elementi invertibili di A, come si voleva dimostrare.

$(ii) \Rightarrow (iii)$.

Poiché h è invertibile, esiste $k \in$ A tale che $hk = kh = 1_{\mathbf{A}}$. Dalla (ii), moltiplicando a destra ambo i membri per k, si ricava allora che

$$bk = (a \cdot h) \cdot k = a \cdot (h \cdot k) = a \cdot 1_{\mathbf{A}} = a$$

cioè la (iii).

$(iii) \Rightarrow (i)$.

La (iii) esprime il fatto che $b|a$, quindi dobbiamo soltanto provare che $a|b$. Poiché k è invertibile, esiste $h \in$ A tale che $kh = 1_{\mathbf{A}}$. Dalla (iii), moltiplicando a destra per h, si ricava allora che

$$ah = (b \cdot k) \cdot h = b \cdot (k \cdot h) = b \cdot 1_{\mathbf{A}} = b$$

cioè $a|b$ come si voleva.

Corollario 8.6.3

Siano $a, b \in \mathbb{Z}$, con $a \neq 0$ e $b \neq 0$. Se $a|b$ e $b|a$, si ha $a = \pm b$.

Dimostrazione – Infatti in $\mathbb{Z}$ gli unici elementi invertibili sono 1 e -1.

8.7 - Elementi irriducibili negli anelli commutativi con unità privi di divisori dello zero.

Le definizioni di "numero irriducibile" e "numero primo" che abbiamo introdotto per i numeri naturali nella sez. 8.1 si estendono facilmente agli anelli commutativi con unità (cfr. sez. 4.8) che siano privi di divisori dello zero.

Sia A un anello commutativo con unità privo di divisori dello zero.Sia h un elemento invertibile di A, e sia $k \in$ A tale che $hk = 1_{\mathbf{A}}$. Per ogni $z \in$ A, si ha

$$z = z \cdot 1_{\mathbf{A}} = z \cdot (h \cdot k) = (z \cdot h) \cdot k$$

da cui, ricordando che in A il prodotto è commutativo, si deduce che

– ogni elemento invertibile di A divide z;

– ogni prodotto tra z e un elemento invertibile di A divide z.

Se si ottengono così tutti i divisori di z, si dice che z è *irriducibile*. In altre parole, un elemento z di A si dice irriducibile se i suoi unici divisori sono gli elementi invertibili di A e i prodotti fra z stesso e un elemento invertibile di A.

Un elemento a di A si dice *riducibile* se non è irriducibile, cioè se ha un divisore $d \in$ A che non è invertibile né è il prodotto di a per un elemento invertibile di A. In tal caso esiste $q \in$ A tale che $a = dq$ ed è facile dimostrare che anche q non è invertibile né è il prodotto di a per un elemento invertibile.

8.8 - Elementi primi negli anelli commutativi con unità privi di divisori dello zero.

Sia A un anello commutativo con unità privo di divisori dello zero.

Un elemento p di A diverso da 0 e da $1_{\mathbf{A}}$ si dice *primo* se

comunque presi $a, b \in$ A, se p divide il prodotto ab e p non divide a allora p divide b.

Teorema 8.8.1

Sia A un anello commutativo con unità privo di divisori dello zero, e sia $p \in \mathrm{A}$, $p \neq 0, 1_{\mathbf{A}}$.

Se p è primo, allora p è irriducibile.

Dimostrazione – Sia p primo, e mostriamo che p è irriducibile, cioè che ogni divisore di p è un elemento invertibile di A oppure è il prodotto fra p e un elemento invertibile di A.

Se d è un divisore di p, deve essere

$$p = dq \quad \text{con } q \in \mathrm{A}.$$

Poiché p divide p (oss. 7.6.1), ci sono due possibilità:

(i) p divide d;

(ii) p non divide d, quindi p divide q (perché p è primo).

Se vale la (i), per l'osservazione 7.6.2 esiste un elemento invertibile h di A tale che $d = ph$, e non c'è altro da dimostrare. Se vale la (ii), poiché per ipotesi q divide p possiamo ancora applicare l'osservazione 7.6.2 per concludere che esiste un elemento invertibile h di A tale che $q = ph$, cosicché (ricordando che il prodotto in A è commutativo)

$$p = dq = dph = pdh$$

e quindi

$$0 = p - pdh = p1_{\mathbf{A}} - pdh = p(1_{\mathbf{A}} - dh)\,.$$

Poiché per ipotesi $p \neq 0$, e poiché in A non ci sono divisori dello zero, deve essere

$$1_{\mathbf{A}} - dh = 0$$

ossia

$$dh = 1_{\mathbf{A}}$$

cosicché (ricordando che il prodotto in A è commutativo) d è invertibile.

Esempio 8.8.2

Sia $\mathcal{E}$ l'insieme dei polinomi nell'indeterminata ϑ a coefficienti in $\mathbb{Z}$ di grado non superiore a 1, cosicché gli elementi di $\mathcal{E}$ sono della forma

$$a + b\vartheta \quad \text{con} \quad a, b \in \mathbb{Z}\,.$$

Definiamo in $\mathcal{E}$ un prodotto ponendo

$$(a + b\vartheta)(c + d\vartheta) := (ac - 3bd) + (ad + bc)\vartheta$$

(si tratta in sostanza dell'usuale prodotto fra polinomi con la particolare convenzione aggiuntiva che $\vartheta \cdot \vartheta = -3$). Rispetto all'usuale somma fra polinomi e al prodotto così definito, $\mathcal{E}$ è un anello commutativo nel quale il numero intero 1 è l'unità (si lascia al lettore di buona volontà e un po' masochista la semplice ma assai noiosa verifica).

Mostriamo adesso che

(i) $\mathcal{E}$ non ha divisori dello zero;

(ii) 2 è irriducibile in $\mathcal{E}$;

(iii) 2 non è primo in $\mathcal{E}$.

Questo servirà per convincersi che, in opportuni anelli commutativi con unità privi di divisori dello zero, esistono elementi irriducibili che non sono primi.

proviamo la (i)

Siano $a+b\vartheta, c+d\vartheta \in \mathcal{E}$ tali che $(a+b\vartheta)(c+d\vartheta)=0$. Ciò significa, per definizione di prodotto fra elementi di $\mathcal{E}$, che

$$ac-3bd=0$$

$$ad+bc=0\,.$$

Dalla seconda uguaglianza si ricava che $ad=-bc$. Dalla prima uguaglianza si ricava che $ac=3bd$; moltiplicando ambo i membri per d e sostituendo $-bc$ ad ad si trova che

$$-bc^2=3bd^2 \qquad \text{ossia} \qquad 0=bc^2+3bd^2=b(c^2+3d^2)\,.$$

Se $a=b=0$, $a+b\vartheta=0$ e non c'è altro da dimostrare. Se $b=0$ e $a\neq 0$, dalle prime due uguaglianze si ricava che $c=d=0$, cosicché $c+d\vartheta=0$ e non c'è altro da dimostrare. Possiamo dunque supporre $b\neq 0$, cosicché $c^2+3d^2=0$; ma per le note proprietà dei numeri interi (di fatto, più in generale di tutti i numeri reali) ciò significa che $c=d=0$ e quindi $c+d\vartheta=0$ come si voleva.

proviamo la (ii)

Sia $a+b\vartheta$ un divisore di 2 in $\mathcal{E}$; ciò significa che esiste $c+d\vartheta\in\mathcal{E}$ tale che $2=(a+b\vartheta)(c+d\vartheta)$. Dunque, per definizione di prodotto fra elementi di $\mathcal{E}$, deve essere

$$ac-3bd=2$$

$$ad+bc=0\,.$$

Sia δ un divisore comune (in $\mathbb{Z}$) di a e b, cosicché $a=a_1\delta$ e $b=b_1\delta$ con $a_1, b_1\in\mathbb{Z}$. Allora

$$2=ac-3bd=a_1\delta c-3b_1\delta d=\delta(a_1c-3b_1d)$$

quindi $\delta=\pm 2$ oppure $\delta=\pm 1$.

Se $\delta=\pm 2$, la relazione $2=(a+b\vartheta)(c+d\vartheta)$ diventa

$$2=(a+b\vartheta)(c+d\vartheta)=\pm 2(a_1+b_1\vartheta)(c+d\vartheta)$$

da cui si ricava che $$1=\pm(a_1+b_1\vartheta)(c+d\vartheta)$$

e in particolare che $a_1+b_1\vartheta$ è un elemento invertibile di $\mathcal{E}$ e quindi $a+b\vartheta=\pm 2(a_1+b_1\vartheta)$ con $a_1+b_1\vartheta$ invertibile.

Ragionando allo stesso modo su un divisore comune δ_1 di c e d si trova che deve essere $\delta_1=\pm 2$ oppure $\delta_1=\pm 1$, e se $\delta_1=\pm 2$ allora $a+b\vartheta$ è invertibile.

Resta da valutare la possibilità che sia $\delta = \pm 1$ e $\delta_1 = \pm 1$ cosicché

$$\text{MCD}(|a|, |b|) = \text{MCD}(|c|, |d|) = 1 .$$

Poiché $ad = -bc$, e quindi $|a||d| = |b||c|$, per il teor.7.3.6

– dal fatto che $\text{MCD}(|a|, |b|) = 1$ segue che $|a|$ divide $|c|$ e $|b|$ divide $|d|$;

– dal fatto che $\text{MCD}(|c|, |d|) = 1$ segue che $|c|$ divide $|a|$ e $|d|$ divide $|b|$.

Dunque (cfr. oss. 6.2.4) $|a| = |c|$ e $|b| = |d|$, ossia $c = \pm a$ e $d = \pm b$.

Se $c = a$ e $d = b$ (oppure $c = -a$ e $d = -b$), l'uguaglianza $ad + bc = 0$ diventa

$$\pm 2ab = 0$$

cosicché $a = 0$ oppure $b = 0$.

Non può essere $a = 0$, perché la $ac - 3bd = 2$ diventerebbe $-3b^2 = 2$, assurdo; ma non può essere nemmeno $b = 0$, perché la $ac - 3bd = 2$ diventerebbe $a^2 = 2$, ancora assurdo.

Se invece $c = -a$ e $d = b$ (oppure $c = a$ e $d = -b$), l'uguaglianza $ac - 3bd = 2$ diventa $-a^2 - 3b^2 = 2$ (ma sappiamo che ciò è impossibile) oppure $a^2 + 3b^2 = 2$, e ricordando che $a, b \in \mathbb{Z}$ anche questa uguaglianza è impossibile.

proviamo la (iii)

Si ha

$$(1 + \vartheta) \cdot (1 - \vartheta) = 4 = 2 \cdot 2$$

dunque 2 divide $(1 + \vartheta) \cdot (1 - \vartheta)$; ma 2 non divide né $1 + \vartheta$ né $1 - \vartheta$, cosicché 2 non è primo.

Se fosse infatti

$$1 \pm \vartheta = 2 \cdot (a + b\vartheta) = 2a + 2b\vartheta \qquad \text{con} \quad a + b\vartheta \in \mathcal{E}$$

dovrebbe essere $2a = 1$ con $a \in \mathbb{Z}$, assurdo perché 2 non è invertibile in $\mathbb{Z}$.

Esempio 8.8.3

Sia $\mathcal{E}$ l'insieme dei polinomi nell'indeterminata ϑ a coefficienti in $\mathbb{Z}$ di grado non superiore a 1, con l'usuale somma fra polinomi e il prodotto definito nell'esempio 8.8.2:

$$(a + b\vartheta)(c + d\vartheta) := (ac - 3bd) + (ad + bc)\vartheta .$$

Abbiamo visto (nel citato esempio 8.8.2) che rispetto a ali operazioni $\mathcal{E}$ è un anello commutativo provo di divisori dello zero nel quale il numero intero 1 è l'unità. Mostriamo adesso che gli unici elementi invertibili di $\mathcal{E}$ sono 1 e -1 .

Sia $a+b\vartheta$ un elemento invertibile di $\mathcal{E}$; ciò significa che esiste $c+d\vartheta \in \mathcal{E}$ tale che $(a+b\vartheta)(c+d\vartheta)=1$. Dunque, per definizione di prodotto fra elementi di $\mathcal{E}$, deve essere

$$ac-3bd=1$$

$$ad+bc=0\,.$$

Sia δ un divisore comune (in $\mathbb{Z}$) di a e b, cosicché $a=a_1\delta$ e $b=b_1\delta$ con $a_1, b_1 \in \mathbb{Z}$. Allora

$$1=ac-3bd=a_1\delta c-3b_1\delta d=\delta(a_1c-3b_1d)$$

quindi $\delta=\pm 1$ e MCD$(|a|,|b|)=1$. Poiché $ad=-bc$, e quindi $|a||d|=|b||c|$, per il teor.7.3.6 $|a|$ divide $|c|$ e $|b|$ divide $|d|$.

Ragionando allo stesso modo su c e d si trova che MCD$(|c|,|d|)=1$ e quindi $|c|$ divide $|a|$ e $|d|$ divide $|b|$. Dunque (cfr. oss. 6.2.4) $|a|=|c|$ e $|b|=|d|$, ossia $c=\pm a$ e $d=\pm b$.

Se $c=a$ e $d=b$ (oppure $c=-a$ e $d=-b$), l'uguaglianza $ad+bc=0$ diventa

$$\pm 2ab=0$$

cosicché $a=0$ oppure $b=0$.

Non può essere $a=0$, perché la $ac-3bd=1$ diventerebbe $-3b^2=1$, assurdo. Dunque $b=0$, e la $ac-3bd=1$ diventa $a^2=1$ e in conclusione $a+b\vartheta=\pm 1$.

Se invece $c=-a$ e $d=b$ (oppure $c=a$ e $d=-b$), l'uguaglianza $ac-3bd=1$ diventa $-a^2-3b^2=1$ (ma sappiamo che ciò è impossibile) oppure $a^2+3b^2=1$, e ricordando che $a, b \in \mathbb{Z}$ può solo essere $b=0$ e $a^2=1$, cioè ancora una volta $a+b\vartheta=\pm 1$.

9.- RETICOLI

9.1 - Definizione.

Sia **L** un insieme, e sia $\preceq$ una relazione di ordine in **L** (cfr. 6.2).

Si dice che **L** *è un reticolo rispetto a* $\preceq$, oppure (più correttamente!) che *l'insieme ordinato* (**L**, $\preceq$) *è un reticolo* (in inglese: *lattice*), se

9.1.R1 comunque presi $x, y \in \mathbf{L}$, esistono in **L** **sup** $\{x, y\}$ e **inf** $\{x, y\}$ (cfr. 6.7 e 6.8).

Esempi

Sono esempi di reticoli:

9.1.1 Qualunque insieme in cui sia data una relazione di ordine totale, rispetto ad essa (quindi ad esempio $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ rispetto all'usuale relazione $\leq$). Si tratta però di esempi banali, perché in tutti questi casi **sup** $\{x, y\}$ è uno dei due elementi x, y e **inf** $\{x, y\}$ è l'altro.

9.1.2 L'insieme $\mathbb{N}$ rispetto alla relazione $|$ ("divide", cfr. oss. 6.2.4). In questo caso **sup** $\{x, y\}$ è il minimo comune multiplo fra x e y, e **inf** $\{x, y\}$ è il massimo comun divisore fra x e y.

9.1.3 Se **I** è un qualsiasi insieme (non vuoto), l'insieme $\mathcal{P}$(**I**) dei sottoinsiemi di **I** rispetto alla relazione $\subseteq$ (di "inclusione", cfr. esempio 6.2.3). In questo caso, **sup** $\{x, y\} = x \cup y$, e **inf** $\{x, y\} = x \cap y$.

9.2 - Unione e intersezione in un reticolo.

Ricordiamo che, in conseguenza del teorema 6.4.1, se esistono l'estremo superiore e l'estremo inferiore di un sottoinsieme essi sono unici (lo si è già osservato in 6.7 e 6.8). Dunque, se (**L**, $\preceq$) è un reticolo restano definite in **L** due operazioni come segue:

$x \vee y \coloneqq$ **sup** $\{x, y\}$;

$x \wedge y \coloneqq$ **inf** $\{x, y\}$.

La $\vee$ si dice *unione* (in caso di ambiguità: *unione reticolare*), e la $\wedge$ si dice *intersezione* (in caso di ambiguità: *intersezione reticolare*). Si noti che nell'esempio 9.1.3 le operazioni $\vee$ e $\wedge$ coincidono proprio con l'usuale unione tra insiemi $\cup$ e l'usuale intersezione tra insiemi $\cap$.

Lemma 9.2.1

Sia (**L**, $\preceq$) un reticolo, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in **L**. Comunque presi $x, y, z \in \mathbf{L}$,

(i) se $x \preceq y$ e $x \preceq z$, allora $x \preceq (y \wedge z)$;

(ii) se $x \preceq (y \wedge z)$, allora $x \preceq y$ e $x \preceq z$;

(iii) se $x \preceq z$ e $y \preceq z$, allora $(x \vee y) \preceq z$;

(iv) se $(x \vee y) \preceq z$, allora $x \preceq z$ e $y \preceq z$.

Dimostrazione – Proviamo la (i): se $x \preceq y$ e $x \preceq z$, x è una limitazione inferiore per $\{y, z\}$ e dunque $x \preceq \mathbf{inf}\,\{y, z\} = y \wedge z$.

Proviamo la (ii): poiché $y \wedge z$ è in particolare una limitazione inferiore per $\{y, z\}$, si ha che $(y \wedge z) \preceq y$ e $(y \wedge z) \preceq z$; dalla proprietà transitiva di $\preceq$ segue l'asserto.

Proviamo la (iii): se $x \preceq z$ e $y \preceq z$, z è una limitazione superiore per $\{y, x\}$ e dunque $x \vee y = \mathbf{sup}\,\{x, y\} \preceq z$.

Proviamo infine la (iv): poiché $x \vee y$ è in particolare una limitazione superiore per $\{x, y\}$, si ha che $x \preceq (x \vee y)$ e $y \preceq (x \vee y)$; dalla proprietà transitiva di $\preceq$ segue l'asserto.

Lemma 9.2.2

Sia (**L**, $\preceq$) un reticolo, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in **L**. Comunque presi $x, y, z \in \mathbf{L}$, sono fatti equivalenti:

(i) $x \preceq y$;

(ii) $x \wedge y = x$;

(iii) $x \vee y = y$.

Dimostrazione –

(i) $\Leftrightarrow$ (ii) Se $x \preceq y$ l'insieme $\{x, y\}$ è totalmente ordinato e ha minimo x; tale minimo è anche estremo inferiore (per il teorema 6.8.1) e dunque $x \wedge y = x$; viceversa, se $x \wedge y = x$ allora x è l'estremo inferiore dell'insieme $\{x, y\}$, dunque in particolare è una limitazione inferiore per l'insieme $\{x, y\}$: ne segue che $x \preceq y$.

(i) $\Leftrightarrow$ (iii) Se $x \preceq y$ l'insieme $\{x, y\}$ è totalmente ordinato e ha massimo x; tale massimo è anche estremo superiore (per il teorema 6.7.1) e dunque $x \vee y = y$; viceversa, se $x \vee y = y$ allora y è l'estremo superiore dell'insieme $\{x, y\}$, dunque in particolare è una limitazione superiore per l'insieme $\{x, y\}$: ne segue che $x \preceq y$.

Teorema 9.2.3

Sia (**L**, $\preceq$) un reticolo. Le operazioni $\vee$ e $\wedge$ definite in **L** godono delle seguenti proprietà:
(i) (*idempotenza*) $x \wedge x = x$ e $x \vee x = x$, $\forall x \in \mathbf{L}$;
(ii) (*propr. commutativa*) $x \wedge y = y \wedge x$ e $x \vee y = y \vee x$, $\forall x, y \in \mathbf{L}$;
(iii) (*propr. associativa*)
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$ e $(x \vee y) \vee z = x \vee (y \vee z)$, $\forall x, y \in \mathbf{L}$;
(iv) (*legge di assorbimento*) $(x \wedge y) \vee x = x$ e $(x \vee y) \wedge x = x$, $\forall x, y \in \mathbf{L}$.

Dimostrazione –

La (i) è immediata perché x è sia il minimo che il massimo (dunque, per i teoremi 6.7.1 e 6.8.1, sia l'estremo inferiore che l'estremo superiore) per l'insieme $\{x\}$.

Anche la (ii) è immediata, perché $\{x, y\} = \{y, x\}$ $\forall x, y \in \mathbf{L}$.

Proviamo la (iii) per l'operazione $\wedge$ lasciando per esercizio la dimostrazione (del tutto analoga) relativa all'operazione $\vee$. Poniamo, per fissare le idee, $h := (x \wedge y) \wedge z$ e $k := x \wedge (y \wedge z)$. Poiché $h \preceq h$, per la (ii) del lemma 9.2.1 deve essere $h \preceq (x \wedge y)$ (da cui ancora $h \preceq x$ e $h \preceq y$) e $h \preceq z$: dunque $h \preceq x$, $h \preceq y$ e $h \preceq z$; per la (i) del lemma 9.2.1 deve essere allora $h \preceq (y \wedge z)$ e infine $h \preceq x \wedge (y \wedge z) = k$. Viceversa, poiché $k \preceq k$, per la (ii) del lemma 9.2.1 deve essere $k \preceq x$ e $k \preceq (y \wedge z)$ (da cui ancora $k \preceq y$ e $k \preceq z$): dunque $k \preceq x$, $k \preceq y$ e $k \preceq z$; per la (i) del lemma 9.2.1 deve essere allora $k \preceq (x \wedge y)$ e infine $k \preceq (x \wedge y) \wedge z = h$. Abbiamo così provato che $h \preceq k$ e $k \preceq h$, cosicché (per la proprietà antisimmetrica) $h = k$ come si voleva dimostrare.

Infine, poiché $x \wedge y \preceq x$, la prima delle (iv) segue immediatamente dal lemma 9.2.2; e, poiché $x \preceq x \vee y$, la seconda delle (iv) segue (dalla proprietà commutativa e) dal lemma 9.2.2.

9.3 - Una definizione alternativa di "reticolo".

Le operazioni $\wedge$ e $\vee$ e le loro proprietà (i), (ii), (iii) e (iv) espresse nell'enunciato del teorema 9.2.3 caratterizzano completamente un reticolo. In questa sezione dimostriamo infatti che: se in un insieme **L** sono definite due operazioni $\wedge$ e $\vee$ idempotenti, commutative, associative e assorbenti, a partire da esse si può definire in **L** una relazione di ordine $\preceq$ tale che

(i) (**L**, $\preceq$) è un reticolo;

(ii) $\mathbf{sup}\{x, y\} = x \vee y$ e $\mathbf{inf}\{x, y\} = x \wedge y$ $\forall x, y \in \mathbf{L}$.

Teorema 9.3.1

Sia **L** un insieme, e siano $\wedge$, $\vee$ operazioni in **L** tali che

(*idempotenza*) $x \wedge x = x$ e $x \vee x = x$, $\forall x \in \mathbf{L}$;
(*propr. commutativa*) $x \wedge y = y \wedge x$ e $x \vee y = y \vee x$, $\forall x, y \in \mathbf{L}$;
(*propr. associativa*) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ e $(x \vee y) \vee z = x \vee (y \vee z)$, $\forall x, y, z \in \mathbf{L}$;
(*legge di assorbimento*) $(x \wedge y) \vee x = x$ e $(x \vee y) \wedge x = x$, $\forall x, y \in \mathbf{L}$.

Allora si ha

(*) $\qquad x \wedge y = x \quad$ se e soltanto se $\quad x \vee y = y \qquad \forall x, y \in \mathbf{L}$ **;**

Inoltre, posto

(°) $\qquad x \preceq y \quad$ se e soltanto se $\quad x \wedge y = x \qquad \forall x, y \in \mathbf{L}$

si ha che

(i) la $\preceq$ è una relazione di ordine in **L**

(ii) comunque presi $x, y \in$ L, esistono **inf** $\{x, y\}$ e **sup** $\{x, y\}$ e si ha

$$\textbf{inf}\,\{x, y\} = x \wedge y, \qquad \textbf{sup}\,\{x, y\} = x \vee y\,.$$

Dimostrazione –

Proviamo in primo luogo la (*). Siano $x, y \in \mathbf{L}$. Se $x \wedge y = x$, allora, tenendo conto della proprietà commutativa di $\wedge$, per la legge di assorbimento

$$x \vee y = (x \wedge y) \vee y = (y \wedge x) \vee y = y\,.$$

Se, viceversa, $x \vee y = y$, allo stesso modo si ha che

$$x \wedge y = x \wedge (x \vee y) = (x \vee y) \wedge x = x\,.$$

Adesso proviamo che la relazione $\preceq$ definita mediante la (°) è una relazione di ordine in **L**. È riflessiva per l'idempotenza di $\wedge$ e antisimmetrica per la commutatività di $\wedge$; se poi $x \preceq y$ (cioè $x \wedge y = x$) e $y \preceq z$ (cioè $y \wedge z = y$), si ha (ricordando la proprietà associativa)

$$x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$$

e dunque $x \preceq z$, cosicché vale anche la proprietà transitiva.

Proviamo ora che, comunque presi $x, y \in \mathbf{L}$, $\{x, y\}$ ha estremo inferiore e

$$\textbf{inf}\,\{x, y\} = x \wedge y\,.$$

Per la legge di assorbimento si ha che $(x \wedge y) \vee x = x$ e (tenendo conto anche della proprietà commutativa) $(x \wedge y) \vee y = y$; dunque $(x \wedge y) \preceq x$ e $(x \wedge y) \preceq y$, cosicché $x \wedge y$ è una limitazione inferiore per $\{x, y\}$. Se z è una qualsiasi limitazione inferiore per $\{x, y\}$, deve essere $z \preceq x$ (ossia $z \wedge x = z$) e $z \preceq y$ (ossia $z \wedge y = z$), cosicché

$$z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$$

ossia $z \preceq (x \wedge y)$; dunque $x \wedge y$ è la massima limitazione inferiore di $\{x, y\}$, come si voleva dimostrare.

Proviamo infine che, comunque presi $x, y \in \mathbf{L}$, $\{x, y\}$ ha estremo superiore e

$$\textbf{sup}\,\{x, y\} = x \vee y\,.$$

Per la legge di assorbimento (e la proprietà commutativa) si ha che $x \wedge (x \vee y) = x$ e $y \wedge (x \vee y) = y$; dunque $x \preceq (x \vee y)$ e $y \preceq (x \vee y)$, cosicché $x \vee y$ è una limitazione superiore per $\{x, y\}$. Se z è una qualsiasi limitazione superiore per $\{x, y\}$, deve essere $x \preceq z$ (ossia $x \vee z = z$) e $y \preceq z$ (ossia $y \vee z = z$), cosicché

$$(x \vee y) \vee z = x \vee (y \vee z) = x \vee z = z$$

ossia $(x \vee y) \preceq z$; dunque $x \vee y$ è la minima limitazione superiore di $\{x, y\}$, come si voleva dimostrare.

9.4 - Complementi in un reticolo.

Sia (**L**, $\preceq$) un reticolo, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in **L** .

Teorema 9.4.1

Sia (**L**, $\preceq$) un reticolo. Se in **L** c'è un elemento minimale, esso è il minimo di **L** . Se in **L** c'è un elemento massimale, esso è il massimo di **L** .

Dimostrazione – Sia m un elemento minimale di **L** (cfr. sez. 6.5) ; proviamo che m è il minimo di **L** . Se x è un elemento di **L**, è $x \wedge m \preceq m$ (per definizione di $\wedge$) e dunque $m \wedge x = m$ (perché m è un elemento minimale di **L**); dunque $m \preceq x$ (per la (i) del teorema). Ciò prova che m è il minimo di **L** .

In modo del tutto analogo si prova che: se in **L** c'è un elemento massimale, esso è il massimo di **L** ; questa dimostrazione si lascia per esercizio.

In questa sezione supporremo che **L** *abbia minimo* **0** *e massimo* **1** .

Osservazione 9.4.2

Benché l'uso di **0** e **1** per indicare rispettivamente il minimo e il massimo di un reticolo sia abbastanza standard, ci sono occasioni in cui può essere fuorviante. Il reticolo ricordato nell'esempio 9.1.2 ha minimo e massimo, ma il suo minimo è il numero naturale 1 e il suo massimo è il numero naturale 0.

Sia $x \in \mathbf{L}$. Si dice *complemento* di x un elemento $x^c \in \mathbf{L}$ tale che sia

$$x \wedge x^c = \mathbf{0} \quad \text{e} \quad x \vee x^c = \mathbf{1} .$$

Osservazione 9.4.3

Gli elementi **0** e **1** hanno sempre uno e un solo complemento (rispettivamente **1** e **0**).

Esempio 9.4.4

Nel reticolo definito in $\mathbb{N}$ dalla relazione "divide" (cfr. esempio 9.1.2) nessun elemento (tranne il minimo e il massimo) ha complemento.

Esempio 9.4.5

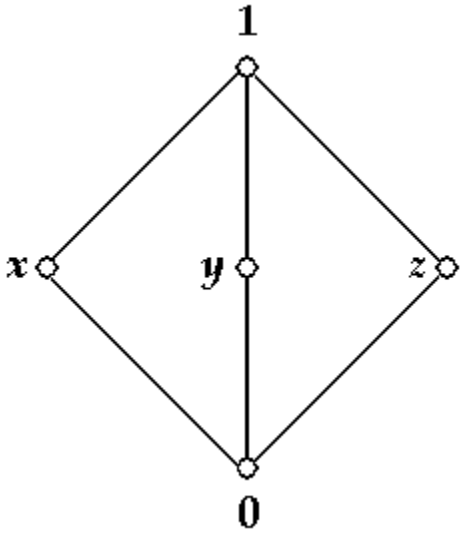
Sia **I** un insieme non vuoto. Nel reticolo definito in $\mathcal{P}$(**I**) dalla relazione di inclusione (cfr. esempio 9.1.3) il minimo è $\emptyset$, il massimo è **I**, e ogni elemento ha per complemento il suo complementare (in senso insiemistico, cfr. la sez. 1.10) rispetto a **I** .

Esempio 9.4.6

Sia $\mathbf{L} := \{\mathbf{0}, x, y, z, \mathbf{1}\}$ e sia $\preceq$ la relazione in $\mathbf{L}$ definita ponendo

$\mathbf{0} \preceq \mathbf{0}$, $\mathbf{0} \preceq x$, $\mathbf{0} \preceq y$, $\mathbf{0} \preceq z$, $\mathbf{0} \preceq \mathbf{1}$, $x \preceq x$, $x \preceq \mathbf{1}$, $y \preceq y$, $y \preceq \mathbf{1}$, $z \preceq z$, $z \preceq \mathbf{1}$, $\mathbf{1} \preceq \mathbf{1}$.

Ognuno dei tre elementi x, y, z ha per complemento ciascuno degli altri due.



9.5 - Distributività.

Teorema 9.5.1

Sia $(\mathbf{L}, \preceq)$ un reticolo, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in $\mathbf{L}$. Sono fatti equivalenti:

(i) $\quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \qquad \forall x, y, z \in \mathbf{L}$;

(ii) $\quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \qquad \forall x, y, z \in \mathbf{L}$.

In altri termini: in un reticolo, $\wedge$ è distributiva rispetto a $\vee$ se e soltanto se $\vee$ è distributiva rispetto a $\wedge$.

Dimostrazione – $(i) \Rightarrow (ii)$:

$$(x \vee y) \wedge (x \vee z) \overset{(i)}{=} ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \overset{\text{(idemp.)}}{=} x \vee ((x \vee y) \wedge z) \overset{\text{(comm.)}}{=}$$
$$\overset{\text{(comm.)}}{=} x \vee (z \wedge (x \vee y)) \overset{(i)}{=} x \vee ((z \wedge x) \vee (z \wedge y)) \overset{\text{(assoc.)}}{=} (x \vee (z \wedge x)) \vee (z \wedge y) \overset{\text{(idemp.)}}{=}$$
$$\overset{\text{(idemp.)}}{=} x \vee (z \wedge y) \overset{\text{(comm.)}}{=} x \vee (y \wedge z).$$

$(ii) \Rightarrow (i)$:

$$(x \wedge y) \vee (x \wedge z) \overset{(ii)}{=} ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee z) \overset{\text{(idemp.)}}{=} x \wedge ((x \wedge y) \vee z) \overset{\text{(comm.)}}{=}$$
$$\overset{\text{(comm.)}}{=} x \wedge (z \vee (x \wedge y)) \overset{(ii)}{=} x \wedge ((z \vee x) \wedge (z \vee y)) \overset{\text{(assoc.)}}{=} (x \wedge (z \vee x)) \wedge (z \vee y) \overset{\text{(idemp.)}}{=}$$
$$\overset{\text{(idemp.)}}{=} x \wedge (z \vee y) \overset{\text{(comm.)}}{=} x \wedge (y \vee z).$$

Un reticolo si dice *distributivo* se in esso valgono le (i) e (ii) del teorema 9.5.1.

Teorema 9.5.2

Sia (**L**, $\preceq$) un reticolo, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in **L**. Comunque presi $x, y, z \in$ L, si ha:

(i) $(x \wedge y) \vee (x \wedge z) \preceq x \wedge (y \vee z)$;

(ii) $x \vee (y \wedge z) \preceq (x \vee y) \wedge (x \vee z)$.

Dimostrazione – Proviamo la (i). Per definizione di $\wedge$, $(x \wedge y) \preceq x$ e $(x \wedge y) \preceq y$; per definizione di $\vee$, $y \preceq (y \vee z)$. Per la proprietà transitiva di $\preceq$, $(x \wedge y) \preceq (y \vee z)$. Per la (i) del lemma 9.2.1, $(x \wedge y) \preceq x \wedge (y \vee z)$.

Analogamente, per definizione di $\wedge$ si ha che $(x \wedge z) \preceq x$ e $(x \wedge z) \preceq z$; per definizione di $\vee$, $z \preceq (y \vee z)$. Per la proprietà transitiva di $\preceq$, $(x \wedge z) \preceq (y \vee z)$. Per la (i) del lemma 9.2.1, $(x \wedge z) \preceq x \wedge (y \vee z)$. Infine, per la (iii) del lemma 9.2.1,

$$(x \wedge y) \vee (x \wedge z) \preceq x \wedge (y \vee z)$$

cioè la (i).

Proviamo adesso la (ii). Per definizione di $\vee$, $x \preceq x \vee y$ e $x \preceq x \vee z$: dunque, per la (i) del lemma 9.2.1 si ha che $x \preceq (x \vee y) \wedge (x \vee z)$.

Per definizione di $\wedge$, $y \wedge z \preceq y$; per definizione di $\vee$, $y \preceq x \vee y$: per la proprietà transitiva di $\preceq$, $y \wedge z \preceq x \vee y$. Analogamente, per definizione di $\wedge$, $y \wedge z \preceq z$; per definizione di $\vee$, $z \preceq x \vee z$: per la proprietà transitiva di $\preceq$, $y \wedge z \preceq x \vee z$. Applicando ancora una volta la (i) del lemma 9.2.1, si ottiene che $y \wedge z \preceq (x \vee y) \wedge (x \vee z)$. Infine, per la (iii) del lemma 9.2.1,

$$x \vee (y \wedge z) \preceq (x \vee y) \wedge (x \vee z)$$

cioè la (ii).

Teorema 9.5.3

Sia (**L**, $\preceq$) un reticolo, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in **L**. Sono fatti equivalenti:

(a) $x \wedge (y \vee z) \preceq (x \wedge y) \vee (x \wedge z)$;
(b) $(x \vee y) \wedge (x \vee z) \preceq x \vee (y \wedge z)$;
(c) (**L**, $\preceq$) è un reticolo distributivo.

Dimostrazione – Se vale la (a), per la (i) del teorema 9.5.2 vale la (i) del teorema 9.5.1; ma allora vale anche la (ii) del teorema 9.5.1 e quindi vale la (b).

Se vale la (b), per la (ii) del teorema 9.5.2 vale la (ii) del teorema 9.5.1; ma allora vale anche la (i) del teorema 9.5.1 e quindi vale la (c).

Se vale la (c), per definizione vale la (i) del teorema 9.5.1 e quindi vale la (a).

Teorema 9.5.4

Sia ($\mathbf{L}$, $\preceq$) un reticolo distributivo con minimo $\mathbf{0}$ e massimo $\mathbf{1}$, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in $\mathbf{L}$. Ogni elemento di $\mathbf{L}$ ha al più un complemento.

Dimostrazione – Sia $x \in \mathbf{L}$; supponiamo che y e z siano entrambi complementi di x, e dimostriamo che $y = z$.

Per ipotesi, $y \vee x = \mathbf{1}$, $x \wedge y = \mathbf{0}$ (perché y è complemento di x), $z \vee x = \mathbf{1}$, $x \wedge z = \mathbf{0}$ (perché z è complemento di x). Allora

$$z = z \vee \mathbf{0} = z \vee (x \wedge y) = (z \vee x) \wedge (z \vee y) = \mathbf{1} \wedge (z \vee y) = z \vee y$$

ossia $y \preceq z$. Analogamente

$$y = y \vee \mathbf{0} = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z) = \mathbf{1} \wedge (y \vee z) = y \vee z$$

ossia $z \preceq y$. Dunque (per la proprietà antisimmetrica) $y = z$, come si voleva dimostrare.

Si dice *algebra di Boole* un reticolo distributivo nel quale ogni elemento ha (esattamente un) complemento.

Teorema 9.5.5

Sia ($\mathbf{B}$, $\preceq$) un'algebra di Boole con minimo $\mathbf{0}$ e massimo $\mathbf{1}$, e siano $\wedge$, $\vee$ le operazioni di intersezione e unione definite in $\mathbf{B}$. Valgono le cosiddette *leggi di De Morgan*:

(i) $(x \vee y)^c = x^c \wedge y^c$;

(ii) $(x \wedge y)^c = x^c \vee y^c$.

Dimostrazione – Proviamo la (i); la dimostrazione della (ii) è del tutto analoga, e si lascia per esercizio.

Per provare la (i), dobbiamo verificare che

$$(x \vee y) \wedge (x^c \wedge y^c) = \mathbf{0} \quad \text{e} \quad (x \vee y) \vee (x^c \wedge y^c) = \mathbf{1}.$$

In effetti,

$$(x \vee y) \wedge (x^c \wedge y^c) \overset{\text{(distribut.)}}{=} (x \wedge (x^c \wedge y^c)) \vee (y \wedge (x^c \wedge y^c)) \overset{\text{(assoc. e commut.)}}{=}$$

$$\overset{\text{(assoc. e commut.)}}{=} ((x \wedge x^c) \wedge y^c) \vee ((y \wedge y^c) \wedge x^c) = (\mathbf{0} \wedge y^c) \vee (\mathbf{0} \wedge x^c) =$$

$$= \mathbf{0} \vee \mathbf{0} = \mathbf{0}$$

e allo stesso modo

$$(x \vee y) \vee (x^c \wedge y^c) \overset{\text{(distribut.)}}{=} ((x \vee y) \vee x^c) \wedge ((x \vee y) \vee y^c) \overset{\text{(assoc. e commut.)}}{=}$$

$$\overset{\text{(assoc. e commut.)}}{=} ((x \vee x^c) \vee y) \wedge (x \vee (y \vee y^c)) = (\mathbf{1} \vee y) \wedge (x \vee \mathbf{1}) =$$

$$= \mathbf{1} \wedge \mathbf{1} = \mathbf{1}.$$

10.- RELAZIONI DI EQUIVALENZA

10.1 - Definizione.

Sia A un insieme.

Una relazione in A riflessiva, simmetrica e transitiva si dice una *relazione di equivalenza* in A .

Esempi

Sono esempi di relazioni di equivalenza:

10.1.1 La relazione di "equiscomponibilità" nell'insieme dei poligoni piani.

10.1.2 La relazione di "similitudine" nell'insieme delle figure piane.

10.1.3 La relazione di "parallelismo" nell'insieme delle rette del piano, definita come segue:
due rette sono parallele sse coincidono oppure non hanno punti in comune.

10.1.4 In ogni insieme A, la relazione (di "misantropia"?) che ad ogni elemento di A associa lui stesso e nessun altro (cioè: se $a, b \in$ A, a è in relazione con b sse $a = b$).

10.1.5 In ogni insieme A, la relazione (di "amore universale"?) che ad ogni elemento di A associa tutti gli elementi di A (cioè: comunque si prendano $a, b \in$ A, a è in relazione con b).

Esempio 10.1.6

Sia $\mathcal{F}$ l'insieme delle frazioni [19]. La relazione ϱ in $\mathcal{F}$ definita ponendo per $\frac{a}{b}, \frac{c}{d} \in \mathcal{F}$

$$\frac{a}{b} \varrho \frac{c}{d} \quad \text{sse} \quad ad = bc$$

è una relazione di equivalenza. Infatti:

ϱ è riflessiva: $\frac{a}{b} \varrho \frac{a}{b}$ per ogni $\frac{a}{b} \in \mathcal{F}$, perché $ab = ba$ (propr. commutat. del prodotto);

ϱ è simmetrica: $\frac{a}{b} \varrho \frac{c}{d} \Rightarrow \frac{c}{d} \varrho \frac{a}{b}$, perché $(ad = bc) \Rightarrow (cb = da)$;

ϱ è transitiva: sia infatti $\frac{a}{b} \varrho \frac{c}{d}$ e $\frac{c}{d} \varrho \frac{e}{f}$, cioè $ad = bc$ e $cf = de$; dalla prima uguaglianza segue $adf = bcf$ e da qui, tenendo conto della seconda, $adf = bde$; dividendo infine ambo i membri per d (che è diverso da 0 per ipotesi) si deduce che $af = be$ ossia che $\frac{a}{b} \varrho \frac{e}{f}$ come si voleva.

---

[19] Ricordiamo che si dice *frazione* una coppia ordinata (cfr. 1.5) di numeri interi in cui la seconda componente sia diversa da 0; si conviene di scrivere $\frac{a}{b}$ anziché (a, b).

10.2 - Classi di equivalenza.

Siano A un insieme e $\sim$ una relazione di equivalenza in A .

Se $a \in$ A, si dice *classe di* $\sim$ *– equivalenza* di a (o anche, quando ciò non dia luogo ad equivoci, *classe di equivalenza* di a) il sottoinsieme $[a]$ di A definito come segue:

$$[a] = \{x \in \text{A} \,/\, a \sim x\}.$$

Osservazione 10.2.1

Per ogni $a \in$ A, si ha $a \in [a]$.

Dimostrazione – Infatti $a \sim a$, perché $\sim$ è riflessiva.

Osservazione 10.2.2

Comunque presi $a, b \in$ A, si ha $[a] = [b]$ se e solo se $a \sim b$.

Dimostrazione – Se $[a] = [b]$, poiché $b \in [b]$ (per 10.2.1) si ha $b \in [a]$ e dunque $a \sim b$ (per definizione di $[a]$).

Viceversa, sia $a \sim b$; dobbiamo provare che $[a] \subset [b]$ e che $[b] \subset [a]$.

Sia $x \in [a]$; allora $a \sim x$. Ma $b \sim a$ (perché $a \sim b$ per ipotesi, e $\sim$ è simmetrica) e dunque $b \sim x$ (perché $\sim$ è transitiva), cioè $x \in [b]$. Per l'arbitrarietà di x in $[a]$, si è provato che $[a] \subset [b]$.

Sia ora $x \in [b]$; allora $b \sim x$. Poiché $a \sim b$ per ipotesi, e poiché $\sim$ è transitiva, si ha $a \sim x$, cioè $x \in [a]$. Per l'arbitrarietà di x in $[b]$, si è così anche provato che $[b] \subset [a]$ e dunque che $[a] = [b]$.

Osservazione 10.2.3

Sia $a \in$ A . Per ogni $x \in [a]$, è $[x] = [a]$.

Dimostrazione – Per definizione di $[a]$, se $x \in [a]$ è $a \sim x$; dunque $[a] = [x]$ per l'osservazione 10.2.2.

Sia $a \in$ A . Per ogni $x \in [a]$, si dice che x *rappresenta* $[a]$, o anche che x *è un rappresentante di* $[a]$. Ciò è giustificato da quanto si è visto nell'osservazione 10.2.3.

Osservazione 10.2.4

Comunque presi $a, b \in \mathrm{A}$, se $[a] \neq [b]$ è $[a] \cap [b] = \emptyset$.

Dimostrazione – Sia $[a] \neq [b]$. Procediamo per assurdo, supponendo che esista $x \in [a] \cap [b]$. In tal caso $a \sim x$ (perché $x \in [a]$) e $b \sim x$ (perché $x \in [b]$); per 10.2.2 si ha allora $[a] = [x] = [b]$, contro l'ipotesi.

Osservazione 10.2.5

L'insieme delle classi di equivalenza di A è una partizione di A.

Dimostrazione – Le classi di equivalenza sono a due a due disgiunte per 10.2.4; per 10.2.1 esse sono non vuote e la loro unione è A.

10.3 - Insieme quoziente.

Siano A un insieme e $\sim$ una relazione di equivalenza in A .

L'insieme delle classi di $\sim$ – equivalenza di A si dice *insieme quoziente* di A rispetto a $\sim$, e si indica con $\frac{\mathrm{A}}{\sim}$. La funzione (suriettiva) $\pi : \mathrm{A} \to \frac{\mathrm{A}}{\sim}$ che ad ogni elemento di A associa la sua classe di equivalenza si dice *proiezione canonica* di A su $\frac{\mathrm{A}}{\sim}$.

Se $\sim$ mette in relazione tra loro gli elementi di A che hanno in comune una certa proprietà astratta, l'insieme quoziente rappresenta intuitivamente l'insieme di tali proprietà astratte, e la proiezione canonica associa ad ogni elemento di A la specifica proprietà che gli è pertinente. Vediamo meglio in che senso ciò avviene, riesaminando gli esempi già considerati in 10.1.

10.3.1

Sia A l'insieme dei poligoni del piano, e sia $\sim$ la relazione di equiscomponibilità.

La proprietà astratta comune a una classe di poligoni equiscomponibili è la "superficie"([20]): tale concetto, in effetti, può essere definito per i poligoni appunto per questa via. La proiezione canonica $\mathrm{A} \to \frac{\mathrm{A}}{\sim}$ associa a ogni poligono la sua superficie.

[20] Non si confonda la nozione di "superficie" con quella di "area" (un numero reale che esprime la "misura" della superficie secondo una teoria matematica niente affatto elementare).

10.3.2

Sia A l'insieme delle figure piane, e sia $\sim$ la relazione di similitudine.

La proprietà astratta comune a una classe di figure piane simili è la "forma". Nell'insieme quoziente $\frac{A}{\sim}$ troviamo elementi che rappresentano i concetti di "triangolo equilatero", "quadrato", "cerchio", ecc.

10.3.3

Sia A l'insieme delle rette del piano, e sia $\sim$ la relazione di parallelismo definita in 10.1.3.

L'insieme quoziente $\frac{A}{\sim}$ si dice *insieme delle direzioni*.

10.3.4

Sia A un insieme, e sia $\sim$ la relazione di "misantropia" definita in 10.1.4.

L'insieme quoziente è (in corrispondenza biunivoca con) A .

10.3.5

Sia A un insieme, e sia $\sim$ la relazione definita in 10.1.5.

L'insieme quoziente è $\{A\}$.

10.3.6

Sia $\mathcal{F}$ l'insieme delle frazioni, e sia ϱ la relazione definita in 10.1.6.

L'insieme quoziente $\frac{\mathcal{F}}{\varrho}$ è (in corrispondenza biunivoca con) $\mathbb{Q}$. In effetti, i numeri razionali si definiscono appunto con questo procedimento a partire dall'insieme $\mathbb{Z}$ degli interi.

La proiezione canonica associa a ogni frazione il numero razionale che essa rappresenta.

10.4 - Le classi di resto.

In tutta la sezione 10.4 supporremo fissato un numero intero positivo n.

Siano $a, b \in \mathbb{Z}$; si dice che a *è congruo* b *modulo* n e si scrive

$$a \equiv b \pmod{n}$$

se e soltanto se

$$a - b \text{ è multiplo di } n$$

cioè (cfr. esempio 6.2.2) se e soltanto se esiste $k \in \mathbb{Z}$ tale che $a - b = kn$.

Si è così definita una relazione in $\mathbb{Z}$, detta "*congruenza modulo* n". Tale relazione è stata studiata fin dall'antichità: sono celebri le opere in proposito del matematico ellenista $\Delta\iota\grave{o}\varphi\alpha\nu\tau o\varsigma$, che abbiamo già citato nella sez. 7.4.

Teorema 10.4.1

La congruenza modulo n è una relazione di equivalenza in $\mathbb{Z}$.

Dimostrazione – In primo luogo, la congruenza modulo n è riflessiva, ossia

$$a \equiv a \pmod{n} \qquad \text{per ogni } a \in \mathbb{Z}.$$

Infatti, $a - a = 0 \cdot n$ con $0 \in \mathbb{Z}$.

Inoltre, la congruenza modulo n è simmetrica: siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e proviamo che $b \equiv a \pmod{n}$. In effetti, se $a \equiv b \pmod{n}$ esiste $k \in \mathbb{Z}$ tale che $a - b = kn$; ma allora $b - a = (-k)n$ con $-k \in \mathbb{Z}$, e dunque $b \equiv a \pmod{n}$.

Infine, la congruenza modulo n è transitiva: siano $a, b, c \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, e proviamo che $a \equiv c \pmod{n}$. In effetti, se $a \equiv b \pmod{n}$ esiste $k_1 \in \mathbb{Z}$ tale che $a - b = k_1 n$; se $b \equiv c \pmod{n}$ esiste $k_2 \in \mathbb{Z}$ tale che $b - c = k_2 n$; ma allora

$$a - c = (a - b) + (b - c) = k_1 n + k_2 n = (k_1 + k_2) \cdot n$$

con $k_1 + k_2 \in \mathbb{Z}$, e dunque $a \equiv c \pmod{n}$.

Per quanto provato nel teorema 10.4.1, se $a \equiv b \pmod{n}$ si può dire che a, b sono *congrui modulo* n senza porre attenzione all'ordine in cui si citano a e b.

Esercizio 10.4.2

Trovare due numeri interi che sono congrui modulo 5 ma non sono congrui modulo 10. Esistono due numeri interi che siano congrui modulo 10 ma non siano congrui modulo 5?

Teorema 10.4.3

Sia $a \in \mathbb{Z}$, e sia r il resto della divisione euclidea di a per n. Allora $a \equiv r \pmod{n}$.

Dimostrazione – Per la nozione di "divisione euclidea" estesa al caso in cui il dividendo appartiene a $\mathbb{Z}$ e il divisore appartiene a $\mathbb{Z}^+$ (cfr. teorema 7.2.5), esiste $q \in \mathbb{Z}$ tale che

$$a = qn + r$$

e dunque $a - r = qn$ con $q \in \mathbb{Z}$, da cui l'asserto.

Le classi di equivalenza rispetto alla relazione di congruenza modulo n si dicono *classi di resto modulo* n. L'insieme delle classi di resto modulo n (cioè l'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza modulo n) si indica con $\mathbb{Z}_n$.

Teorema 10.4.4

L'insieme $\mathbb{Z}_n$ ha n elementi, precisamente: $[0]$, $[1]$, $\ldots$, $[n-1]$.

Dimostrazione – Per il teorema 10.4.3, ogni numero intero appartiene a una delle classi $[0]$, $[1]$, $\ldots$, $[n-1]$. Resta da provare che tali classi sono tutte distinte.
Se fosse $[i] = [j]$ con $0 \leq i < j < n$, per l'osservazione 10.2.2 sarebbe $i \equiv j \pmod{n}$ ossia esisterebbe $k \in \mathbb{Z}$ tale che $j - i = kn$.
Ma $j - i > 0$ (perché $j > i$) e $j - i < n$ (perché $j < n$ e $i \geq 0$), dunque $j - i$ non può essere multiplo di n. Abbiamo così ottenuto una contraddizione; ne segue che le classi $[0]$, $[1]$, $\ldots$, $[n-1]$ sono tutte distinte, come si voleva.

Esercizio 10.4.5

Si deduca dai teoremi 10.4.3 e 10.4.4 che due numeri interi a, b sono congrui modulo n se e solo se la divisione euclidea di a per n e la divisione euclidea di b per n danno lo stesso resto.

Esercizio 10.4.6

Si studi la congruenza modulo 1, la congruenza modulo 2, la congruenza modulo 3, la congruenza modulo 10, la congruenza modulo 12 e la congruenza modulo 24; in particolare, per ciascuna di tali relazioni si scrivano esplicitamente le classi di resto e si precisi come opera la proiezione canonica.

10.5 - L'anello $\mathbb{Z}_n$.

In tutta la sezione 10.5 supporremo fissato un numero intero positivo n.

Definiamo nell'insieme $\mathbb{Z}_n$ (cfr. 10.4) due operazioni: le indicheremo con " $+$ " e " $\cdot$ ", e le chiameremo rispettivamente *somma* e *prodotto*. Se $[a], [b] \in \mathbb{Z}_n$, poniamo

$$[a] + [b] := [a + b]$$

e

$$[a] \cdot [b] := [a \cdot b].$$

Si noti che con lo stesso simbolo " $+$ " abbiamo indicato a sinistra l'operazione che stiamo definendo in $\mathbb{Z}_n$ e a destra la ben nota operazione di somma in $\mathbb{Z}$; analogamente per il simbolo " $\cdot$ " (che, per di piú, spesso si omette, proprio come in $\mathbb{Z}$). Ciò usualmente non dà luogo ad ambiguità né a confusione. Di fatto, per come abbiamo definito la somma e il prodotto in $\mathbb{Z}_n$, la proiezione canonica (cfr. sez. 10.3) risulta immediatamente essere un omomorfismo tra l'anello $\mathbb{Z}$ e l'anello $\mathbb{Z}_n$ (cfr. sez. 4.8).

Si noti inoltre che abbiamo definito la "somma" (e il "prodotto") di due classi di resto mediante la somma (o, rispettivamente, il prodotto) dei loro rappresentanti: poiché tali rappresentanti non sono univocamente determinati, è importante assicurarsi che la definizione sia "ben posta", ossia dipenda solo dalle classi considerate e non dai rappresentanti scelti in esse (cfr. l'esempio 3.4.1 e, più avanti, l'esempio 10.5.2). Ciò avviene mediante il

Teorema 10.5.1

Siano a, b, a', b' $\in \mathbb{Z}$. Se $[a] = [a']$ e $[b] = [b']$, allora $[a + b] = [a' + b']$ e $[ab] = [a'b']$.

Dimostrazione – Per l'osservazione 10.2.2, se $[a] = [a']$ e $[b] = [b']$ deve essere

$$a \equiv a' \pmod{n} \qquad \text{e} \qquad b \equiv b' \pmod{n},$$

ossia devono esistere $h, k \in \mathbb{Z}$ tali che

$$a - a' = hn \qquad \text{e} \qquad b - b' = kn.$$

Allora

$$(a + b) - (a' + b') = (a - a') + (b - b') = hn + kn = (h + k)n$$

e dunque

$$a + b \equiv a' + b' \pmod{n}$$

ossia, ancora per l'osservazione 10.2.2, $[a + b] = [a' + b']$ come si voleva dimostrare.

Inoltre,

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a') = akn + b'hn = (ak + b'h)n$$

e dunque

$$ab \equiv a'b' \pmod{n}$$

ossia, ancora per l'osservazione 10.2.2, $[ab] = [a'b']$ come si voleva dimostrare.

Esempio 10.5.2

Sia $n = 3$.
Si ha $[2] = [5]$, tuttavia $[2^2] = [1] \neq [2] = [2^5]$. Non sarebbe dunque possibile definire, analogamente a come si è fatto per somma e prodotto, un "elevamento a potenza" in $\mathbb{Z}_n$ ponendo $[a]^{[b]} := [a^b]$.
Analogamente, per $n = 5$, si ha $[3] = [8]$, tuttavia $[2^3] = [8] = [3] \neq [1] = [256] = [2^8]$.

Esempio 10.5.3

Sia $n = 6$.
Si ha $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$, cioè gli elementi $[2]$ e $[3]$ di $\mathbb{Z}_6$ sono divisori dello zero (cfr. sez. 4.8). Dunque in $\mathbb{Z}_6$ non vale la legge di annullamento del prodotto.

Esempio 10.5.4

Sia $n = 4$.
Si ha $[2] \cdot [2] = [2 \cdot 2] = [4] = [0]$; dunque in $\mathbb{Z}_4$ l'elemento $[2] \neq 0$ ha per quadrato 0. In particolare, l'elemento $[2]$ di $\mathbb{Z}_4$ è un divisore dello zero; e in $\mathbb{Z}_4$ non vale la legge di annullamento del prodotto.

Esempio 10.5.5

Sia $n = 3$.
Il polinomio $x^3 + [2]x$ si annulla per ogni elemento di $\mathbb{Z}_3$, ma non è il polinomio nullo.

Esempio 10.5.6

Sia $n = 6$.
Si ha $[4] = [4] \cdot [4] = [4] \cdot [4] \cdot [4] = [4] \cdot [4] \cdot \ldots [4]$.

Esercizio 10.5.7

Sia $n = 6$.
Risolvere, se è possibile, le seguenti equazioni in $\mathbb{Z}_6$ nell'incognita x:

$$\begin{array}{ll} [3] \cdot x = [2]; & [3] \cdot x = [3]; \\ [4] \cdot x = [2]; & [4] \cdot x = [3]; \\ [5] \cdot x = [1]; & [5] \cdot x = [2]; \\ x^2 = [2]; & x^2 = [3]; \\ x^2 + [1] = [0]; & x^2 + [2] = [0]; \end{array}$$

$$x^5 + [3] \cdot x^4 + x^3 + [3] \cdot x^2 + [4] \cdot x = [0].$$

Esercizio 10.5.8

Sia $n = 7$.
Risolvere, se è possibile, le seguenti equazioni in $\mathbb{Z}_7$ nell'incognita x:

$$\begin{array}{c} [3] \cdot x = [2]; \\ [4] \cdot x = [3]; \\ [5] \cdot x = [1]; \\ [5] \cdot x = [2]; \\ x^2 = [2]; \\ x^2 = [3]; \\ x^2 + [1] = [0]. \end{array}$$

10.6 - La notazione posizionale in base "dieci" e in altre basi.

Come "si chiamano" i numeri naturali? Come si indicano, oltre che col loro nome?

In base agli assiomi di Peano, c'è un numero che si chiama "zero"; inoltre, ogni numero ha un successivo, e questo ci permette di assegnare nomi ad altri numeri: si decide così di chiamare "uno" il successivo di "zero", "due" il successivo di "uno", ecc. ecc.. Questi nomi dipendono dalla lingua che si usa: "zero", "uno", "due" sono nomi di numeri nella lingua italiana ma non nella lingua tedesca o in altre lingue.

Per superare le barriere linguistiche, ma anche per poter utilizzare efficaci algoritmi di calcolo, è comodo indicare i numeri naturali con opportuni simboli grafici: è ad esempio molto diffuso l'uso dei simboli "0" e "1" per indicare rispettivamente i numeri "zero" e "uno" (però nei paesi arabi "zero" si indica col simbolo " · ") .

In questa sezione descriviamo la cosiddetta *notazione posizionale* per i numeri naturali: si tratta di una convenzione (straordinariamente efficace per lo sviluppo di algoritmi di calcolo) che dipende da un numero naturale b fissato, detto *base*, e consente di esprimere qualsiasi numero naturale mediante l'uso (eventualmente ripetuto) di al più b simboli. La più diffusa, e comunque quella adottata ovunque in questi appunti, è la notazione posizionale in base "dieci", chiamata anche *notazione decimale*; ma per certe applicazioni sono utilizzate altre notazioni posizionali: quella in base "due" (detta anche *binaria*), e quella in base "sedici" (detta anche *esadecimale*) .

Teorema 10.6.1

Sia b un numero naturale maggiore di 1.

(i) Per ogni $n \in \mathbb{N}$ esistono $k, c_0, c_1, \ldots, c_k \in \mathbb{N}$ tali che

(*) $\quad n = c_k b^k + c_{k-1} b^{k-1} + \ldots + c_1 b + c_0 \quad$ con $\quad 0 \leq c_i < b \quad$ e $\quad c_k \neq 0$ se $k > 0$;

(ii) Se vale la (*), detto q_j il quoziente della divisione euclidea di n per b^j, c_j è il resto della divisione euclidea di q_j per b, per $j := 1, \ldots, k$.

In particolare, i numeri naturali $k, c_0, c_1, \ldots, c_k$ per i quali vale la (*) sono univocamente determinati da n e da b.

Dimostrazione -

Proviamo la (i) per induzione su n, applicando il teorema 2.5.2. Se $n < b$ si può prendere $k := 0$ e $c_0 := n$; supponiamo dunque che la (i) valga per ogni numero naturale $n < \overline{n}$ e proviamola per $\overline{n}$. Come si è osservato, possiamo supporre che sia $\overline{n} \geq b$; sia allora (per il teorema 7.2.1)

$$\overline{n} = qb + c_0 \quad \text{con} \quad 0 \leq c_0 < b\,.$$

Poiché $b > 1$, è $q < \overline{n}$ e dunque applicando a q l'ipotesi di induzione devono esistere $k, c_1, c_2, \ldots, c_k \in \mathbb{N}$ tali che

$$q = c_k b^{k-1} + c_{k-1} b^{k-2} + \ldots + c_2 b + c_1 \quad \text{con} \quad 0 \leq c_i < b \quad \text{e} \quad c_k \neq 0 \text{ se } k - 1 > 0\,;$$

allora è immediato che

$$\overline{n} = qb + c_0 = (c_k b^{k-1} + c_{k-1} b^{k-2} + \ldots + c_2 b + c_1) b + c_0 =$$
$$= c_k b^k + c_{k-1} b^{k-1} + \ldots + c_1 b + c_0 \quad \text{con} \quad 0 \leq c_i < b \quad \text{e} \quad c_k \neq 0 \text{ se } k > 0$$

cioè la (*), come si voleva.

Per provare la (ii), basta scrivere la (*) nella forma

$$n = (c_k b^{k-j} + c_{k-1} b^{k-j-1} + \ldots + c_{j+1} b + c_j) b^j + c_{j-1} b^{j-1} + \ldots + c_1 b + c_0$$

e osservare che

– il quoziente della divisione euclidea di n per b^j è

$$c_k b^{k-j} + c_{k-1} b^{k-j-1} + \ldots + c_{j+1} b + c_j$$

(bisogna soltanto provare che $c_{j-1} b^{j-1} + \ldots + c_1 b + c_0 < b^j$, e lo si lascia per esercizio: si tenga presente che i c_s sono tutti numeri naturali strettamente minori di b, e si proceda per induzione su j);

– il resto della divisione euclidea di tale quoziente per b è c_j.

Sia b un numero naturale maggiore di 1 . Sia n un numero naturale, e sia

$$n = \sum_{i=0}^{k} c_i b^i \qquad \text{con } 0 \leq c_i < b \text{ (cfr. teor. 10.6.1) ..}$$

I numeri c_0, c_1, … , c_k si dicono le *cifre* della *rappresentazione di n in base b* .

Per scrivere effettivamente i numeri naturali si scelgono innanzitutto dei simboli grafici per indicare quelli minori di b . È convenzione ormai diffusa utilizzare i simboli

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E,\ F$$

per indicare, nell'ordine, i numeri naturali da "zero" a "quindici" (di questi, come si è già detto, si usano solo i primi b) .

Se è $n = \sum_{i=0}^{k} c_i b^i$ con $0 \leq c_i < b$, la *notazione posizionale in base* b di n consiste nello scrivere in sequenza i simboli che rappresentano (nell'ordine) le cifre c_k, c_{k-1}, … , c_1, c_0 . Se n è diverso da "zero", si scelgono inoltre c_k , … , c_0 in modo che sia $c_k \neq 0$; mentre, come si è già detto, il numero "zero" si indica col simbolo 0.

Esempio 10.6.2

Sia $b :=$ "dieci". Si ha

"quattromilacinquecentosei" = "quattro" $\cdot\, b^{\text{"}tre\text{"}}$ + "cinque" $\cdot\, b^{\text{"}due\text{"}}$ + "zero" $\cdot\, b$ + "sei" ;

pertanto "quattro", "cinque", "zero" e "sei" sono (nell'ordine) le cifre della rappresentazione in base "dieci" di "quattromilacinquecentosei", che quindi in tale base si indica appunto con la scrittura "4506" .

Queste cifre si determinano facilmente mediante la (ii) del teorema 10.6.1. Infatti

quattromilacinquecentosei = quattrocentocinquanta · dieci + sei ;
quattrocentocinquanta = quarantacinque · dieci + zero ;
quarantacinque = quattro · dieci + cinque ;
quattro = zero · dieci + quattro.

Sia $b :=$ "due". Si ha

"quattromilacinquecentosei" =
$= $ "uno" $\cdot\, b^{\text{"}dodici\text{"}}$ + "zero" $\cdot\, b^{\text{"}undici\text{"}}$ + "uno" $\cdot\, b^{\text{"}dieci\text{"}}$ + "uno" $\cdot\, b^{\text{"}nove\text{"}}$ +
+ "uno" $\cdot\, b^{\text{"}otto\text{"}}$ + "uno" $\cdot\, b^{\text{"}sette\text{"}}$ + "zero" $\cdot\, b^{\text{"}sei\text{"}}$ + "zero" $\cdot\, b^{\text{"}cinque\text{"}}$ +
+ "uno" $\cdot\, b^{\text{"}quattro\text{"}}$ + "uno" $\cdot\, b^{\text{"}tre\text{"}}$ + "zero" $\cdot\, b^{\text{"}due\text{"}}$ + "uno" $\cdot\, b$ + "zero" ;

pertanto "uno", "zero", "uno", "uno", "uno", "uno", "zero", "zero", "uno", "uno", "zero", "uno" e "zero" sono (nell'ordine) le cifre della rappresentazione in base "due" di "quattromilacinquecentosei", che quindi in tale base si indica appunto con la scrittura "1011110011010" .

Queste cifre si determinano facilmente mediante la (ii) del teorema 10.6.1. Infatti
quattromilacinquecentosei = duemiladuecentocinquantatré · due + zero ;
duemiladuecentocinquantatré = millecentoventisei · due + uno ;
millecentoventisei = cinquecentosessantatré · due + zero ;
cinquecentosessantatré = duaecentoottantuno · due + uno ;
duecentotottantuno = centoquaranta · due + uno ;
centoquaranta = settanta · due + zero ;
settanta = trentacinque · due + zero ;
trentacinque = diciassette · due + uno ;
diciassette = otto · due + uno ;
otto = quattro · due + uno ;
quattro = due · due + uno ;
due = uno · due + zero ;
uno = zero · due + uno .

Sia b := "otto". Si ha

"quattromilacinquecentosei" = "uno" · $b^{\text{"quattro"}}$ + "zero" · $b^{\text{"tre"}}$ + "sei" · $b^{\text{"due"}}$ + "tre" · b + "due" ;

pertanto "uno", "zero", "sei", "tre" e "due" sono (nell'ordine) le cifre della rappresentazione in base "otto" di "quattromilacinquecentosei", che quindi in tale base si indica appunto con la scrittura "10632" .

Queste cifre si determinano facilmente mediante la (ii) del teorema 10.6.1. Infatti
quattromilacinquecentosei = cinquecentosessantatré · otto + due ;
cinquecentosessantatré = settanta · otto + tre ;
settanta = otto · otto+sei ;
otto = uno · otto + zero ;
uno = zero · due + 1 .

Sia b := "sedici". Si ha

"quattromilacinquecentosei" = "uno" · $b^{\text{"tre"}}$ + "uno" · $b^{\text{"due"}}$ + "nove" · b + "dieci" ;

pertanto "uno", "uno", "nove" e "dieci" sono (nell'ordine) le cifre della rappresentazione in base 16 di "quattromilacinquecentosei", che quindi in tale base si indica appunto con la scrittura "$119A$" .

Queste cifre si determinano facilmente mediante la (ii) del teorema 10.6.1. Infatti
quattromilacinquecentosei = duecentoottantuno · sedici + dieci ;
duecentoottantuno = diciassette · sedici + nove ;
diciassette = uno · sedici + uno ;
uno = zero · sedici + uno .

Esempio 10.6.3

Sia b = "dieci". Allora:
"nove" si scrive 9 ; "dieci" si scrive 10 ; "trentuno" si scrive 31 ; "trentasette" si scrive 37 .
Sia b = "due". Allora:
"nove" si scrive 1001 ; "dieci" si scrive 1010 ; "trentuno" si scrive 11111 ; "trentasette" si scrive 100101 .
Sia b = "otto". Allora:
"nove" si scrive 11 ; "dieci" si scrive 12 ; "trentuno" si scrive 37 ; "trentasette" si scrive 45 .
Sia b = "sedici". Allora:
"nove" si scrive 9 ; "dieci" si scrive A ; "trentuno" si scrive $1F$; "trentasette" si scrive 25 .

10.7 - I criteri di divisibilità per i numeri interi.

Come applicazione della teoria sviluppata nella sez. 10.5, dimostriamo i classici criteri di divisibilità per i numeri interi.

In tutta questa sezione, indichiamo con m un numero intero e con n un numero intero positivo. Ci proponiamo di stabilire condizioni necessarie e sufficienti affinché m sia divisibile per n, ossia (cfr. teorema 10.4.3 ed esercizio 10.4.5) affinché si abbia

$$m \equiv 0 \pmod{n}.$$

Poiché numeri opposti hanno gli stessi divisori, possiamo supporre che sia $m > 0$.

I nostri criteri faranno riferimento alle cifre della rappresentazione posizionale di m in base 10 (cfr. sez. 10.6); sia dunque

$$m = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \ldots + c_3 \cdot 10^3 + c_2 \cdot 10^2 + c_1 \cdot 10 + c_0.$$

Per ogni numero intero a, indicheremo con $[a]$ la classe di resto modulo n a cui appartiene a; possiamo scrivere

$$(\bigstar) \qquad [m] = [c_k] \cdot [10]^k + [c_{k-1}] \cdot [10]^{k-1} + \ldots + [c_3] \cdot [10]^3 + [c_2] \cdot [10]^2 + [c_1] \cdot [10] + [c_0].$$

Teorema 10.7.1

Sia c_0 l'ultima cifra di m. Si ha

$$m \equiv c_0 \pmod{2}$$
$$m \equiv c_0 \pmod{5}$$

e

$$m \equiv c_0 \pmod{10}.$$

Pertanto: m è divisibile per 2 sse l'ultima cifra di m è 0, 2, 4, 6 oppure 8; m è divisibile per 5 sse l'ultima cifra di m è 0 oppure 5; m è divisibile per 10 sse l'ultima cifra di m è 0.

Dimostrazione – Se $n = 2$ oppure $n = 5$ oppure $n = 10$, è $[10] = [0]$ e quindi dalla $(\bigstar)$ si ricava che

$$[m] = [c_0]$$

ossia (cfr. osservazione 10.2.2) $$m \equiv c_0 \pmod{n}.$$

Le uniche cifre divisibili per 2 sono 0, 2, 4, 6 e 8; le uniche cifre divisibili per 5 sono 0 e 5; e l'unica cifra divisibile per 10 è 0. L'asserto è così completamente provato.

Teorema 10.7.2

Siano c_2, c_1 e c_0 le ultime tre cifre di m. Si ha

$$m \equiv c_1 \cdot [10] + c_0 \pmod 4$$

e

$$m \equiv c_2 \cdot [10]^2 + c_1 \cdot [10] + c_0 \pmod 8.$$

Pertanto: m è divisibile per 4 sse è divisibile per 4 il numero formato dalle ultime due cifre di m; m è divisibile per 8 sse è divisibile per 8 il numero formato dalle ultime tre cifre di m.

Dimostrazione – Dalla $(\bigstar)$ si ricava che

$$[m] = [h_0] \cdot [1000] + [c_2] \cdot [10]^2 + [c_1] \cdot [10] + [c_0] =$$
$$= [h_1] \cdot [100] + [c_1] \cdot [10] + [c_0].$$

Se $n = 8$, è $[1000] = [0]$ e quindi

$$[m] = [c_2] \cdot [10]^2 + [c_1] \cdot [10] + [c_0];$$

Se $n = 4$, è $[100] = [0]$ e quindi

$$[m] = [c_1] \cdot [10] + [c_0]$$

come si voleva.

Teorema 10.7.3

Sia m un numero intero, e siano c_k, $c_{k-1}\ldots$, c_2, c_1 e c_0 le cifre di m. Si ha

$$m \equiv (c_k + c_{k-1} + \ldots + c_2 + c_1 + c_0) \pmod 3$$

e

$$m \equiv (c_k + c_{k-1} + \ldots + c_2 + c_1 + c_0) \pmod 9$$

Pertanto: m è divisibile per 3 [risp.: per 9] sse è divisibile per 3 [risp.: per 9] la somma delle sue cifre.

Dimostrazione – Se $n = 3$ oppure $n = 9$, è $[10] = [1]$ e quindi dalla $(\bigstar)$ si ricava che

$$[m] = [c_k] \cdot [1]^k + [c_{k-1}] \cdot [1]^{k-1} + \ldots + [c_2] \cdot [1]^2 + [c_1] \cdot [1] + [c_0] =$$
$$= [c_k] + [c_{k-1}] + \ldots + [c_2] + [c_1] + [c_0] = [c_k + c_{k-1} + \ldots + c_2 + c_1 + c_0].$$

Dall'osservazione 10.2.2 segue l'asserto.

Osservazione 10.7.4

Sia $n = 9$.
Per il teorema 10.5.11, se $a = b + c$ allora è anche $[a] = [b] + [c]$; se $a = b - c$ allora è anche $[a] = [b] - [c]$; se $a = b \cdot c$ allora è anche $[a] = [b] \cdot [c]$; se $a = bq + r$ allora è anche $[a] = [b][q] + [r]$. Attenzione: non vale il viceversa!
Il teorema 10.7.3 giustifica la cosiddetta "prova del 9" per la somma, la sottrazione, la moltiplicazione e la divisione euclidea.

Esercizio 10.7.5

Sia $n = 9$.
Si trovino dei numeri interi a, b e c tali che $a \neq bq + r$ ma $[a] = [b][q] + [r]$, mostrando così che la "prova del 9" fornisce una condizione necessaria ma non sufficiente per l'esattezza del calcolo.

Esercizio 10.7.6

Si enunci una "prova del 3" analoga a quella "del 9". Si può enunciare analogamente una "prova del 2" ? E una "prova dell' 8" ? E una "prova del 10" ? E una "prova del 6" ?
Perché la più diffusa è la "prova del 9" ?

Teorema 10.7.7

Siano c_k, c_{k-1}, …, c_2, c_1 e c_0 le cifre di m, e supponiamo k pari (ponendo $c_k := 0$ qualora m abbia un numero pari di cifre). Si ha

$$m \equiv (c_k - c_{k-1} + \ldots + c_2 - c_1 + c_0) \pmod{11}$$

ossia $$m \equiv (c_k + c_{k-2} + \ldots + c_2 + c_0) - (c_{k-1} + c_{k-3} + \ldots + c_1) \pmod{11}.$$

Pertanto: m è divisibile per 11 sse è divisibile per 11 la differenza tra la somma delle sue cifre "di posto dispari" e la somma delle sue cifre "di posto pari".

Dimostrazione – Se $n = 11$ si ha $[10] = -[1]$, da cui (per il teorema 10.5.11)

$$[10]^h = -[1] \quad \text{se } h \text{ è dispari} \quad \text{e} \quad [10]^h = [1] \quad \text{se } h \text{ è pari.}$$

Ancora per il teorema 10.5.11, e ricordando che abbiamo scelto c_k in modo che k sia pari, dalla $(\bigstar)$ si ricava che

$$[m] = [c_k] \cdot [1]^k + [c_{k-1}] \cdot (-[1]) + \ldots + [c_2] \cdot [1] + [c_1] \cdot (-[1]) + [c_0] =$$
$$= [c_k] - [c_{k-1}] + \ldots + [c_2] - [c_1] + [c_0] = [c_k - c_{k-1} + \ldots + c_2 - c_1 + c_0].$$

Dall'osservazione 10.2.2 segue l'asserto.

Esercizio 10.7.8

Si enunci una "prova dell'11" analoga a quella "del 9", discutendone in raffronto vantaggi e svantaggi

Esercizio 10.7.9

È un utile (e facile) esercizio la riformulazione dei criteri di divisibilità visti in questa sezione con riferimento a basi diverse dalla base dieci (cfr. sez. 10.6). Si enuncino e dimostrino i criteri di divisibilità per due, tre, quattro, sei, undici, dodici e tredici quando il numero da dividere è scritto in base dodici. Si enuncino e dimostrino i criteri di divisibilità per due, quattro, sette, otto e nove quando il numero da dividere è scritto in base otto.

11.- ALCUNE EQUAZIONI IN $\mathbb{Z}_n$

In tutto il capitolo 11 supporremo fissato un numero intero positivo $n > 1$*, e per ogni* $z \in \mathbb{Z}$ *indicheremo con* $[z]$ *la classe di resto modulo* n *a cui appartiene* z**.**

11.1 - Equazioni di primo grado in $\mathbb{Z}_n$.

Chi avesse provato a risolvere (procedendo per tentativi, come era ragionevole fare visti i pochi elementi coinvolti) gli esercizi 10.5.7 e 10.5.8 si dovrebbe essere accorto che l'anello $\mathbb{Z}_n$ presenta situazioni piuttosto diverse rispetto all'anello $\mathbb{Z}$, del quale peraltro è immagine mediante un omomorfismo fra anelli (come si è osservato nella sez. 10.5). Alcune di queste situazioni possono essere facilmente descritte, ed è ciò che faremo in questo capitolo.

Iniziamo osservando che la risoluzione delle equazioni di primo grado in $\mathbb{Z}_n$ può essere facilmente affrontata applicando le tecniche studiate nella sez. 7.4.

Teorema 11.1.1

Siano $a, b, n \in \mathbb{Z}^+$, e sia $\delta := \text{MCD}(a, n)$. L'equazione

$$[a]\overline{x} = [b]$$

ha soluzione in $\mathbb{Z}_n$ se e soltanto se δ divide b.

In tal caso essa ha esattamente δ soluzioni in $\mathbb{Z}_n$, della forma $\overline{x} := [x_0 + h\frac{n}{\delta}]$ dove h varia in $\mathbb{Z}$ tra 0 e $\delta - 1$ e (x_0, y_0) è una qualsiasi soluzione in $\mathbb{Z}$ dell'equazione diofantina

$$ax + ny = b\,.$$

Dimostrazione – Posto $\overline{x} := [x]$, per come si è definito il prodotto in $\mathbb{Z}_n$ si ha $[a]\overline{x} = [b]$ (cioè $[a][x] = [b]$) se e soltanto se $[ax] = [b]$, ossia (per l'oss. 10.2.2) se e soltanto se $ax \equiv b \pmod{n}$; ciò equivale a chiedere che esista $y \in \mathbb{Z}$ tale che $ax - b = ny$ ossia tale che

$$ax - ny = b\,.$$

Questa è un'equazione diofantina le cui soluzioni differiscono da quelle di

$$ax + ny = b$$

soltanto per il segno della y. Poiché a noi interessa soltanto la x possiamo considerare quest'ultima equazione: per quanto osservato sopra, dunque, $[x_0]$ è soluzione di $[a]\overline{x} = [b]$ se e soltanto se esiste $y_0 \in \mathbb{Z}$ tale che (x_0, y_0) è soluzione di $ax + ny = b$.

Possiamo applicare adesso i teoremi 7.4.1 e 7.4.4: dal primo deduciamo che l'equazione data ha soluzione in $\mathbb{Z}_n$ se e soltanto se δ divide b; dal secondo, che se (x_0, y_0) è una soluzione dell'equazione

$$ax + ny = b\,,$$

tutte le soluzioni di tale equazione in $\mathbb{Z} \times \mathbb{Z}$ sono della forma $x := x_0 + h\frac{n}{\delta}$, $y := y_0 - h\frac{a}{\delta}$ al variare di $h \in \mathbb{Z}$ e dunque tutte le soluzioni in $\mathbb{Z}_n$ di $[a]\overline{x} = [b]$ sono della forma

$$\overline{x} := [x_0 + h\tfrac{n}{\delta}]$$

al variare di h in $\mathbb{Z}$. Resta solo da osservare che per $h := 0, 1, \ldots, \delta - 1$ i numeri della forma $x_0 + h\frac{n}{\delta}$ danno luogo a δ classi di resto a due a due distinte, mentre per ogni altro valore intero di h si ottiene nuovamente una di tali classi di resto.

11.2 - Divisori dello zero ed elementi invertibili in $\mathbb{Z}_n$.

Come si è osservato negli esempi 10.5.3 e 10.5.4, in generale negli anelli $\mathbb{Z}_n$ non vale la legge di annullamento del prodotto, cioè esistono divisori dello zero. D'altro lato, chi avesse provato a svolgere (per tentativi) gli esercizi 10.5.7 e 10.5.8 si sarebbe accorto che, sempre in generale, nell'anello $\mathbb{Z}_n$ molti elementi hanno l'inverso (ossia il simmetrico rispetto al prodotto, cfr. sez. 4.5) a differenza di quanto accade in $\mathbb{Z}$ (cfr. esempio 4.5.3). Grazie al teorema 11.1.1 possiamo precisare questa situazione, descrivendo con esattezza in funzione di n gli elementi invertibili e i divisori dello zero di $\mathbb{Z}_n$.

Teorema 11.2.1

Sia $a \in \mathbb{Z}^+$. Sono fatti equivalenti:

(i) $[a]$ è invertibile in $\mathbb{Z}_n$;

(ii) $\mathrm{MCD}(a, n) = 1$.

Dimostrazione – L'elemento $[a]$ è invertibile in $\mathbb{Z}_n$ se e soltanto se in $\mathbb{Z}_n$ l'equazione

$$[a]\,x = [1]$$

ha soluzione; per il teorema 11.1.1 ciò avviene se e soltanto se $\mathrm{MCD}(a, n)$ divide 1, ossia se e soltanto se $\mathrm{MCD}(a, n) = 1$.

Teorema 11.2.2

Sia $a \in \mathbb{Z}^+$. Se $[a] \neq [0]$, sono fatti equivalenti:

(i) $[a]$ è un divisore dello zero in $\mathbb{Z}_n$;

(ii) MCD$(a, n) \neq 1$.

Dimostrazione – Se l'elemento $[a]$ è diverso da $[0]$, esso è un divisore dello zero in $\mathbb{Z}_n$ se e soltanto se in $\mathbb{Z}_n$ l'equazione

$$[a]\, x = [0]$$

ha almeno una soluzione diversa da $[0]$, cioè (poiché certamente $[0]$ è soluzione) se e soltanto se ha più di una soluzione; per il teorema 11.1.1 ciò avviene se e soltanto se MCD(a, n) è diverso da 1.

Corollario 11.2.3

Sia $\mathcal{I}$ l'insieme degli elementi invertibili di $\mathbb{Z}_n$ e sia $\mathcal{D}$ l'insieme dei divisori dello zero di $\mathbb{Z}_n$. Allora $\{\{[0]\}, \mathcal{I}, \mathcal{D}\}$ è una partizione $\mathbb{Z}_n$; dunque ogni elemento diverso da $[0]$ di $\mathbb{Z}_n$è invertibile oppure è un divisore dello zero (ma non è entrambe le cose).

Dimostrazione – L'elemento $[0]$ non è un divisore dello zero (per definizione di divisore dello zero) e non è invertibile (infatti moltiplicato per qualsiasi elemento dà come risultato $[0]$ e non $[1]$, per l'osservazione 4.8.4 ([21])). Per il teorema 10.4.4, ogni altro elemento di $\mathbb{Z}_n$ è della forma $[a]$ con $1 < a < n$; se MCD$(a, n) = 1$ esso è invertibile in $\mathbb{Z}_n$ per il teorema 11.2.1, altrimenti esso è un divisore dello zero in $\mathbb{Z}_n$ per il teorema 11.2.2.

Teorema 11.2.4

Sono fatti equivalenti:

(i) in $\mathbb{Z}_n$ esistono divisori dello zero;

(ii) n non è un numero primo.

Dimostrazione – $(i) \Rightarrow (ii)$.

Anziché mostrare direttamente che dalla (i) segue la (ii), proviamo che se non è vera la (ii) allora non vale la (i), cioè che se n è un numero primo allora in $\mathbb{Z}_n$ non esistono divisori dello zero. Se $[a]$ fosse un divisore dello zero in $\mathbb{Z}_n$, dovrebbe essere per definizione $[a] \neq [0]$; inoltre per il teorema 11.2.2 sarebbe MCD$(a, n) \neq 1$ e quindi (essendo n irriducibile per il teorema 8.1.3) MCD$(a, n) = n$; ma allora a sarebbe un multiplo di n e avremmo la contraddizione $[a] = [0]$.

[21] Si noti che $[0] \neq [1]$ perché $n > 1$.

$(ii) \Rightarrow (i)$.

Se n non è un numero primo, allora (per il teorema 8.1.3) n non è irriducibile, dunque esistono $a, b \in \mathbb{Z}^+$ con $1 < a < n$ e $1 < b < n$ tali che $n = ab$. Pertanto

$$[a][b] = [ab] = [n] = [0]$$

con $[a], [b] \neq [0]$, e dunque $[a]$ è un divisore dello zero in $\mathbb{Z}_n$.

Teorema 11.2.5

Sono fatti equivalenti:

(i) in $\mathbb{Z}_n$ ogni elemento diverso da $[0]$ è invertibile;

(ii) n è un numero primo.

Dimostrazione – $(i) \Rightarrow (ii)$.

Per il corollario 11.2.3, se vale la (i) in $\mathbb{Z}_n$ non ci sono divisori dello zero, dunque n è un numero primo per il teorema 11.2.4.

$(ii) \Rightarrow (i)$.

Supponiamo che n sia un numero primo. Poiché, per il teorema 10.4.4, ogni elemento di $\mathbb{Z}_n$ diverso da $[0]$ è della forma $[a]$ con $1 < a < n$, e quindi MCD$(a, n) = 1$, per il teorema 11.2.1 ogni elemento di $\mathbb{Z}_n$ diverso da $[0]$ è invertibile.

Corollario 11.2.6

Siano $i, j, k \in \mathbb{Z}$. Se MCD$(k, n) = 1$, allora

$$[i][k] = [j][k] \quad \Rightarrow \quad [i] = [j].$$

Dimostrazione – Per il teorema 11.2.1, $[k]$ è invertibile in $\mathbb{Z}_n$, quindi esiste $\overline{k} \in \mathbb{Z}$ tale che $[k][\overline{k}] = [1]$. Dunque dall'uguaglianza

$$[i][k] = [j][k]$$

moltiplicando a destra ambo i membri per $[\overline{k}]$ si trova che

$$([i][k])[\overline{k}] = ([j][k])[\overline{k}]$$

ossia, per la proprietà associativa del prodotto,

$$[i]\big([k][\overline{k}]\big) = [j]\big([k][\overline{k}]\big)$$

da cui $[i][1] = [j][1]$ e infine $[i] = [j]$ come si voleva.

11.3 - La funzione φ di Euler.

Questa è una sezione tecnica, nella quale definiamo (e in parte studiamo) una importante funzione $\mathbb{N}\backslash\{0\} \to \mathbb{N}$ che svolgerà un ruolo essenziale nella sez. 11.4.

Sia $n \in \mathbb{N}$, $n \geq 1$. Si indica con $\varphi(n)$ il numero dei numeri naturali minori di n che sono primi con n (cfr. sez. 7.2). La funzione $\varphi : \mathbb{N}\backslash\{0\} \to \mathbb{N}$ così definita è nota col nome di "funzione φ di Euler" in onore del matematico svizzero Leonhard Euler ($1707 - 1783$).

Nel resto di questo capitolo, col simbolo φ indicheremo sempre la funzione φ di Euler.

Esempi

11.3.1 $\varphi(3) = 2$. Infatti i numeri naturali minori di 3 sono: $0, 1$ e 2; di questi, due (per la precisione: 1 e 2) sono primi con 3.

11.3.2 $\varphi(6) = 2$. Infatti i numeri naturali minori di 6 sono: $0, 1, 2, 3, 4$ e 5; di questi, solo due (per la precisione: 1 e 5) sono primi con 6.

11.3.3 $\varphi(8) = 4$. Infatti i numeri naturali minori di 8 sono: $0, 1, 2, 3, 4, 5, 6$ e 7; di questi, quattro (per la precisione: $1, 3, 5$ e 7) sono primi con 8.

11.3.4 $\varphi(15) = 8$. Infatti i numeri naturali minori di 15 sono: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13$ e 14; di questi, otto (per la precisione: $1, 2, 4, 7, 8, 11, 13$ e 14) sono primi con 15.

11.3.5 $\varphi(18) = 6$. Infatti i numeri naturali minori di 18 sono: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$ e 17; di questi, soltanto sei (per la precisione: $1, 5, 7, 11, 13$ e 17) sono primi con 18.

Teorema 11.3.6

Se p è un numero primo, allora per ogni numero intero positivo h si ha

$$\varphi(p^h) = p^{h-1}(p-1).$$

Dimostrazione – Contiamo quanti dei numeri naturali minori di p^h non sono primi con p^h (cioè, poiché p è primo, sono multipli di p). I multipli di p sono tutti e soli i numeri naturali della forma kp con $k \in \mathbb{N}$; sono minori di p^h se e soltanto se $k < p^{h-1}$, dunque i valori possibili per k vanno da 0 a $p^{h-1} - 1$, cioè sono in numero di p^{h-1}.

D'altra parte, i numeri naturali minori di p^h vanno da 0 a $p^h - 1$, cioè sono in numero di p^h.Si è così provato che $\varphi(p^h) = p^h - p^{h-1} = p^{h-1}(p-1)$, come si voleva.

Teorema 11.3.7

Siano $a, b \in \mathbb{N}\backslash\{0\}$. Se MCD$(a, b) = 1$, si ha

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Dimostrazione – Omettiamo la dimostrazione di questo teorema. Questo risultato si esprime talvolta dicendo che la funzione φ di Euler è *moltiplicativa*.

Osservazione 11.3.8

Siano $a, b \in \mathbb{N}\backslash\{0\}$. Se MCD$(a, b) \neq 1$, non si ha in generale $\varphi(ab) = \varphi(a)\varphi(b)$, come si è visto negli esempi 11.3.1, 11.3.2 e 11.3.5. Tuttavia il teorema 11.3.7, grazie al teorema 11.3.6, consente di calcolare $\varphi(n)$ per ogni numero naturale n del quale sia nota l'espressione come prodotto di fattori primi (tale espressione peraltro esiste sempre, in base al teorema 8.2.2).

Esempi

11.3.9 $\varphi(15) = 8$. Infatti $15 = 3 \cdot 5$ con MCD$(3, 5) = 1$ e dunque per il teorema 11.3.7

$$\varphi(15) = \varphi(3) \cdot \varphi(5) \overset{\text{(teor. 11.3.6)}}{=} 2 \cdot 4 = 8\,.$$

11.3.10 $\varphi(270) = 72$. Infatti $270 = 2 \cdot 3^3 \cdot 5$ e dunque per il teorema 11.3.7

$$\varphi(270) = \varphi(2) \cdot \varphi(3^3) \cdot \varphi(5) \overset{\text{(teor. 11.3.6)}}{=} 1 \cdot 18 \cdot 4 = 72\,.$$

11.3.11 $\varphi(171\,275) = 72$. Infatti $171\,275 = 5^2 \cdot 13 \cdot 17 \cdot 31$ e dunque per il teorema 11.3.7

$$\varphi(171\,275) = \varphi(5^2) \cdot \varphi(13) \cdot \varphi(17) \cdot \varphi(31) \overset{\text{(teor. 11.3.6)}}{=} 20 \cdot 12 \cdot 16 \cdot 30 = 115\,200\,.$$

11.4 - Il teorema di Fermat-Euler.

In questa sezione studiamo l'equazione esponenziale

$$[a]^x = [1]$$

nell'incognita $x \in \mathbb{N}\backslash\{0\}$. Notiamo esplicitamente che l'esponente x non può essere un elemento di $\mathbb{Z}_n$: infatti in $\mathbb{Z}_n$ la scrittura $[a]^{[b]}$ non ha senso, come si è visto nell'esempio 10.5.2.

Osservazione 11.4.1

Sia $a \in \mathbb{N}$. Se l'equazione

(*) $$[a]^x = [1]$$

nell'incognita x ha soluzione in $\mathbb{N}\backslash\{0\}$, allora

(i) MCD$(a, n) = 1$

e inoltre

(ii) detta x_0 la più piccola soluzione in $\mathbb{N}\backslash\{0\}$ dell'equazione (*), le soluzioni in $\mathbb{N}\backslash\{0\}$ dell'equazione (*) sono tutti e soli i multipli non nulli di x_0.

Dimostrazione – Supponiamo che l'equazione (*) abbia in $\mathbb{N}\backslash\{0\}$ una soluzione $\overline{x}$. Proviamo la (i). Poiché $\overline{x} \in \mathbb{N}\backslash\{0\}$, è $\overline{x} - 1 \in \mathbb{N}$ e si ha

$$[a]^{\overline{x}-1}[a] = [a][a]^{\overline{x}-1} = [1]$$

cioè $[a]$ è invertibile in $\mathbb{Z}_n$: dunque per il teorema 11.2.1 deve essere MCD$(a, n) = 1$.

Proviamo ora la (ii). Sia x_0 la più piccola soluzione in $\mathbb{N}\backslash\{0\}$ dell'equazione (*) e sia x una qualsiasi soluzione della (*); siano rispettiamente q e r il quoziente e il resto della divisione euclidea tra x e x_0. Allora $x = x_0q + r$ e si ha

$$[1] = [a]^x = [a]^{x_0q+r} = ([a]^{x_0})^q \cdot [a]^r = [1]^q \cdot [a]^r = [1] \cdot [a]^r = [a]^r$$

cioè anche r è soluzione della (*); ma poiché $r < x_0$ e x_0 è la più piccola soluzione in $\mathbb{N}\backslash\{0\}$ dell'equazione (*), deve essere $r = 0$ e quindi x è multiplo di x_0. Viceversa è immediato che per ogni multiplo non nullo x_0q di x_0 si ha

$$[a]^{x_0q} = ([a]^{x_0})^q = [1]^q = [1].$$

Teorema 11.4.2 (Fermat-Eulero)

Sia $a \in \mathbb{N}$. Se MCD$(a, n) = 1$, allora

$$[a]^{\varphi(n)} = [1].$$

Dimostrazione – Posto $k := \varphi(n)$, sia

$$\mathrm{J} := \{i_1, i_2, \ldots, i_k\}$$

l'insieme dei numeri naturali minori di n che sono primi con n.

Posto

$$\mathrm{X} := \{[i_1], [i_2], \ldots, [i_k]\}$$

e

$$\mathrm{Y} := \{[ai_1], [ai_2], \ldots, [ai_k]\},$$

osserviamo in primo luogo che $\mathrm{X} = \mathrm{Y}$.

Gli elementi di Y sono a due a due distinti: infatti, se $[ai_s] = [ai_t]$, cioè $[a][i_s] = [a][i_t]$, dal corollario 11.2.6 deduciamo che $[i_s] = [i_t]$ e quindi $s = t$ perché gli elementi di X sono a due a due distinti per definizione. Pertanto Y ha k elementi, cioè tanti quanti ne ha X: per provare che $\mathrm{X} = \mathrm{Y}$ basterà mostrare che $\mathrm{Y} \subset \mathrm{X}$.

Sia dunque $[ai_j] \in$ Y, sia r il resto della divisione euclidea di ai_j per n (cosicché $[ai_j] = [r]$ per il teorema 10.4.3 e l'oss. 10.2.2) e sia $\delta :=$ MCD(r, n). Se fosse $\delta \neq 1$, esisterebbe un numero primo p che divide δ e quindi sia r che n; per l'oss. 7.3.1, p dividerebbe ai_j e quindi (essendo p primo) dividerebbe a oppure dividerebbe i_j: assurdo in ogni caso, perché sia a che i_j sono primi con n. Dunque r è primo con n; è anche minore di n (perché è il resto della divisione euclidea di ai_j per n) e quindi appartiene a J, cosicché $[ai_j](= [r]) \in$ X come si voleva dimostrare.

Dunque X = Y. Ma allora anche il prodotto di tutti gli elementi di X è uguale al prodotto di tutti gli elementi di Y, cioè (ricordando la definizione di prodotto in $\mathbb{Z}_n$)

$$[i_1] \cdot [i_2] \cdot \ldots \cdot [i_k] = [ai_1] \cdot [ai_2] \cdot \ldots \cdot [ai_k] = [a] \cdot [i_1] \cdot [a] \cdot [i_2] \cdot \ldots \cdot [a][i_k] =$$
$$= [a]^k \cdot [i_1] \cdot [i_2] \cdot \ldots \cdot [i_k]$$

e infine, applicando il corollario 11.2.6,

$$[1] = [a]^k$$

come si voleva.

Osservazione 11.4.3

Per il teorema 11.4.2, se MCD$(a, n) = 1$ allora $\varphi(n)$ è una soluzione in $\mathbb{N}\backslash\{0\}$ dell'equazione $[a]^x = [1]$. Vale la pena di notare che non solo non è l'unica soluzione (è ovvio infatti che ogni multiplo di $\varphi(n)$ è ancora soluzione) ma in generale non è nemmeno la più piccola. Ad esempio, per $n := 7$, si ha $[2]^3 = 1$ con $3 < 6 = \varphi(7)$.

Corollario 11.4.4

Sia n un numero primo. Per ogni $a \in \mathbb{N}$,

$$[a]^n = [a].$$

Dimostrazione – Se MCD$(a, n) = 1$, l'asserto segue dal teorema di Fermat-Euler moltiplicando per $[a]$ ambo i membri.

Se invece MCD$(a, n) \neq 1$, deve essere MCD$(a, n) = n$ (e quindi a deve essere multiplo di n) perché per ipotesi n è un numero primo. In questo caso, $[a] = [0]$ e l'asserto è ovvio.

Osservazione 11.4.5

Nel corollario 11.4.4, è essenziale l'ipotesi che n sia un numero primo. Ad esempio, per $n := 6$, si ha che

$$[2]^6 = [2^6] = [64] = [4] \neq [2].$$

Esempio 11.4.6

Applicando il teorema di Fermat-Euler, calcoliamo le ultime due cifre della rappresentazione in base 10 di 7^{963}. In sostanza, dobbiamo trovare il resto della divisione per 100 di 7^{963}, cioè il rappresentante compreso fra 0 e 99 per la classe di resto modulo 100 a cui appartiene 7^{963}.

Lavoriamo dunque in $\mathbb{Z}_{100}$ e (poiché MCD$(7, 100) = 1$) applichiamo il teorema 11.4.2 per $n := 100$. Poiché $100 = 2^2 \cdot 5^2$, è $\varphi(100) = 40$ (per i teoremi 11.3.6 e 11.3.7), cosicché sappiamo che $[7^{40}] = [7]^{40} = 1$. Poiché però a noi interessa $[7^{963}]$, conviene effettuare la divisione euclidea di 963 per 40, ottenendo $963 = 24 \cdot 40 + 3$. Dunque

$$[7^{963}] = [7]^{963} = [7]^{40 \cdot 24 + 3} = [7]^{40 \cdot 24} \cdot [7]^3 = ([7]^{40})^{24} \cdot [7]^3 = 1^{24} \cdot [7^3] = 1 \cdot [7]^3 = [343] = [43] .$$

Pertanto, la rappresentazione in base 10 di 7^{963} termina con 43.

Esempio 11.4.7

Applicando il teorema di Fermat-Euler, calcoliamo il resto della divisione per 11 di 2^{677}. In sostanza, dobbiamo trovare il rappresentante compreso fra 0 e 10 per la classe di resto modulo 11 a cui appartiene 2^{677}.

Lavoriamo dunque in $\mathbb{Z}_{11}$ e (poiché MCD$(2, 11) = 1$) applichiamo il teorema 11.4.2 per $n := 11$. Poiché 11 è un numero primo, $\varphi(11) = 10$ (per il teorema 11.3.6), cosicché sappiamo che $[2^{10}] = [2]^{10} = 1$. Poiché però a noi interessa $[2^{677}]$, conviene effettuare la divisione euclidea di 677 per 10, ottenendo $677 = 67 \cdot 10 + 7$. Dunque

$$[2^{677}] = [2]^{677} = [2]^{10 \cdot 67 + 7} = [2]^{10 \cdot 67} \cdot [2]^7 = ([2]^{10})^{67} \cdot [2]^7 = 1^{67} \cdot [2]^7 = 1 \cdot [2^7] = [128] = [7] .$$

Pertanto, 2^{677} diviso 11 dà resto 7.

11.5 - Cenni sul criptosistema RSA.

Accenniamo in questa sezione al sistema crittografico RSA, che utilizza come fondamento teorico quanto descritto nelle sezioni precedenti.

L'idea è che un certo signor X desideri ricevere in sicurezza (cioè senza che il significato venga intercettato da terzi) messaggi da chiunque: ciascun messaggio dovrà dunque essere trasformato ("codificato") utilizzando un algoritmo disponibile a tutti; ma l'algoritmo deve essere tale che nessuno, tranne ovviamente il signor X, possa risalire dal messaggio modificato al messaggio originale (una tale operazione si dice anche "decrittazione" del messaggio).

Il primo algoritmo efficace con tali caratteristiche è stato sviluppato nel 1977 al Massachusets Institute of Technology da Ronald Linn Rivest (1947 –), Adi Shamir (1952 –) e Leonard Max Adleman (1945 –) ed è noto come "criptosistema RSA" dalle iniziali dei cognomi dei suoi ideatori.

Possiamo supporre che i messaggi da ricevere siano numeri naturali non superiori a un certo $n_0 \in \mathbb{N}$. Il signor X sceglie due numeri primi p_1, p_2 entrambi maggiori di n_0 (e comunque "molto grandi", nel senso che il prodotto $p_1 p_2$ non possa essere fattorizzato in tempo ragionevole; generalmente si considera adeguato un ordine di grandezza di 10^{75}) e un numero naturale s primo con $\varphi(p_1 p_2)$ (cioè con $(p_1 - 1)(p_2 - 1)$). Poiché il signor X conosce p_1 e p_2, può calcolare l'inverso t di s in $\mathbb{Z}_{\varphi(p_1 p_2)}$ (tale inverso esiste per il teorema 11.2.1). Egli rende pubblici il prodotto $p_1 p_2$ e il numero naturale s; da queste informazioni, gli altri non hanno modo di ricavare p_1 e p_2, quindi $\varphi(p_1 p_2)$, e quindi nemmeno t.

Adesso vediamo come può operare chi desidera inviare in sicurezza al signor X un messaggio, cioè un numero naturale a minore di n_0 (che possiamo identificare con la classe di resto modulo n_0 che esso rappresenta). Semplicemente, il mittente calcola (e trasmette)

$$a^s \pmod{p_1 p_2}.$$

Il signor X non deve far altro che elevare il numero ricevuto alla potenza t. Ricordiamo che t è l'inverso di s in $\mathbb{Z}_{\varphi(p_1 p_2)}$, cioè

$$st \equiv 1 \pmod{\varphi(p_1 p_2)}$$

ossia esiste $k \in \mathbb{Z}$ tale che $st = \varphi(p_1 p_2) \cdot k + 1$. Ne segue che in $\mathbb{Z}_{p_1 p_2}$ si ha

$$\left(a^s\right)^t = a^{st} = a^{\varphi(p_1 p_2)\cdot k + 1} = a^{\varphi(p_1 p_2)\cdot k} \cdot a = \left(a^{\varphi(p_1 p_2)}\right)^k \cdot a = 1^k \cdot a = a$$

ricordando che a è minore di n_0 e quindi sia di p_1 che di p_2 (entrambi primi), cosicché certamente $\mathrm{MCD}(a, p_1 p_2) = 1$.

.

12.- CARDINALITÀ

12.1 - Equipotenza.

Siano **A**, **B** insiemi.

Si dice che **A** è *equipotente* a **B** se esiste una corrispondenza biunivoca tra **A** e **B**.

Osservazione 12.1.1

Ogni insieme è equipotente a se stesso.

Dimostrazione – Sia **A** un insieme: la funzione $\mathbf{id_A}$ definita in 3.6.4 è una corrispondenza biunivoca tra **A** e **A**.

Osservazione 12.1.2

Siano **A**, **B** insiemi. Se **A** è equipotente a **B**, allora **B** è equipotente ad **A**.

Dimostrazione – Se $\mathbf{f}:\mathbf{A} \to \mathbf{B}$ è una corrispondenza biunivoca, $\mathbf{f}^{-1}:\mathbf{B} \to \mathbf{A}$ è una corrispondenza biunivoca (cfr. 3.7).

Osservazione 12.1.3

Siano **A**, **B**, **C** insiemi. Se **A** è equipotente a **B** e **B** è equipotente a **C**, allora **A** è equipotente a **C**.

Dimostrazione – Se $\mathbf{f}:\mathbf{A} \to \mathbf{B}$ e $\mathbf{g}:\mathbf{B} \to \mathbf{C}$ sono corrispondenze biunivoche, $\mathbf{g} \circ \mathbf{f}:\mathbf{A} \to \mathbf{C}$ è una corrispondenza biunivoca (cfr. esercizio 3.8.5).

12.2 - Cardinalità.

Per quanto osservato in 12.1.1, 12.1.2 e 12.1.3, in ogni insieme i cui elementi siano insiemi la relazione di "equipotenza" (definita in accordo con 12.1) è una relazione di equivalenza. Questo fatto suggerisce intuitivamente che tutti gli insiemi tra loro equipotenti abbiano in comune una proprietà astratta, che diremo *cardinalità*. Osserviamo esplicitamente che per il teorema 1.3.3 non è possibile dare una definizione di cardinalità mediante il procedimento visto in 10.3.

Per "misurare" la cardinalità di un insieme dovremo considerare degli insiemi – campione a due a due non equipotenti. Per ogni numero naturale n, sia

$$\mathbf{I}_n = \{x \in \mathbb{N} \,/\, 1 \leq x \leq n\}.$$

Gli insiemi $\mathbf{I}_n$, l'insieme $\mathbb{N}$ e l'insieme $\mathbb{R}$ sono tutti a due a due non equipotenti (cfr. teorema 12.3.3).

Sia **A** un insieme. Se **A** è equipotente a $\mathbf{I}_n$ per un certo numero naturale n, diremo che *ha cardinalità* n e scriveremo $|\mathbf{A}| = n$. Se **A** è equipotente a $\mathbb{N}$, diremo che *ha cardinalità* $\aleph_0$ (si legge: aleph con zero) oppure che *è numerabile* e scriveremo $|\mathbf{A}| = \aleph_0$. Se **A** è equipotente a $\mathbb{R}$, diremo che *ha la potenza del continuo* e scriveremo $|\mathbf{A}| = c$.

L'insieme **A** si dice *finito* se è equipotente a $\mathbf{I}_n$ per un certo numero naturale n; si dice *infinito* se non è finito.

Esempio 12.2.1

Il sottoinsieme di $\mathbb{N}$ costituito dai numeri pari ha cardinalità $\aleph_0$.

Dimostrazione – La funzione definita in 3.5.1 è una corrispondenza biunivoca tra $\mathbb{N}$ e l'insieme dei numeri naturali pari.

Raccogliamo qui di seguito alcuni importanti risultati sulla cardinalità degli insiemi; si vedano anche i teoremi 12.3.2, 12.3.3 e 12.3.5.

Teorema 12.2.2

$|\mathbb{Q}| = \aleph_0$.

Dimostrazione – Omettiamo la dimostrazione di questo teorema.

Teorema 12.2.3

Se $|\mathbf{A}| = n$ con $n \in \mathbb{N}$, si ha $|\mathcal{P}(\mathbf{A})| = 2^n$.

Dimostrazione – Questo risultato si può facilmente dimostrare per induzione su n; ma si veda anche il teorema 14.4.7 più avanti.

Teorema 12.2.4

Siano $\mathbf{A}, \mathbf{B}$ insiemi finiti, con $|\mathbf{A}| = n$ e $|\mathbf{B}| = m$ ($n, m \in \mathbb{N}$). Si ha

$$|\mathbf{A} \cup \mathbf{B}| = |\mathbf{A}| + |\mathbf{B}| - |\mathbf{A} \cap \mathbf{B}| \qquad \text{e} \qquad |\mathbf{A} \times \mathbf{B}| = nm\,.$$

Dimostrazione – Omettiamo la dimostrazione di questo teorema.

Teorema 12.2.5

Il sottoinsieme $(0, 1)$ di $\mathbb{R}$ è equipotente a $\mathbb{R}$.

Dimostrazione – È facile verificare che la funzione

$$\mathbf{f}(\mathrm{x}) = \pi\mathrm{x} - \tfrac{\pi}{2}$$

è una corrispondenza biunivoca tra $(0, 1)$ e $(-\frac{\pi}{2}, \frac{\pi}{2})$. D'altro lato, è noto dallo studio della trigonometria che la funzione **tg**(x) ("tangente trigonometrica") è una corrispondenza biunivoca tra $(-\frac{\pi}{2}, \frac{\pi}{2})$ e $\mathbb{R}$. Per l'osservazione 12.1.3 si ha l'asserto.

12.3 - Confronto tra cardinalità.

Siano $\mathbf{A}, \mathbf{B}$ insiemi.

Se $\mathbf{A}$ è equipotente a un sottoinsieme di $\mathbf{B}$, scriveremo $\mathbf{A} \preceq \mathbf{B}$ (si dice talvolta in questo caso che $\mathbf{B}$ *domina* $\mathbf{A}$). Se $\mathbf{A} \preceq \mathbf{B}$ e $\mathbf{A}$ non è equipotente a $\mathbf{B}$, scriveremo $\mathbf{A} \prec \mathbf{B}$.

In ogni insieme i cui elementi siano insiemi, $\preceq$ definisce una relazione evidentemente riflessiva e transitiva. Tale relazione non può in generale essere però antisimmetrica; infatti, se $\mathbf{A}, \mathbf{B}$ sono insiemi distinti equipotenti si ha $\mathbf{A} \preceq \mathbf{B}$ e $\mathbf{B} \preceq \mathbf{A}$ ma $\mathbf{A} \neq \mathbf{B}$. Vale comunque il seguente famoso teorema, la cui dimostrazione esula dai limiti di questi appunti:

Teorema 12.3.1 (Schröder-Bernstein)

Siano $\mathbf{A}, \mathbf{B}$ insiemi. Se $\mathbf{A} \preceq \mathbf{B}$ e $\mathbf{B} \preceq \mathbf{A}$, allora $\mathbf{A}$ e $\mathbf{B}$ sono equipotenti.

Teorema 12.3.2

Se $\mathbf{A}$ è un insieme infinito, e $\mathbf{B}$ è un insieme tale che $\mathbf{B} \preceq \mathbf{A}$, si ha $|\mathbf{A} \times \mathbf{B}| = |\mathbf{A} \cup \mathbf{B}| = |\mathbf{A}|$.

Dimostrazione – Omettiamo la dimostrazione di questo teorema.

Teorema 12.3.3

$|\mathcal{P}(\mathbb{N})| = c$.

Dimostrazione – Omettiamo la dimostrazione di questo teorema.

Mostriamo ora che esistono infinite cardinalità infinite.

Teorema 12.3.4 (Cantor)

Per ogni insieme **A**, è **A** $\prec \mathcal{P}$(**A**).

Dimostrazione - La funzione che all'elemento x di **A** associa l'elemento $\{x\}$ di $\mathcal{P}$(**A**) è evidentemente una corrispondenza biunivoca tra **A** e un sottoinsieme di $\mathcal{P}$(**A**); dunque, **A** $\preceq \mathcal{P}$(**A**). Resta da provare che **A** non è equipotente a $\mathcal{P}$(**A**).

In effetti, non può esistere alcuna funzione suriettiva da **A** a $\mathcal{P}$(**A**). Sia infatti **f**: **A** $\to \mathcal{P}$(**A**). Posto

$$\mathbf{X} := \{a \in \mathbf{A} \,/\, a \notin \mathbf{f}(a)\}$$

non esiste alcun elemento x in **A** per il quale si abbia **f**(x) = **X**. (Per un tale x non potrebbe essere $x \in$ **X**, perché ne seguirebbe $x \notin$ **f**(x) = **X**, né $x \notin$ **X**, perché -essendo **X** = **f**(x)- ne seguirebbe $x \in$ **X**).

Teorema 12.3.5

$\mathbb{N} \prec \mathbb{R}$.

Dimostrazione - L'asserto segue immediatamente dai teoremi 12.3.3 e 12.3.4.

Esiste un insieme **A** tale che $\mathbb{N} \prec$ **A** $\prec \mathbb{R}$? La supposizione che un tale insieme non esista è nota come *ipotesi del continuo*. L'*ipotesi generalizzata del continuo* afferma che per nessun insieme infinito **X** esiste un insieme **A** tale che **X** $\prec$ **A** $\prec \mathcal{P}$(**X**).

Esercizio 12.3.6

Siano **A**, **B** insiemi, e siano **A'**, **B'** insiemi equipotenti rispettivamente ad **A** e **B**. Si provi che **A** $\preceq$ **B** se e solo se **A'** $\preceq$ **B'**. Se ne deduca che è lecito convenire di scrivere |**A**| $\leq$ |**B**| quando **A** $\preceq$ **B**.

13.- PICCIONI E MATRIMONI

13.1 - Il "*principio dei buchi di piccionaia*".

Noto nei paesi anglofoni come "*pigeonhole principle*", questo teorema ha una denominazione che si riferisce probabilmente più agli scomparti dedicati alle lettere nei dipartimenti universitari (detti appunto *pigeonhole*) che ai veri e propri rifugi per i simpatici (ma sporchi) volatili. I matematici "seri" lo chiamano più volentieri "principio dei cassetti di Dirichlet", ritenendo forse nobilitante il richiamo a Peter Gustav Dirichlet (Düren, 13 febbraio 1805 – Gottinga, 5 maggio 1859). Noi lo enunciamo scegliendo una via di mezzo, cioè facendo riferimento alla collocazione di oggetti dentro scatole.

Teorema 13.1.1 ("principio dei buchi di piccionaia")

Siano $n, m \in \mathbb{N}\backslash\{0\}$ con $n > m$.

Se n oggetti vengono posti in m scatole, comunque ciò avvenga c'è almeno una scatola nella quale viene posto più di un oggetto.

Dimostrazione - Sia rispettivamente $x_1, x_2, \ldots, x_m$ il numero degli oggetti deposto in ciascuna delle m scatole. Se fosse $x_i \leq 1$ per ogni $i \in \{1, 2, \ldots, m\}$, sarebbe

$$n = x_1 + x_2 + \ldots + x_m \leq 1 + 1 + \ldots + 1 = m$$

contro l'ipotesi che sia invece $n > m$.

La "traduzione matematica" più ovvia del principio riguarda le funzioni fra insiemi finiti (cfr. sez. 12.2):

Teorema 13.1.2

Siano A, B insiemi finiti, con $|\mathrm{A}| = n > m = |\mathrm{B}|$.

Se **f** è una funzione A $\rightarrow$ B, **f** non è iniettiva.

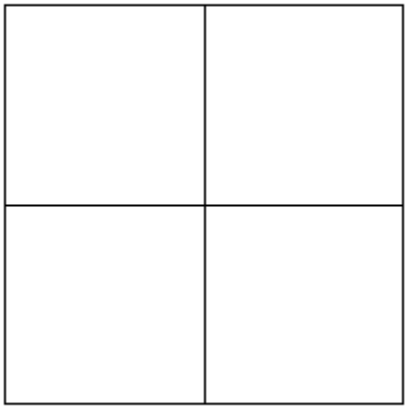
Dimostrazione - Interpretiamo gli elementi di A come "oggetti", gli elementi di B come "scatole" e la funzione **f** come la "collocazione" di $a \in$ A in **f**(a) $\in$ B. Per il principio dei buchi di piccionaia (teor. 13.1.1), almeno due elementi di A vengono "collocati" nello stesso elemento di B, e dunque **f** non è iniettiva.

In questa sezione vedremo alcuni significativi esempi di applicazione del principio dei buchi di piccionaia.

Esempio 13.1.3

Comunque si scelgano cinque punti in un quadrato di lato 2, ce ne sono almeno due la cui distanza è non superiore a $\sqrt{2}$.

Dimostrazione - Tracciando gli assi dei lati del quadrato, suddividiamolo in quattro quadrati Q_1, Q_2, Q_3 e Q_4 tutti di lato 1.



Interpretando i cinque punti da scegliere come "oggetti" e i Q_i come scatole, il principio dei buchi di piccionaia (teor. 13.1.1) ci assicura che almeno due punti apparterranno a uno stesso quadrato Q_{i_0}; la loro distanza non potrà essere superiore alla misura della diagonale di Q_{i_0}, cioè a $\sqrt{2}$.

Esercizio 13.1.4

Si dimostri che: comunque si scelgano cinque punti in un triangolo equilatero di lato 2, ce ne sono almeno due la cui distanza è non superiore a 1 .

Esempio 13.1.5

Se al termine di una riunione, quando gli intervenuti lasciano la sala, ciascuno stringe la mano a tutti e soli quelli che conosce (tranne, ovviamente, a se stesso), almeno due degli intervenuti stringono la mano allo stesso numero di persone.

Dimostrazione - Sia n il numero delle persone presenti alla riunione. Distinguiamo due casi: quello in cui ciascuno dei presenti conosce almeno uno degli altri (e quindi stringe la mano ad almeno una persona) e quello in cui qualcuno dei presenti non conosce nessuno (e quindi non stringe la mano a nessuno).

Nel primo caso il numero delle possibili strette di mano scambiate da ciascuno va da 1 a $n-1$; se distribuiamo le n persone nelle $n-1$ "scatole" corrispondenti alle strette di mano che ciascuno ha scambiato, per il principio dei buchi di piccionaia vediamo che almeno due persone vanno nella stessa "scatola", cioè hanno scambiato lo stesso numero di strette di mano.

Nel secondo caso il numero delle possibili strette di mano scambiate da ciascuno va da 0 a $n-2$; se distribuiamo le n persone nelle $n-1$ "scatole" corrispondenti alle strette di mano che ciascuno ha scambiato, per il principio dei buchi di piccionaia vediamo che anche in questo caso almeno due persone vanno nella stessa "scatola", cioè hanno scambiato lo stesso numero di strette di mano.

Esercizio 13.1.6

Al termine di una riunione, gli intervenuti lasciano la sala e ciascuno stringe la mano a tutti e soli quelli che conosce; qualche eccentrico addirittura stringe la mano a se stesso. Si mostri con un esempio che ciascuno degli intervenuti potrebbe stringere la mano a un diverso numero di persone.

Esempio 13.1.7

Siano $m, n \in \mathbb{Z}^+$. In ogni sequenza di $mn+1$ numeri reali tutti diversi fra loro, c'è almeno una sottosequenza crescente di lunghezza $m+1$ oppure almeno una sottosequenza decrescente di lunghezza $n+1$.

Dimostrazione - Sia $(a_1, a_2, a_3, \ldots, a_{mn+1})$ la sequenza data. Per ogni indice i, indichiamo con c_i la lunghezza della più lunga sottosequenza *crescente* che inizia con a_i e indichiamo con d_i la lunghezza della più lunga sottosequenza *decrescente* che inizia con a_i . Per ogni coppia di indici distinti i, j per ipotesi $a_i \neq a_j$ (abbiamo supposto che gli a_i siano ttutti diversi fra loro); se $a_i < a_j$ è ovviamente $c_i > c_j$, mentre se $a_i > a_j$ deve essere $d_i > d_j$: in ogni caso, per $i \neq j$ le coppie ordinate (c_i, d_i) e (c_j, d_j) sono diverse.

Ciò premesso, procediamo per assurdo e supponiamo che tutte le sottosequenze crescenti abbiano lunghezza $\leq m$ (e quindi sia in particolare $c_i \leq m$ per ogni i) e che tutte le sottosequenze decrescenti abbiano lunghezza $\leq n$ (e quindi sia in particolare $d_i \leq n$ per ogni i).

In questo caso i possibili valori delle coppie ordinate $(c_i,\ d_i)$ sono al più mn; per il principio dei buchi di piccionaia, poiché i assume $mn+1$ valori diversi ne devono esistere due, i_1 e i_2, tali che $i_1 \neq i_2$ ma $(c_{i_1},\ d_{i_1}) = (c_{i_2},\ d_{i_2})$ e questo è un assurdo perché abbiamo mostrato nel paragrafo precedente che per $i \neq j$ le coppie ordinate $(c_i,\ d_i)$ e $(c_j,\ d_j)$ sono diverse. Dunque nella sequenza data c'è almeno una sottosequenza crescente di lunghezza $m+1$ oppure almeno una sottosequenza decrescente di lunghezza $n+1$.

Esercizio 13.1.8

Sia $m := 3$ e $n := 4$. Si trovi una sequenza di 12 numeri reali tutti diversi fra loro che non contenga né una sottosequenza crescente di lunghezza 4 né una sottosequenza decrescente di lunghezza 5.

Esercizio 13.1.9

Sia **ABC** un triangolo. Si dimostri che una retta che non passa per nessuno dei tre vertici **A**, **B** e **C** del triangolo incontra al più due dei tre lati del triangolo.

Esercizio 13.1.10

Sia $(a_1, a_2, a_3, \ldots, a_s)$ una $s-$pla ordinata di numeri interi positivi (cfr. sez. 1.5). Si dimostri che (se nessuno degli a_i è $\equiv 0 \pmod{s}$) esiste una sequenza di a_j (consecutivi nella $s-$pla ordinata considerata) la cui somma è $\equiv 0 \pmod{s}$.

13.2 - Il "*principio generalizzato dei buchi di piccionaia*".

Comunque prese settemila persone, ce ne sono almeno 20 che festeggiano il compleanno nello stesso giorno. Per convincersi di questo non basta il teorema 13.1.1 ma ce ne serve una versione più generale, la cui dimostrazione è però sostanzialmente la stessa.

Teorema 13.2.1 ("principio generalizzato dei buchi di piccionaia")

Siano $n, m, t \in \mathbb{N}\backslash\{0\}$ con $n > mt$.

Se n oggetti vengono posti in m scatole, comunque ciò avvenga c'è almeno una scatola nella quale vengono posti più di t oggetti.

Dimostrazione - Sia rispettivamente $x_1, x_2, \ldots, x_m$ il numero degli oggetti deposto in ciascuna delle m scatole. Se fosse $x_i \leq t$ per ogni $i \in \{1, 2, \ldots, m\}$, sarebbe

$$n = x_1 + x_2 + \ldots + x_m \leq t + t + \ldots + t = mt$$

contro l'ipotesi che sia invece $n > mt$.

Esempio 13.2.2

Comunque prese settemila persone, ce ne sono almeno 20 che festeggiano il compleanno nello stesso giorno.

Dimostrazione - I possibili giorni per festeggiare i compleanni sono 366, e $19 \cdot 366 = 6\,954$. Per il principio generalizzato dei buchi di piccionaia (con $m := 366$, $t := 19$ e $n := 7\,000$) se le $7\,000$ persone vengono disposte nelle 366 "scatole" corrispondenti ai loro compleanni, in almeno una "scatola" vengono poste più di 19 (e quindi almeno 20) persone.

Esempio 13.2.3

A Parigi ci sono almeno 8 abitanti con lo stesso numero di capelli.

Dimostrazione - A Parigi ci sono almeno $2\,200\,000$ abitanti; ed è noto che nessun essere umano ha più di $300\,000$ capelli. Poiché $7 \cdot 300\,000 = 2\,100\,000$, per il principio generalizzato dei buchi di piccionaia (con $m := 300\,000$, $t := 7$ e $n := 2\,200\,000$) se gli abitanti di Parigi vengono disposti nelle $300\,000$ "scatole" corrispondenti ai possibili numeri di capelli, in almeno una "scatola" vengono poste più di 7 (e quindi almeno 8) persone.

Analogo al principio generalizzato dei buchi di piccionaia (anche nella dimostrazione) è il

Teorema 13.2.4 ("principio della media aritmetica")

Siano $n \in \mathbb{Z}^+$ e $\alpha \in \mathbb{R}$. Se la media aritmetica di n numeri reali positivi è α, almeno uno dei numeri è $\geq \alpha$ (e almeno uno dei numeri è $\leq \alpha$).

Dimostrazione - Siano $x_1, x_2, \ldots, x_n$ i numeri reali dati. Se fosse $x_i < \alpha$ per ogni $i \in \{1, 2, \ldots, n\}$, sarebbe

$$x_1 + x_2 + \ldots + x_n < \alpha + \alpha + \ldots + \alpha = n\alpha$$

contro l'ipotesi che sia invece $x_1 + x_2 + \ldots + x_n = n\alpha$. Analogamente si ragiona se $x_i > \alpha$ per ogni $i \in \{1, 2, \ldots, n\}$.

13.3 - Il "teorema dei matrimoni".

In questa sezione studiamo un importante teorema di ottimizzazione degli accoppiamenti che i matematici esprimono folcloristicamente in termini di matrimoni. Va detto che (non sorprendentemente, visto che il teorema risale al 1935) si tratta rigidamente di matrimoni fra persone di genere diverso.

Il problema dei matrimoni (*eterosessuali*).

Siano dati un insieme D (di "donne"), un insieme U (di "uomini") (disgiunto dal precedente) e una funzione s:D $\to \mathcal{P}$(U) (che associa a ogni donna l'insieme degli uomini che le piacciono). Il "*problema dei matrimoni*" per la terna (D, U, s) consiste nel trovare una funzione iniettiva m:D $\to$ U tale che

$$m(d) \in s(d) \quad \text{per ogni } d \in \text{D}$$

cioè nello sposare ogni donna con un uomo che le piace in modo che nessun uomo sia bigamo.

Si noti che la situazione descritta dal problema non è simmetrica: del parere degli uomini non ci preoccupiamo.

Teorema 13.3.1 ("dei matrimoni eterosessuali" – Philip Hall, 1935)

Se $|\text{D}| = n$, condizione necessaria e sufficiente affinché il problema dei matrimoni abbia soluzione è che, per ogni $k \leq n$, ad ogni insieme di k donne piacciano, complessivamente, almeno k uomini.

Dimostrazione - Se a un insieme di k_0 donne, per qualche $k_0 \leq n$, piacciono complessivamente meno di k_0 uomini, per il principio dei buchi di piccionaia non è possibile accoppiarle con quegli uomini senza che almeno un uomo risulti accoppiato ad almeno due donne: dunque la condizione espressa dal teorema è necessaria affinché il problema dei matrimoni abbia soluzone.

Viceversa, dimostriamo che tale condizione è sufficiente procedendo per induzione su $|\text{D}|$. Se $|\text{D}| = 1$, c'è una sola donna alla quale piace almeno un uomo e quindi il problema ha soluzione. Ora supponiamo che il teorema sia vero per $|\text{D}| < n$ e dimostriamo che è vero per $|\text{D}| = n$. Distinguiamo due casi.

Supponiamo in primo luogo che esista un numero naturale k_0 ($1 \leq k_0 < n$) e un insieme di k_0 donne tale che ad esse piacciono complessivamente k_0 uomini (e non di più). La restrizione del problema dei matrimoni a queste k_0 donne (e all'insieme dei k_0 uomini che a loro piacciono) verifica le ipotesi del teorema: infatti se $k_1 \leq k_0$ comunque prese k_1 donne sappiamo che esistono k_1 uomini che a loro complessivamente piacciono; e questi k_1 uomini devono essere un sottoinsieme dei k_0 che stiamo considerando. Dunque, per l'ipotesi di induzione, possiamo felicemente sposare queste k_0 donne ai k_0 uomini che piacciono loro. Restano un insieme di $n - k_0$ ($< n$) donne (disgiunto dal precedente insieme di k_0 donne) e un insieme U* di uomini (disgiunto dal precedente insieme di k_0 uomini); per ogni $k \leq n - k_0$ e per ogni insieme formato da k di queste $n - k_0$ donne, ci sono in U* almeno k uomini che piacciono loro: altrimenti riaggiungendo le k_0 donne già sposate avremmo trovato un insieme di $k + k_0$ donne alle quali complessivamente piacciono meno di $k + k_0$ uomini, contro l'ipotesi del teorema. Dunque anche le restanti $n - k_0$ donne (e l'insieme U* dei restanti uomini) verificano l'ipotesi del teorema e per l'ipotesi di induzione anche queste possono venire felicemente sposate.

Supponiamo adesso che quanto ipotizzato nel paragrafo precedente non accada: ciò significa che per ogni $k < n$ ($k \geq 1$) ad ogni insieme di k donne piacciano complessivamente almeno $k+1$ uomini. Prendiamo una donna a caso, sposiamola con un uomo che le piace e consideriamo le $n-1$ donne rimanenti: esse verificano le ipotesi del teorema (perché per ogni $k < n$, e quindi per ogni $k \leq n-1$, ad ogni insieme di k donne piacciono complessivamente almeno k uomini (erano $k+1$, forse adesso uno non è più disponibile perché è quello che abbiamo già dato in matrimonio ma ne restano comunque almeno k). Dunque, per l'ipotesi di induzione, anche le $n-1$ donne rimanenti possono essere sposate e abbiamo trovato una soluzione anche per $|\mathrm{D}| = n$.

Vediamo adesso un'applicazione "seria" del teorema dei matrimoni (è la versione originariamente pubblicata da Philip Hall…).

Siano S un insieme finito, $n \in \mathbb{Z}^+$ e $\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_n$ sottoinsiemi di S. Si dice *insieme di rappresentanti distinti* per $\{\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_n\}$ un sottoinsieme $\{x_1, x_2, \ldots, x_n\}$ di S tale che

(i) $x_i \in \mathrm{S}_i$ per $i := 1, 2, \ldots, n$;

(ii) $x_i \neq x_j$ se $i \neq j$.

Teorema 13.3.2

Siano S un insieme finito, $n \in \mathbb{Z}^+$ e $\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_n$ sottoinsiemi di S. Condizione necessaria e suffiiciente affinché esista un insieme di rappresentanti distinti per $\{\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_n\}$ è che, per ogni $k \leq n$, l'unione di k degli S_i comunque scelti contenga, complessivamente, almeno k elementi.

Dimostrazione - Gli S_i sono le "donne", gli elementi di S sono gli "uomini" e diciamo che alla "donna" S_i "piace" l'elemento x se e soltanto se $x \in \mathrm{S}_i$. Trovare un insieme di rappresentanti distinti per $\{\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_n\}$ significa allora risolvere il problema dei matrimoni per queste "donne" e per questi "uomini"…

Esempio 13.3.3

Dimostriamo che: comunque si distribuiscano in 13 mazzetti di 4 le 52 carte da gioco di un mazzo "francese", è possibile estrarre da ciascun mazzetto una carta in modo da formare un mazzo di 13 carte tutte di diverso valore facciale (dall'Asso al Re).

Le "donne" da sposare sono i 13 mazzetti di 4 carte in cui sono state distribuite le 52 carte del mazzo francese, gli "uomini" sono i valori da 1 (= Asso) a 13 (= Re); a ogni "donna" (= mazzetto) "piacciono" i valori facciali delle 4 carte che lo costituiscono. Comunque scelti k mazzetti, se nelle $4k$ carte che li costituiscono comparissero in tutto $h < k$ valori allora per il principo generalizzato dei buchi di piccionaia (teorema 13.2.1) ci sarebbe almeno un valore che compare in più di 4 carte, assurdo; dunque nelle carte di k mazzetti compaiono almeno k valori ("a ogni insieme di k donne piacciono complessivamente almeno k uomini") e per il teorema dei matrimoni (teorema 13.1.1) si può associare a ogni mazzetto il valore facciale di una delle carte che lo compongono in modo che a mazzetti diversi restino associati valori diversi; in altre parole, da ognuno dei 13 mazzetti si può estrarre una carta con un diverso valore facciale, come si voleva.

Per stabilire che il problema dei matrimoni è risolubile, qualche volta è utile una condizione soltanto sufficiente ma di più semplice verifica.

Teorema 13.3.4

Se esiste un $k_0 \in \mathbb{Z}^+$ tale che

(i) ad ogni donna piacciono almeno k_0 uomini

e

(ii) ogni uomo piace ad al più k_0 donne

allora il problema dei matrimoni è risolubile.

Dimostrazione - Applichiamo il teorema 13.3.1 verificando che ad ogni insieme di k donne piacciono complessivamente almeno k uomini.

Scegliamo un insieme I di k donne. Per la (i), le coppie (d, u) tali che $d \in$ I e alla donna d piace l'uomo u sono almeno kk_0 ; supponiamo che in tali coppie siano coinvolti m uomini. Per applicare il teorema 13.3.1 dobbiamo dimostrare che $m \geq k$. Se fosse (per assurdo) $k > m$, per il principio generalizzato dei buchi di piccionaia, "distribuendo" le kk_0 coppie fra gli m uomini otterremmo (poiché $kk_0 > mk_0$) che almeno un uomo compare in più di k_0 coppie, cioè che almeno un uomo piace a più di k_0 donne. Ma ciò è assurdo per la (ii), e dunque $m \geq k$ come si voleva dimostrare.

Esercizio 13.3.5

Si mostri con un esempio che la condizione del teorema 13.3.4 non è necessaria affinché il problema dei matrimoni abbia soluzione.

Naturalmente, anche il teorema 13.3.4 si può riformulare in termini insiemistici.

Teorema 13.3.6

Siano S un insieme finito, $n \in \mathbb{Z}^+$ e $S_1, S_2, \ldots, S_n$ sottoinsiemi di S. Se esiste un $k_0 \in \mathbb{Z}^+$ tale che

(i) ad ogni S_i appartengono almeno k_0 elementi

e

(ii) ogni elemento di S appartiene ad al più k_0 degli S_i

allora esiste un insieme di rappresentanti distinti per $\{S_1, S_2, \ldots, S_n\}$.

Dimostrazione - Basta applicare il teorema 13.3.4 come si è applicato il teorema 13.3.1 nella dimostrazione del teorema 13.3.2 .

Esempio 13.3.7

Siano $m, n \in \mathbb{N}\backslash\{0\}$ con $m \leq n$. Si dice *rettangolo latino* di ordine $m \times n$ una matrice $m \times n$ R (cfr. sez. 1.5) tale che

(i) ogni riga di R è una permutazione dei numeri naturali compresi tra 1 e n

(ii) in ogni colonna di R gli elementi sono tutti diversi fra loro.

Un rettangolo latino di ordine $n \times n$ si dice un *quadrato latino* di ordine n ([22]). Dimostriamo che ogni rettangolo latino di ordine $m \times n$ può essere completato, aggiungendo opportunamente $n - m$ righe, in modo da ottenere un quadrato latino di ordine n.

Basterà dimostrare che ad ogni rettangolo latino R di ordine $m \times n$ (con $m < n$) si può aggiungere una riga in modo da trasformarlo in un rettangolo latino di ordine $(m + 1) \times n$; lo facciamo applicando il teorema 13.3.4. Le "donne" sono le colonne di R, gli "uomini" sono i numeri naturali da 1 a n e ad ogni donna "piacciono" i numeri che non vi compaiono; dunque, ad ogni "donna" piacciono esattamente (quindi, in particolare "almeno") $n - m$ "uomini" e ogni "uomo" (= ogni numero naturale tra 1 e n) piace ad esattamente (quindi, in particolare, ad "al più") $n - m$ donne (= le $n - m$ colonne in cui non compare). Per il teorema 13.3.4, ad ogni colonna si può aggiungere un numero che "le piace" (= che non vi compare) in modo che a colonne diverse restino associati numeri diversi (e quindi la nuova riga è anch'essa una permutazione dei numeri naturali compresi tra 1 e n).

[22] Gli usuali schemi di Sudoku sono casi particolari di quadrati latini di ordine 9.

14.- ELEMENTI DI CALCOLO COMBINATORIO

14.1 - Introduzione. Due princìpi per contare.

In questo capitolo ci occuperemo del problema di contare il numero degli elementi di un insieme finito, cioè di determinarne la cardinalità nel senso del capitolo 12. Vedremo i due princìpi fondamentali che si utilizzano in questi casi (teorema 14.1.1 e teorema 14.1.2) e li applicheremo ad alcune situazioni classiche del "calcolo combinatorio", determinando fra altre cose in funzione dei numeri interi positivi k e n il numero delle cosiddette $k-$ disposizioni e $k-$ combinazioni di n oggetti.

Le tecniche che vedremo in questo capitolo risulteranno preziose, ad esempio, quando si dovranno affrontare questioni di calcolo delle probabilità nelle ipotesi che lo spazio dei risultati sia finito e che i risultati elementari siano tutti equiprobabili.

Teorema 14.1.1 (*principio di addizione*)

Siano $m, n \in \mathbb{Z}^+$. Supponiamo che una certa attività possa essere svolta in m modi diversi, e un'altra attività possa essere svolta in n modi tutti diversi fra loro e dai primi m. Allora il numero dei modi diversi in cui si può svolgere l'una o l'altra delle due attività è $m + n$.

Dimostrazione – La possibilità di svolgere la seconda attività in alternativa alla prima aggiunge gli n modi in cui essa può essere svolta agli m modi in cui può essere svolta la prima.

Teorema 14.1.2 (*principio di moltiplicazione*)

Siano $m, n \in \mathbb{Z}^+$. Supponiamo che una certa attività possa essere svolta in m modi diversi fra loro, e che dopo averla svolta in uno qualsiasi di tali modi un'altra attività possa essere svolta in n modi diversi fra loro (ma non necessariamente diversi dai precedenti m). Allora il numero dei modi diversi in cui si possono svolgere una dopo l'altra le due attività è $m \cdot n$.

Dimostrazione – Procediamo per induzione su n.

Se n $= 1$, c'è un solo modo nel quale si può svolgere la seconda attività, quindi l'unica discrezionalità è nella scelta di come svolgere la prima: il numero dei modi in cui si può fare questa scelta, cioè m, è anche il numero dei modi in cui si possono svolgere una dopo l'altra le due attività. L'asserto è dunque vero se $n = 1$.

Supponiamo ora vero l'asserto quando la seconda attività può essere svolta in n modi diversi, e dimostriamolo nel caso in cui la seconda attività B può essere svolta in $n + 1$ modi diversi. Scegliamo n di tali modi, e indichiamo con B_0 l'attività consistente nell'effettuare uno di tali n svolgimenti e con B_1 l'attività consistente nell'effettuare lo svolgimento rimanente. Sia A la prima attività, che per ipotesi si può svolgere in m modi diversi, e siano

– C_0 l'attività consistente nello svolgere prima A e poi B_0; essa può venire svolta, per l'ipotesi di induzione, in mn modi diversi;

– C_1 l'attività consistente nello svolgere prima A e poi B_1; essa può venire svolta, come si è visto nel paragrafo precedente, in m modi diversi.

Svolgere prima l'attività A e poi la B equivale a svolgere una o l'altra delle due attività C_0 e C_1. Poiché i modi in cui può essere svolta l'attività C_1 sono tutti distinti fra loro (nella parte iniziale, relativa ad A) e dai modi in cui si può svolgere l'attività C_0 (nella parte finale, essendo l'unico modo in cui si può svolgere l'attività B_1 diverso da ciascuno di quelli in cui si può svolgere l'attività B_0) si può applicare il principio di addizione per concludere che le due attività A e B una dopo l'altra possono essere svolte in $mn + m$ ($= m(n + 1)$) modi diversi, come si voleva dimostrare.

In tutto questo capitolo, ***supporremo fissato un insieme finito*** $A_n = \{a_1, a_2, \ldots, a_n\}$. È ovvio, e lo osserviamo una volta per tutte, che quanto diremo non dipende in alcun modo dalla "natura" degli elementi $a_1, a_2, \ldots, a_n$ ma solo dal numero naturale n; in particolare, non perdiamo in generalità nel ragionamento "etichettando" gli elementi di A_n con i numeri naturali da 1 a n (come abbiamo fatto apponendovi l'indice).

14.2 - *k*-disposizioni con ripetizione.

Il Totocalcio è un concorso a premi istituito in Italia nel 1946, il cui obiettivo è la previsione degli esiti di (attualmente, 2019) 14 partite di calcio riportate, ogni settimana, nel tagliando di gioco denominato "schedina". Per ogni partita (indicata con la coppia ordinata delle squadre in gara) si deve marcare 1 se si prevede la vittoria della prima squadra, X se si prevede un pareggio, 2 se invece si prevede la vittoria della seconda squadra. La sequenza ordinata delle 14 previsioni (1, X oppure 2) è detta un *pronostico*.

Quanti sono i pronostici possibili?

Si tratta di contare le 14 – ple ordinate dell'insieme $A_3 := \{1, X, 2\}$, le quali in questo contesto assumono una denominazione particolare.

Sia k un numero intero positivo.

Si dice *k-disposizione* (*con ripetizione*) di $a_1, a_2, \ldots, a_n$ (o anche *disposizione di $a_1, a_2, \ldots, a_n$ a k a k*) ogni k-pla ordinata di elementi di A_n (cioè ogni elemento del prodotto cartesiano $(\mathrm{A}_n)^k$).

Naturalmente l'espressione "con ripetizione" (che infatti abbiamo scritto fra parentesi) sta ad indicare la possibilità, non l'obbligatorietà che qualche elemento di A_n compaia più volte nella k-pla; le "ripetizioni" sono forzate solo se $k > n$ (come accade per i pronostici del Totocalcio).

Teorema 14.2.1

Per ogni $k \in \mathbb{Z}^+$, il numero delle k-disposizioni (con ripetizione) di $a_1, a_2, \ldots, a_n$ è n^k.

Dimostrazione – In funzione di k, indichiamo con $\mathbf{D}_k$ il numero delle $k-$ disposizioni (con ripetizione) di $a_1, a_2, \ldots, a_n$. Osserviamo in primo luogo che

(*) $$\mathbf{D}_{k+1} = n \cdot \mathbf{D}_k.$$

Infatti le $(k+1)-$ disposizioni $(x_1, x_2, x_3, \ldots x_k, x_{k+1})$ di $a_1, a_2, \ldots, a_n$ si possono "raggruppare" secondo l'ultimo elemento (cioè x_{k+1}): ogni possibile scelta di x_{k+1} (scelta che può avvenire in n modi diversi, cioè tanti quanti sono gli a_j) vede ai primi k posti una delle $\mathbf{D}_k$ $k-$ disposizioni (con ripetizione) di $a_1, a_2, \ldots, a_n$, da cui la (*) per il principio di moltiplicazione.

Proviamo allora l'asserto procedendo per induzione su k.

Se $k = 1$, è immediato che le 1-disposizioni di $a_1, a_2, \ldots, a_n$ sono n. Supponiamo allora (ipotesi di induzione) che le $k-$ disposizioni siano n^k; per la (*), le $(k+1)-$ disposizioni semplici di $a_1, a_2, \ldots, a_n$ sono n^{k+1} e l'asserto è completamente provato.

Per il teorema 14.2.1, i possibili pronostici del Totocalcio sono 3^{14} ($= 4\,782\,969$).

Esercizio 14.2.2

Il codice di accesso a una banca dati è una sequenza ordinata di cinque caratteri alfanumerici (lettere dell'alfabeto inglese e cifre). Quanti sono i codici possibili?

Soluzione – Sono tanti quante le disposizioni con ripetizione di 36 $(= 26 + 10)$ oggetti a 5 a 5, cioè $36^5 = 60.466.176$.

Esercizio 14.2.3

In una nazione, le automobili sono targate con sequenze ordinate di sei cifre; in un'altra, con sequenze ordinate di cinque caratteri alfanumerici escludendo le lettere "I", "O", "Q", "B" che possono dar luogo ad ambiguità di lettura da lontano. Quante auto possono essere targate con questi metodi?

Soluzione – Col primo metodo si possono targare 10^6 $(= 1.000.000)$ auto; col secondo, $32^5 = 33.554.432$.

14.3 - *k*-disposizioni semplici.

A partire dall'ultimo decennio del ventesimo secolo lo stato italiano consente le scommesse sugli avvenimenti sportivi anche in forma più generale rispetto al "Totocalcio" (a cui si è accennato nella sez. 14.2). È possibile, ad esempio, scommettere su quali saranno le squadre che occuperanno rispettivamente i primi cinque posti in classifica al termine del Campionato di calcio di prima serie. In questo contesto, chiameremo *pronostico* una $5-$pla ordinata di squadre di calcio della prima serie italiana tutte diverse fra loro. Analogamente a quanto si è fatto all'inizio della sez. 14.2 ci chiediamo: per una siffatta scommessa, quanti sono i diversi pronostici possibili?

Questa volta A_n è l'insieme delle squadre di prima serie del campionato italiano di calcio (cosicché, ad oggi, $n = 20$) e consideriamo particolari $5-$disposizioni degli elementi di A_n: quelle in cui tutti gli elementi sono diversi fra loro. Esse assumono il nome particolare di $k-$ *disposizioni semplici*, e ne diamo adesso la definizione precisa.

Sia $k \in \mathbb{Z}^+$ con $k \leq n$.

Si dice $k-$ *disposizione semplice* di $a_1, a_2, \ldots, a_n$ (o anche *disposizione semplice di* $a_1, a_2, \ldots, a_n$ *a k a k*) ogni $k-$pla ordinata di elementi di A_n tutti distinti fra loro.

Teorema 14.3.1

Per ogni $k \in \mathbb{Z}^+$, $k \leq n$, il numero delle $k-$disposizioni semplici di $a_1, a_2, \ldots, a_n$ è

$$n \cdot (n-1) \cdot \ldots \cdot (n-k+1)\,.$$

Dimostrazione – In funzione di k e n, indichiamo con $\mathbf{D}_k^n$ il numero delle $k-$disposizioni semplici di n oggetti. Osserviamo in primo luogo che (se $k < n$)

(*) $$\mathbf{D}_{k+1}^n = n \cdot \mathbf{D}_k^{n-1}.$$

Infatti le $(k+1)-$disposizioni semplici $(x_1, x_2, x_3, \ldots x_k, x_{k+1})$ di $a_1, a_2, \ldots, a_n$ si possono "raggruppare" secondo il primo elemento (cioè x_1): ogni possibile scelta di x_1 (scelta che può avvenire in n modi diversi, cioè tanti quanti sono gli a_j) vede ai successivi k posti una delle $\mathbf{D}_k^{n-1}$ $k-$disposizioni semplici dei restanti $n-1$ a_j, da cui la (*) per il principio di moltiplicazione.

Proviamo ora l'asserto procedendo per induzione su k.

Se $k = 1$, è immediato che le $1-$disposizioni semplici di $a_1, a_2, \ldots, a_n$ sono n. Supponiamo allora (ipotesi di induzione) che le $k-$disposizioni semplici di n oggetti siano $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ (e le $k-$disposizioni semplici di $n-1$ oggetti siano $(n-1) \cdot \ldots \cdot ((n-1)-(k-1))$, cioè $(n-1) \cdot \ldots \cdot (n-k)$).

Allora le $(k+1)-$disposizioni semplici di n oggetti sono, ricordando la (*),

$$n \cdot (n-1) \cdot \ldots \cdot (n-k)$$

e dunque l'asserto è completamente provato.

Per il teorema 14.3.1, i possibili pronostici sulle squadre che occuperanno rispettivamente i primi cinque posti in classifica al termine del Campionato di serie A sono

$$20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \ (= 1\,860\,480).$$

Particolare importanza riveste il caso $k = n$: il problema non è in questo caso quello di scegliere gli elementi (vanno presi tutti!) ma quello di ordinarli. Il numero dei modi distinti in cui ciò si può fare in base al teorema 14.3.1 è $n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$: si tratta del prodotto dei primi n numeri naturali, cioè si tratta (cfr. esercizio 3.9.6) di quel numero che abbiamo indicato con la scrittura $n!$.

In effetti, la nozione di "fattoriale" consente di riformulare il teorema 14.3.1 anche nel caso più generale:

Teorema 14.3.2

Sia k un numero intero positivo minore o uguale a n.
Il numero delle disposizioni semplici di n oggetti a k a k è $\frac{n!}{(n-k)!}$.

Dimostrazione – Basta ricordare che, per definizione (cfr. esempio 3.9.5), si ha $0! = 1! = 1$.

Osservazione 14.3.3

Ricordiamo (cfr. sez. 5.1) che si dice *permutazione* su A_n ogni corrispondenza biunivoca $A_n \to A_n$. Ogni permutazione π di A_n individua una n-disposizione semplice di $a_1, a_2, \ldots, a_n$, precisamente la

$$(\ \pi(a_1), \pi(a_2), \ldots, \pi(a_n)\ );$$

è chiaro che permutazioni distinte individuano n – disposizioni distinte e che si ottengono così tutte le n – disposizioni semplici di $a_1, a_2, \ldots, a_n$. Ciò si esprime a volte dicendo che *i due concetti* (permutazione su A_n, n – disposizione semplice di $a_1, a_2, \ldots, a_n$) *sono equivalenti*.

Teorema 14.3.4

Il numero delle permutazioni su n oggetti è $n!$.

Dimostrazione – Segue dall'oss. 14.3.3 applicando il teorema 14.3.2 per $k := n$.

Esercizio 14.3.5

Quante bandiere tricolori (formate da tre bande verticali colorate) si possono formare con cinque colori assegnati?

Soluzione – La risposta è: $5 \cdot 4 \cdot 3 = 60$.

Esercizio 14.3.6

Quante sono le possibili classifiche finali di un campionato di calcio a 20 squadre? Naturalmente prescindiamo, anche qui, dalle capacità agonistiche delle squadre.

Soluzione – La risposta è: $20!$ ($\simeq 2{,}433 \cdot 10^{18}$).

Esercizio 14.3.7

Una certa emittente televisiva privata trasmette solo film. In quanti modi diversi può organizzare un palinsesto di 5 film scegliendoli tra 7 titoli?

Soluzione – La risposta è: $\frac{7!}{2!}$ ($= 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2.520$).

Esercizio 14.3.8

Quanti anagrammi (a prescindere dal senso) si possono ottenere dalla parola "ramo"? E dalla parola "mamma"? E dalla parola "babbo"?

Soluzione – Gli anagrammi di "ramo" sono tanti quante le permutazioni su 4 oggetti, ossia $4!$ ($= 24$).

Se però anagrammiamo la parola "mamma", o la parola "babbo", non ha senso distinguere fra loro gli anagrammi che differiscono per una permutazione sulle tre "m", sulle due "a" o sulle tre "b"; conviene affrontare questo tipo di problemi utilizzando direttamente il principio di moltiplicazione. Ci servono però alcune nozioni che introdurremo nella prossima sezione, quindi riprenderemo la questione nell'esercizio 14.4.9 .

Una trattazione più generale di questo tipo di problema sarà data nell'osservazione 14.4.10.

14.4 - *k*-combinazioni semplici.

Il Superenalotto è un concorso a premi istituito in Italia nel 1997, il cui obiettivo è la previsione di 6 numeri interi estratti *senza reimbussolamento* ([23]) fra quelli dell'intervallo $[1, 90]$ (cfr. 4.3). I 6 numeri vanno riportati nel tagliando di gioco, usualmente denominato "schedina". In questo contesto, l'insieme dei 6 numeri riportati su ciascuna schedina è detto un *pronostico*.

Come nelle sezioni 14.2 e 14.3, ci chiediamo: quanti sono i pronostici possibili?

Si noti che i numeri su ciascuna schedina vengono disposti in ordine strettamente crescente: ciò significa che dobbiamo formare tutti i possibili raggruppamenti di 6 numeri distinti (scelti tra 1 e 90) senza poterli distinguere in base all'ordine in cui vengono scritti (perché tale ordine resta univocamente determinato dalla scelta dei numeri).

Sia k un numero naturale minore o uguale a n.

Si dice *k-combinazione semplice* di $a_1, a_2, \ldots, a_n$ (o anche *combinazione semplice di* $a_1, a_2, \ldots, a_n$ *a* k *a* k) ogni k-pla ordinata $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$ per la quale sia $i_1 < i_2 < \ldots < i_k$.

È utile (lo vedremo più avanti) formalizzare la definizione di k-combinazione semplice utilizzando, come abbiamo fatto, la nozione di k-pla ordinata; bisogna però aver ben chiaro che l'ordinamento è determinato dagli elementi, e quindi le k-combinazioni semplici sono individuate solo dalla scelta degli elementi, e non dal loro ordinamento. Lo ribadiamo col seguente teorema:

Teorema 14.4.1

Le k-combinazioni semplici di $a_1, a_2, \ldots, a_n$ sono in corrispondenza biunivoca con i sottoinsiemi di $\{a_1, a_2, \ldots, a_n\}$ che hanno cardinalità k.

Dimostrazione – Sia $\mathcal{C}$ l'insieme delle k-combinazioni semplici di $a_1, a_2, \ldots, a_n$, e sia $\mathcal{S}$ l'insieme dei sottoinsiemi di A_n formati da k elementi.

Sia $\mathbf{f}: \mathcal{C} \to \mathcal{S}$ la funzione che alla k-combinazione semplice $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ associa l'insieme $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$ (poiché per ipotesi $i_1 < i_2 < \ldots < i_k$, gli elementi $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ sono tutti distinti e dunque effettivamente $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\} \in \mathcal{S}$).

Proviamo che **f** è suriettiva: se $\{a_{j_1}, a_{j_2}, \ldots, a_{j_k}\} \in \mathcal{S}$, riordinando opportunamente i suoi elementi possiamo ottenere una k-combinazione semplice, la cui immagine mediante **f** è proprio $\{a_{j_1}, a_{j_2}, \ldots, a_{j_k}\}$.

Proviamo infine che **f** è iniettiva: k-combinazioni semplici che hanno la stessa immagine mediante **f** sono formate dagli stessi elementi; poiché tali elementi possono essere ordinati in un solo modo rispettando la condizione che gli indici siano strettamente crescenti, le k-combinazioni semplici da cui eravamo partiti devono coincidere.

[23] Ciò significa che il primo numero viene estratto fra i 90 numeri interi compresi nell'intervallo $[1, 90]$, il secondo fra gli 89 numeri interi restanti, il terzo fra gli 88 numeri interi restanti, e così via. In particolare, i 6 numeri interi estratti sono certamente tutti diversi.

Teorema 14.4.2

Sia k un numero naturale minore o uguale a n.
Il numero delle k-combinazioni semplici di $a_1, a_2, \ldots, a_n$ è $\frac{n!}{k!\cdot(n-k)!}$.

Dimostrazione – Sia $\mathcal{D}$ l'insieme delle k-disposizioni semplici di $a_1, a_2, \ldots, a_n$. Definiamo in $\mathcal{D}$ la seguente relazione:

$(a_{i_1}, a_{i_2}, \ldots, a_{i_k}) \sim (a_{j_1}, a_{j_2}, \ldots, a_{j_k})$ se e solo se esiste una permutazione π su $i_1, i_2, \ldots, i_k$
tale che $\pi(i_1) = j_1, \pi(i_2) = j_2, \ldots, \pi(i_k) = j_k$.

Si verifica facilmente che $\sim$ è una relazione di equivalenza su $\mathcal{D}$, e che ogni k-combinazione semplice appartiene ad una e una sola classe di equivalenza. Ogni classe di equivalenza ha $k!$ elementi (perchè le permutazioni su k oggetti sono $k!$, cfr. 14.3.2), dunque le classi di equivalenza sono

$$\frac{|\mathcal{D}|}{k!} = \frac{n!}{k!\cdot(n-k)!}.$$

Questo è anche il numero delle k-combinazioni semplici di $a_1, a_2, \ldots, a_n$.

Sia k un numero naturale minore o uguale a n. Il numero

$$\frac{n!}{k!\cdot(n-k)!}$$

si indica con $\binom{n}{k}$ (leggi: "n su k"). Tutti i numeri della forma $\binom{n}{k}$ (con $k \leq n$) si dicono *coefficienti binomiali*.

Possiamo così riformulare il teorema 14.4.2:

Teorema 14.4.3

Sia k un numero naturale minore o uguale a n.
Il numero delle $k-$ combinazioni semplici di $a_1, a_2, \ldots, a_n$ è $\binom{n}{k}$.

Dunque, il numero dei possibili pronostici al Superenalotto è

$$\binom{90}{6} = \frac{90\cdot89\cdot88\cdot87\cdot86\cdot85}{6\cdot5\cdot4\cdot3\cdot2} = 622\,614\,630.$$

Esempio 14.4.4

Sia X un insieme che ha esattamente 24 elementi. Il numero dei sottoinsiemi di X che hanno esattamente 8 elementi è

$$\binom{24}{8} = \frac{24\cdot23\cdot22\cdot21\cdot20\cdot19\cdot18\cdot17}{8\cdot7\cdot6\cdot5\cdot4\cdot3\cdot2} = 735\,471.$$

Il teorema che segue espone le relazioni più importanti che intercorrono fra i coefficienti binomiali: su di esse, fra l'altro, è fondata una importante regola pratica per il calcolo degli stessi.

Teorema 14.4.5

Sia k un numero naturale minore o uguale a n. Si ha

$$(a)\ \binom{n}{k} = \binom{n}{n-k}; \qquad (b)\ \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1};$$

$$(c)\ k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}; \qquad (d)\ \binom{n}{0} = 1.$$

Dimostrazione – Si tratta di semplici verifiche.

Proviamo la (a).

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

Proviamo la (b). Si ha

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

Riduciamo allo stesso denominatore le due frazioni al secondo membro; a tale scopo, moltiplichiamo la prima per $\frac{n-k}{n-k}$ e la seconda per $\frac{k}{k}$.

Si ottiene

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

Proviamo la (c). Si ha

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

Proviamo infine la (d). Si ha

$$\binom{n}{0} = \frac{n!}{0!\cdot(n-0)!} = \frac{n!}{n!} = 1.$$

Applicando le relazioni espresse dal teorema 14.4.5 si costruisce il *triangolo di Tartaglia* (detto anche *triangolo di Pascal*), riportando su righe successive i coefficienti binomiali $\binom{n}{k}$ in modo che (numerando le righe con 0, 1, 2, ...) la riga n-sima consista nell'ordine dei numeri $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$.

Precisamente:

– Il primo e ultimo numero di ogni riga è 1 (per la (c) del teorema 14.4.5, tenendo conto della (a));

– Ogni numero di ciascuna riga, eccetto il primo e l'ultimo, è la somma dei due numeri immediatamente soprastanti (per la (b) del teorema 14.4.5);

– Lo schema è simmetrico rispetto a un asse di simmetria verticale (per la (a) del teorema 14.4.5).

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 \quad 1 \\
\multicolumn{11}{c}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots}
\end{array}
$$

Teorema 14.4.6

Se $a, b \in \mathbb{R}$ e $n \in \mathbb{N}\backslash\{0\}$, si ha

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

Dimostrazione – Valutiamo $(a+b)^n$. Si ha

$$(a+b)^n = (a+b)\cdot(a+b)\cdot\ldots\cdot(a+b) \quad (n \text{ volte}).$$

L'espressione al secondo membro si sviluppa nella somma di prodotti ottenuti scegliendo uno dei due termini a, b per ciascuno degli n fattori in tutti i modi possibili. Tali prodotti, per la proprietà commutativa della moltiplicazione, si possono scrivere tutti nella forma $a^k b^{n-k}$ (notiamo che la somma degli esponenti deve essere n).
Fissiamo l'attenzione su un particolare valore di k: quante diverse scelte dei termini a, b danno luogo al prodotto $a^k b^{n-k}$? "Etichettiamo" ogni fattore $(a+b)$ con un a_i ($i = 1, \ldots, n$); ogni scelta che comprende esattamente k volte "a" corrisponde a un sottoinsieme di A_n di cardinalità k (formato da quei k elementi che "etichettano" i fattori dai quali è stato scelto "a"): dunque (per 14.4.1 e 14.4.3) nello sviluppo di $(a+b)^n$ vi sono esattamente $\binom{n}{k}$ termini della forma $a^k b^{n-k}$. Da ciò segue l'asserto.

Dimostrazione alternativa – Possiamo in alternativa procedere per induzione su n. L'asserto è ovvio se $n = 1$, dunque supponiamo sia vero per n e proviamolo per $n+1$. Si ha che

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

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

Posto $h := k+1$, da cui $k = h-1$, si ha

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

e scrivendo di nuovo k in luogo di h si è trovato che

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

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

(per la (b) del teorema 14.4.5)

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

cioè l'asserto per $n+1$, come si voleva.

I coefficienti binomiali hanno questo nome proprio perché compaiono come coefficienti negli sviluppi delle potenze di un binomio.

Teorema 14.4.7

$|\mathcal{P}(\mathrm{A}_n)| = 2^n$.

Dimostrazione – Per ogni numero naturale $k \leq n$, esistono esattamente $\binom{n}{k}$ sottoinsiemi di A_n aventi cardinalità k (cfr. 14.4.1 e 14.4.3). Dunque,

$$|\mathcal{P}(\mathbf{A}_n)| = \sum_{k=0}^{n} \binom{n}{k}.$$

D'altro lato, applicando il teorema 14.4.6 con $a = b = 1$, si ottiene

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = (1+1)^n = 2^n.$$

Esercizio 14.4.8

Si dimostri il teorema 14.4.7 procedendo per induzione su n.

Esercizio 14.4.9

Quanti anagrammi (a prescindere dal senso) si possono ottenere dalla parola "mamma"? E dalla parola "babbo"?

Soluzione – Per "riordinare" la parola "mamma" è sufficiente assegnare il posto alle tre lettere "m" (nei rimanenti due posti collocheremo le due lettere "a"). I modi in cui si possono scegliere tre posti fra cinque a disposizione sono tanti quanti i modi in cui si può scegliere un sottoinsieme formato da tre elementi in un insieme di cinque elementi, cioè (teorema 14.4.1 e teorema 14.4.2) sono $\binom{5}{3} = 10$.

Per "riordinare" la parola "babbo" conviene procedere in due passi (e applicare il principio di moltiplicazione). Prima si assegnano i posti alle tre lettere "b" (e abbiamo visto che, su cinque posti a disposizione, questo si può fare in 10 modi diversi), poi nei due posti rimasti disponibili sistemiamo le due lettere "a" e "o" (e questo si può fare in $2! = 2$ modi diversi). Applicando il principio di moltiplicazione, si trova che (a prescindere dal senso) gli anagrammi effettivamente diversi della parola "babbo" sono $10 \cdot 2 = 20$.

Osservazione 14.4.10

Se abbiamo n oggetti dei quali k_1 sono tutti uguali fra loro, k_2 sono tutti uguali fra loro, …, k_s sono tutti uguali da loro, il numero delle $n-$ple ordinate effettivamente distinte che si possono formare con tali oggetti è

$$\frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_s!} .$$

Dimostrazione – Per formare le $n-$ple ordinate, procediamo per passi applicando poi il principio di moltiplicazione.

Primo passo: scegliamo il posto dei primi k_1 oggetti; questo si può fare in $\binom{n}{k_1}$ modi diversi.

Secondo passo: scegliamo il posto dei successivi k_2 oggetti; poiché sono rimasti disponibili $n - k_1$ posti, questo si può fare in $\binom{n-k_1}{k_2}$ modi diversi.

Terzo passo: scegliamo il posto dei successivi k_3 oggetti; poiché sono rimasti disponibili $n - k_1 - k_2$ posti, questo si può fare in $\binom{n-k_1-k_2}{k_3}$ modi diversi.

Si procede così per s passi, sistemando i primi $k_1 + k_2 + \ldots + k_s$ oggetti. Per il principio di moltiplicazione, ripetutamente applicato, ciò si può fare in

$$\binom{n}{k_1} \cdot \binom{n-k_1}{k_2} \cdot \binom{n-k_1-k_2}{k_3} \cdot \ldots \cdot \binom{n-k_1-k_2\ldots-k_{s-1}}{k_s}$$

modi diversi.

Nei rimanenti $n - k_1 - k_2 \ldots - k_{s-1}$ posti sistemiamo infine i restanti oggetti; questo si può fare in $(n - k_1 - k_2 \ldots - k_{s-1})!$ modi diversi. Applicando ancora una volta il principio di moltiplicazione, si trova che il numero delle $n-$ple ordinate effettivamente distinte che si possono formare con gli n oggetti dati è

$$\binom{n}{k_1} \cdot \binom{n-k_1}{k_2} \cdot \binom{n-k_1-k_2}{k_3} \cdot \ldots \cdot \binom{n-k_1-k_2\ldots-k_{s-1}}{k_s} \cdot (n - k_1 - k_2 \ldots - k_{s-1})! =$$

$$= \frac{n!}{k_1!\cdot(n-k_1)!} \cdot \frac{(n-k_1)!}{k_2!\cdot(n-k_1-k_2)!} \cdot \frac{(n-k_1-k_2)!}{k_3!\cdot(n-k_1-k_2-k_3)!} \cdot \frac{(n-k_1-\ldots-k_{s-1})!}{k_s!\cdot(n-k_1-k_2-\ldots-k_s)!} \cdot (n - k_1 - k_2 \ldots - k_{s-1})! =$$

$$= \frac{n!}{k_1!\cdot k_2!\cdot\ldots\cdot k_s!} \cdot$$

14.5 - *k*-combinazioni con ripetizione.

Supponiamo di avere a disposizione una quantità illimitata di palline di tre colori: rosso, verde, azzurro. Quanti sacchetti "diversi" di sette palline possiamo formare? (Due sacchetti si considerano "diversi" se differiscono per il numero delle palline di uno almeno dei tre colori). È chiaro che questo non può essere interpretato come un problema di *disposizioni* dei tre colori dati (l'ordine delle palline non conta!); non si tratta però nemmeno di *combinazioni semplici*, perché i colori possono (in questo esempio, devono) essere ripetuti.

Se l'esempio delle palline colorate sembra troppo frivolo, si pensi a quest'altro problema: quanti termini ha il polinomio omogeneo generale di grado sette nelle tre indeterminate x, y, z? La risposta è data dal numero dei monomi "diversi" della forma $x^\alpha y^\beta z^\gamma$ con α, β, $\gamma \in \mathbb{N}$ e $\alpha + \beta + \gamma = 7$; ciascuno di questi monomi è un "sacchetto" di sette lettere scelte tra x, y, z. Questo problema ha dunque la stessa soluzione del precedente.

Sia k un numero intero positivo.

Si dice *k-combinazione con ripetizione* di a_1, a_2, …, a_n (o anche *combinazione con ripetizione di a_1, a_2, …, a_n a k a k*) ogni k-pla ordinata $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ per la quale sia

$$i_1 \leq i_2 \leq \ldots \leq i_k.$$

Notiamo che in questa definizione, come già in quella di k-combinazione semplice, la scelta degli elementi a_{i_j} determina il loro ordinamento; solo tale scelta caratterizza dunque le k-combinazioni.

Teorema 14.5.1

Sia k un numero intero positivo.

Il numero delle k-combinazioni con ripetizione di $a_1, a_2, \ldots, a_n$ è

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

Dimostrazione – Sia $\mathcal{C}^{(r)}$ l'insieme delle k-combinazioni con ripetizione di $a_1, a_2, \ldots, a_n$, e sia $\mathcal{K}$ l'insieme delle k-combinazioni semplici di $1, 2, \ldots, n+k-1$.

Per provare l'asserto, sarà sufficiente dimostrare che la funzione $\mathbf{f}: (A_n)^k \to \mathbb{N}^k$ che alla k-pla ordinata $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ associa la k-pla ordinata $(i_1, i_2+1, i_3+2, \ldots, i_k+k-1)$ è una corrispondenza biunivoca tra $\mathcal{C}^{(r)}$ e $\mathcal{K}$.

Osserviamo in primo luogo che $\mathbf{f}(\mathcal{C}^{(r)}) \subset \mathcal{K}$. In effetti, se

$$1 \le i_1 \le i_2 \le i_3 \le \ldots \le i_k \le n,$$

si ha certamente

$$1 \le i_1 < i_2 + 1 < i_3 + 2 < \ldots < i_k + k - 1 \le n + k - 1.$$

Inoltre, **f** è iniettiva (se due k-combinazioni con ripetizione differiscono per la j-sima componente, ciò avviene anche per le corrispondenti $(n+k-1)$-combinazioni).

Resta da provare che **f** è suriettiva. Sia $(j_1, j_2, \ldots, j_k) \in \mathcal{K}$; allora

$$1 \le j_1 < j_2 < \ldots < j_k \le n + k - 1,$$

da cui

$$1 \le j_1 \le j_2 - 1 \le j_3 - 2 \le \ldots \le j_k - k + 1$$

e quindi

$$(a_{j_1}, a_{j_2-1}, a_{j_3-2}, \ldots, a_{j_k-1}) \in \mathcal{C}^{(r)};$$

ma

$$\mathbf{f}(a_{j_1}, a_{j_2-1}, a_{j_3-2}, \ldots, a_{j_k-k+1}) = (j_1, j_2, \ldots, j_k)$$

e l'asserto risulta così completamente provato.

Siamo in grado ora di risolvere il problema (anzi, i due problemi) da cui eravamo partiti.

La risposta è

$$\binom{3+7-1}{7} = \binom{9}{7} = \frac{9!}{7!\cdot 2!} = \frac{9\cdot 8}{2} = 36.$$

Esercizio 14.5.2

Quanti sono i numeri di 6 cifre nei quali ogni cifra è maggiore o uguale alla successiva? (Sono esempi di tali numeri: 755420, 555555, 654311.)

Soluzione – I numeri considerati restano individuati dalle 6-combinazioni con ripetizione delle 10 cifre (bisogna escludere la $(0, 0, 0, 0, 0, 0)$, che non corrisponde a un numero di sei cifre); sono dunque

$$\binom{10+6-1}{6} - 1 = \binom{15}{6} - 1 = \frac{15!}{6!\cdot 9!} - 1 = \frac{15\cdot 14\cdot 13\cdot 12\cdot 11\cdot 10}{6\cdot 5\cdot 4\cdot 3\cdot 2} - 1 = 5\,004\,.$$

Esercizio 14.5.3

Quante soluzioni in $\mathbb{N}^7$ ha l'equazione

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 100 \quad ?$$

Soluzione – Se pensiamo di avere a disposizione una quantità illimitata di palline (o di oggetti di qualsiasi natura) ciascuna etichettata con uno dei sette simboli x_1, x_2, x_3, x_4, x_5, x_6 e x_7, ogni soluzione dell'equazione considerata si può identificare con un "sacchetto" formato da 100 di queste palline (e soluzioni diverse corrispondono a diverse composizioni del sacchetto). Per quanto osservato all'inizio della sezione, il numero cercato è dunque il numero delle 100 – combinazioni con ripetizione di 7 oggetti, ossia

$$\binom{100+7-1}{100} = \binom{106}{100} = \frac{106!}{6!\cdot 100!} = \frac{106\cdot 105\cdot 104\cdot 103\cdot 102\cdot 101}{6\cdot 5\cdot 4\cdot 3\cdot 2} =$$
$$= 1\,705\,904\,746\,.$$

14.6 - Esercizi di ricapitolazione.

14.6.1

È dato un insieme finito **X**. Se il numero dei sottoinsiemi di **X** che hanno cardinalità 5 è uguale al numero dei sottoinsiemi di **X** che hanno cardinalità 3, qual è la cardinalità di **X**?

Soluzione – Sia $|\mathbf{X}| = n$. Per ipotesi, $\binom{n}{5} = \binom{n}{3}$, ossia

$$\frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)\cdot(n-4)}{5\cdot 4\cdot 3\cdot 2} = \frac{n\cdot(n-1)\cdot(n-2)}{3\cdot 2}$$

da cui $$(n-3)\cdot(n-4) = 20.$$

Tale equazione di secondo grado nell'incognita n ha la sola radice positiva $n = 8$. Dunque

$$|\,\mathbf{X}\,| = 8.$$

14.6.2

Sono dati nel piano 10 punti, fra i quali non ve ne sono tre allineati. Quante rette si ottengono congiungendoli a due a due? Quanti triangoli hanno tutti i vertici fra quei punti?

Soluzione – Due punti individuano una retta; poiché fra i punti dati non ve ne sono tre allineati, coppie distinte di punti individuano rette distinte. Dunque si ottengono

$$\binom{10}{2} = 45$$

rette.

I triangoli sono individuati dalla scelta dei vertici; il loro numero è quindi $\binom{10}{3} = 120$.

14.6.3

Quanti sono gli ambi che si possono giocare al lotto? Quanti di essi vengono estratti su ogni ruota? E i terni? E le cinquine?

Soluzione – Gli ambi che si possono giocare sono $\binom{90}{2} = 4005$. Di questi ne vengono estratti su ogni ruota $\binom{5}{2} = 10$.

I terni che si possono giocare sono $\binom{90}{3} = 117.480$. Di questi ne vengono estratti su ogni ruota $\binom{5}{3} = 10$.

Le cinquine che si possono giocare sono $\binom{90}{5} = 43.949.268$. Di queste ne viene estratta una su ogni ruota.

14.6.4

In quanti modi diversi possiamo allineare 8 segni " $+$ " e 3 segni " $-$ " in modo che due segni " $-$ " non siano mai adiacenti?

Soluzione – Scriviamo gli 8 segni " $+$ " intervallati da "x", come segue:

$$x + x + x + x + x + x + x + x + x\,.$$

I tre segni " $-$ " vanno sostituiti a tre delle "x", e scelte diverse delle tre "x" danno luogo ad allineamenti diversi. Dunque il numero dei possibili diversi allineamenti è uguale al numero dei modi diversi in cui possiamo scegliere tre elementi in un insieme di nove elementi, ossia $\binom{9}{3} = \binom{9}{6} = \frac{9 \cdot 8 \cdot 7}{3 \cdot 2} = 84$.