I NUMERI NATURALI

PREREQUISITI. Per la comprensione del testo sono richieste alcune nozioni elementari su insiemi, relazioni d'equivalenza e d'ordine, funzioni, operazioni, reperibili nel capitolo d'introduzione.

SCOPI. Ripasso di nozioni già note dal corso di Algebra I e dalla scuola secondaria.

Contenuti:

§ 1 Gli assiomi di Peano; operazioni, potenze, divisori e multipli, ordinamenti, il principio del minimo; sistemi di numerazione.

§ 2 I numeri cardinali: equipotenza, numeri cardinali, operazioni e loro proprietà, ordinamento; cardinali finiti; insiemi numerabili.

§ 3 Calcolo combinatorio: principio di addizione, principio dei cassetti, principio di moltiplicazione, funzioni iniettive e permutazioni, sottoinsiemi di un insieme, coefficienti binomiali ed applicazioni.

§ 4 I monoidi costruiti sui numeri naturali. Immersione di un monoide commutativo in un gruppo. Da da $\mathbf{N}$ a $\mathbf{Z}$ o da $\mathbf{N}$ a $\mathbf{Q}^+$.

§ 1. I numeri naturali secondo Peano

In queste pagine si richiama la definizione secondo Peano dell'insieme **N** = {0, 1, 2, ...} dei numeri naturali, rivisitata con un linguaggio più attuale; successivamente si introducono le operazioni di addizione e moltiplicazione di **N** e le relative relazioni d'ordine e ne sono descritte le proprietà principali.

Assiomi di Peano. L'insieme **N** dei numeri naturali può essere definito mediante gli assiomi di Peano, che, con il linguaggio degli insiemi, tradurremo nel modo seguente:

I. **N** contiene un elemento, indicato con 0.

II. E' definita una funzione iniettiva $\sigma : \mathbf{N} \xrightarrow{1\text{–}1} \mathbf{N}$, la cui immagine è $\mathbf{N} \setminus \{0\}$

III. Per ogni $M \subseteq \mathbf{N}$, se $0 \in M$ e se per ogni $n \in M$ anche $\sigma(n) \in M$, allora $M = \mathbf{N}$.

Per ogni $n \in \mathbf{N}$, l'elemento $\sigma(n)$ è detto *successivo* di n. Dalla proprietà II segue che **N** è infinito (si veda la sezione 2).

La proprietà III si chiama *principio d'induzione* e si usa in definizioni e dimostrazioni che coinvolgano una variabile $n \in \mathbf{N}$.

Le *dimostrazioni per induzione* seguono lo schema seguente: si debba provare un'affermazione P(n) che abbia senso per ogni numero naturale.

a) Si dimostra innanzitutto che è vera P(0).

b) Si dimostra che l'essere vera P(n) (*ipotesi induttiva*) implica che è vera P(σ(n)).

In tal modo l'insieme M dei numeri n per i quali P(n) è vera contiene 0 e per ogni $n \in M$ contiene anche σ(n). Dunque, per il principio d'induzione, $M = \mathbf{N}$.

Analogamente, la proprietà III serve per definire nozioni, secondo lo schema seguente (*definizioni ricorsive*): si debba definire una nozione, che denoteremo con D(n), e che abbia senso per ogni numero naturale.

a) Si definisce esplicitamente D(0).

b) Supposta definita D(n), si definisce mediante essa D(σ(n)).

In tal modo l'insieme M dei numeri n per i quali D(n) è definita contiene 0 e per ogni $n \in M$ contiene anche σ(n). Dunque, per il principio d'induzione, $M = \mathbf{N}$.

A volte si parte da un numero n_0 anziché da 0. In tal caso, l'affermazione P(n) sarà provata solo per ogni $n \geq n_0$. Analogamente per le definizioni D(n).

NOTA. In alcuni casi, per dimostrare un'affermazione P(n) si segue uno schema un po' diverso, detto *Il principio d'induzione*:

a) si dimostra P(0)

b) supposto vero P(k) per ogni $k \leq n$, si dimostra $P(\sigma(n))$.

Ciò posto, incominciamo con il definire le operazioni.

ADDIZIONE. Su **N** si può definire ricorsivamente la somma di un numero m con un numero n qualsiasi, nel modo seguente:

$$\text{poniamo: } \begin{cases} m+0=m \\ m+\sigma(n)=\sigma(m+n) \end{cases}$$

In tal modo, per la proprietà III, per ogni $m \in \mathbf{N}$ la *somma* m+n è definita per ogni $n \in \mathbf{N}$. Posto $1 = \sigma(0)$, si ottiene subito, per ogni $m \in \mathbf{N}$:

$$\sigma(m) = \sigma(m+0) = m+\sigma(0) = m+1.$$

Chiamiamo *addizione* l'operazione $+ : \mathbf{N}^2 \to \mathbf{N}$, $+ : (m,n) \mapsto m+n$, che associa a una coppia ordinata (m, n) di numeri naturali la loro somma.

PROPOSIZIONE 1.1. - L'addizione possiede le proprietà seguenti:

a) *associativa*: per ogni a, b, $c \in \mathbf{N}$ risulta: (a+b)+c = a+(b+c);

b) *elemento neutro*: per ogni $a \in \mathbf{N}$ si ha a+0 = 0+a = a;

c) *commutativa*: per ogni a, $b \in \mathbf{N}$ risulta a+b = b+a.

Dimostrazione.

a) L'uguaglianza è vera per c = 0, risultando (a+b)+0 = a+b = a+(b+0).

Supponendola provata per c = n (ipotesi induttiva), dimostriamo che è vera per $c = \sigma(n)$ nel modo seguente:

	(a+b)+c = (a+b)+σ(n) =
(per la definizione di +)	= σ((a+b)+n) =
(per l'ipotesi induttiva)	= σ(a+(b+n)) =
(per la definizione di +)	= a+σ(b+n) =
(ancora per la definizione di +)	= a+(b+σ(n)) = a+(b+c),

come si voleva.

b) Per definizione di + si ha a+0 = a. L'uguaglianza 0+a = a è vera ovviamente per a = 0. Supponendola provata per a = n, se a = σ(n) si ha:

$$0+a = 0+\sigma(n) = \sigma(0+n) = \sigma(n) = a.$$

c) La dimostrazione della proprietà commutativa è più complessa, occorrendo procedere per induzione rispetto ad entrambi gli addendi. Per b) è vera se a = 0. Sia vera per a = n e dimostriamo che è vera per a = σ(n). Per questo procediamo per induzione rispetto a b.

E' vera per definizione di + se b = 0. Sia vera per b = m. Per b = σ(m) si ha allora:

$$a+b = \sigma(n)+\sigma(m) = \sigma(\sigma(n)+m) =$$

(per l'ipotesi induttiva su b) $= \sigma(m+\sigma(n)) = \sigma(\sigma(m+n)) =$

(per l'ipotesi induttiva su a) $= \sigma(\sigma(n+m)) = \sigma(n+\sigma(m)) =$

(ancora per l'ipotesi induttiva su a) $= \sigma(\sigma(m)+n) = \sigma(m)+\sigma(n) = b+a,$

come si voleva.

PROPOSIZIONE 1.2. - Ulteriori proprietà dell'addizione.

a) Per ogni a, b∈**N**, se a+b = 0 allora a = b = 0.

b) *Legge di cancellazione*: per ogni a, b, c∈**N**, se a+b = a+c allora b = c.

c) Per ogni a, b∈**N**, una e, se a ≠ b, una sola delle due equazioni: $\begin{cases} a+x=b \\ b+y=a \end{cases}$, nelle incognite x ed y∈**N**, ha una ed una sola soluzione.

Dimostrazione. Sia a ≠ 0. Per induzione su b proviamo che a+b ≠ 0. Innanzitutto, a+0 = a ≠ 0. Sia a+n ≠ 0. Allora a+σ(n) = σ(a+n) ≠ 0 perché 0∉σ(**N**). Pertanto, può essere a+b = 0 solo se a = 0, ma allora b = 0+b = 0 implica b = 0.

b) Sia a+b = a+c. Se a = 0 si ha b = c. Sia vero per a = n. Allora, per a = σ(n) si ha: a+b = σ(n)+b = σ(n+b), e analogamente a+c = σ(n+c). Perciò, da a+b = a+c segue σ(n+b) = σ(n+c), da cui, per la iniettività di σ, si ha n+b = n+c. Per l'ipotesi induttiva segue allora b = c.

c). Per induzione rispetto a b proviamo che una delle due equazioni ha soluzione. Se b = 0 allora si ha y = a. Sia vero per b = n. Sia ora b = n+1. Se si aveva a+x = n, allora a+(x+1) = n+1 = b. Invece nel caso n+y = a, se y = 0 si ha anche a+0 = a, per cui siamo nel caso precedente; se y ≠ 0, allora y appartiene all'immagine di σ e quindi esiste z tale che z+1 = σ(z) = y. Allora b+z = (n+1)+z = n+(1+z) = n+y = a. Se risulta contemporaneamente a+x = b e b+y = a, per la proprietà associativa si ha: b+0 = b = a+x = (b+y)+x = b+(y+z), quindi per la legge di cancellazione si ha y+z = 0, ma per a) si ha y = z = 0 e quindi b = a. La soluzione è unica per la legge di cancellazione.

Sottrazione. Se risulta a+d = b, si pone b-a = d e d si chiama *differenza* di b ed a. In particolare si ha a-a = 0.

Moltiplicazione. Si definisce ricorsivamente l'operazione di *moltiplicazione* $\cdot$ definendo dapprima il *prodotto* di un m per un n qualsiasi, nel modo seguente (ricordando che $\sigma(n) = n+1$):

$$\text{per ogni } m, n \in \mathbf{N}, \text{ poniamo: } \begin{cases} m \cdot 0 = 0 \\ m \cdot (n+1) = m \cdot n + m \end{cases}.$$

Di conseguenza, per esempio, $m \cdot 1 = m \cdot (0+1) = m \cdot 0 + m = m$, ecc. Solitamente il prodotto di m per n si denota con mn, anziché con $m \cdot n$.

La moltiplicazione è l'operazione che ad ogni coppia (m,n) associa il prodotto $m \cdot n$.

PROPOSIZIONE 1.3. - Proprietà della moltiplicazione.

1) *Elemento assorbente*: per ogni $a \in \mathbf{N}$, $0 \cdot a = a \cdot 0 = 0$
2) *Elemento neutro*: per ogni $a \in \mathbf{N}$ si ha $a \cdot 1 = 1 \cdot a = a$.
3) *Distributiva* rispetto al +: per ogni a, b, $c \in \mathbf{N}$ risulta $\begin{cases} (a+b)c = ac + bc \\ a(b+c) = ab + ac \end{cases}$
4) *Associativa*: per ogni a, b, $c \in \mathbf{N}$ risulta $(ab)c = a(bc)$
5) *Commutativa*: per ogni a, $b \in \mathbf{N}$ risulta $ab = ba$.

Dimostrazione. 1) Basta provare che si ha $0 \cdot a = 0$. E' vera per $a = 0$. Sia vera per a, allora $0 \cdot \sigma(a) = 0 \cdot a + 0 = 0 + 0 = 0$, quindi è vero anche per $\sigma(a)$.

2) $a \cdot 1 = a \cdot \sigma(0) = a \cdot 0 + a = 0 + a = a$. Invece, $1 \cdot 0 = 0$ e, supposto $1 \cdot a = a$, allora si ha $1 \cdot \sigma(a) = 1 \cdot a + 1 = a + 1 = \sigma(a)$ e anche la 2) è dimostrata.

3) Vediamo la prima uguaglianza, ossia la *distributività a sinistra*. Se $c = 0$ entrambi i membri sono nulli, quindi per $c = 0$ l'uguaglianza è vera. Sia c un numero per il quale l'uguaglianza è vera. Allora, usando la definizione di prodotto, l'ipotesi su c e le proprietà della somma, si ha:

$$(a+b) \cdot \sigma(c) = (a+b) \cdot c + (a+b) = a \cdot c + a \cdot c + a + b =$$
$$= (a \cdot c + a) + (b \cdot c + b) = a \cdot \sigma(c) + b \cdot \sigma(c)$$

Vediamo la *distributività a destra*. Se $a = 0$ è vera. Sia vera per un $a \in \mathbf{N}$; allora, usando questa informazione, la proprietà di 1 e la prima uguaglianza, si ha:

$$\sigma(a) \cdot (b+c) = (a+1) \cdot (b+c) = a \cdot (b+c) + (b+c) = ab + ac + b + c =$$
$$= (a \cdot b + 1 \cdot b) + (a \cdot c + 1 \cdot c) = (a+1) \cdot b + (a+1) \cdot c = \sigma(a) \cdot b + \sigma(a) \cdot c$$

4) Per induzione su c: se $c = 0$ è vero. Sia c un numero per il quale si ha $(ab)c = a(bc)$. Allora, per la proprietà distributiva e l'ipotesi induttiva si ha:

$$(ab)\cdot\sigma(c) = (ab)\cdot c + ab = a\cdot(bc) + ab = a\cdot(bc + b) = a\cdot(b\cdot\sigma(c))$$

Quindi è vero anche per $\sigma(c)$.

5) E' vero se b = 0. Sia b tale che ab = ba. Allora:

$$a\cdot\sigma(b) = a\cdot b + a = b\cdot a + 1\cdot a = (b+1)\cdot a = \sigma(b)\cdot a$$

PROPOSIZIONE 1.4. - Ulteriori proprietà della moltiplicazione.

a) L'unico elemento dotato di *inverso* è 1, cioè per ogni a, b∈**N**, se a·b = 1 allora a = b = 1.

b) *Legge di annullamento del prodotto*: per ogni a, b∈**N** si ha a·b = 0 se e solo se a = 0 oppure b = 0.

Consideriamo ora il sottoinsieme $\mathbf{N}^+ = \mathbf{N}\setminus\{0\}$: la legge di annullamento del prodotto ha come conseguenza che se a, b∈$\mathbf{N}^+$ anche a·b∈$\mathbf{N}^+$.

PROPOSIZIONE 1.5. - Proprietà della moltiplicazione in $\mathbf{N}^+$.

a) *Legge di cancellazione*: per ogni a, b, c∈$\mathbf{N}^+$, se ab = ac allora b = c.

b) Per ogni a, b∈$\mathbf{N}^+$ al massimo una delle due equazioni $\begin{cases} a\cdot x = b \\ b\cdot y = a \end{cases}$, nelle incognite x ed y∈$\mathbf{N}^+$, ha soluzione. Tale soluzione, se esiste, è unica (per la legge di cancellazione).

NOTA. A differenza della analoga proprietà dell'addizione, la proprietà 1.5.b della moltiplicazione contiene solo l'affermazione dell'unicità dell'eventuale soluzione.

L'ordine naturale. L'ordine naturale di **N** si può definire a partire dall'addizione, ponendo per ogni a, b∈**N**,

$$a \le b \text{ se esiste } d\in\mathbf{N} \text{ tale che } a+d = b.$$

PROPOSIZIONE 1.6. - Proprietà della relazione ≤:

a) *Proprietà riflessiva*: per ogni a∈**N** si ha a ≤ a.

b) *Proprietà antisimmetrica*: per ogni a,b∈**N**, se a ≤ b e b ≤ a allora a = b.

c) *Proprietà transitiva:* per ogni a, b, c∈**N**, se a ≤ b e b ≤ c allora a ≤ c.

d) *Dicotomia*: per ogni a, b∈**N** si ha a ≤ b oppure b ≤ a.

Dimostrazione. a) Per ogni a∈**N** si ha: a+0 = a, quindi a ≤ a.

b) Se a+m = b e b+n = a allora a+(m+n) = a, ed essendo a = a+0, per la legge di cancellazione si ha m+n = 0, da cui segue m = n = 0 e a = b.

c) Da a+m = b, b+n = c segue a+(m+n) = c.

d) Basta applicare la proprietà 1.2.c.

Le prime tre proprietà ci dicono che (**N**, ≤) è un *insieme ordinato* e la quarta ci dice che l'ordine è *totale*. Inoltre, poiché per ogni n∈**N** si ha 0+n = n allora 0 ≤ n. Dunque 0 è il *minimo*. Non c'è invece *massimo*, poiché per ogni n∈**N** si ha n < n+1. Inoltre:

PROPOSIZIONE 1.7. - Relazioni tra operazioni ed ordine.

a) Per ogni a, b, c∈**N**, si ha a ≤ b se e solo se a+c ≤ b+c.

b) Per ogni a, b, c∈**N**, c ≠ 0, si ha a ≤ b se e solo se a·c ≤ b·c.

c) Per ogni n∈**N**, se n ≤ x ≤ n+1 allora x = n oppure x = n+1.

Dimostrazione. a) Da a+m = b segue (a+c)+m = (b+c) e viceversa.

b) a ≤ b ⇒ ∃ d, a+d = b ⇒ (a+d)·c = b·c ⇒ a·c ≤ a·c + d·c = b·c. Inversamente, se a·c ≤ b·c e se fosse b ≤ a allora b·c ≤ a·c ⇒ b·c = a·c, e poiché c ≠ 0, ⇒ b = a. Allora a ≤ b in ogni caso.

c) Se n < x allora x = n+m, con 1 ≤ m, quindi da n+1 ≤ n+m = x ≤ n+1 segue x = n+1.

Sia H un sottoinsieme di **N**. Un elemento x∈**N** si dice *minorante* di H se per ogni h∈H si ha x ≤ h. Si dice *minorante stretto* se per ogni h∈H si ha x < h. Ciò posto:

PROPOSIZIONE 1.8 (**principio del minimo**). - Ogni sottoinsieme non vuoto H di **N** possiede il minimo.

Dimostrazione. Se 0∈H allora 0 è il suo minimo. Sia 0∉H e sia M(H) l'insieme dei minoranti stretti di H. Innanzitutto, 0∈M(H). Se per ogni x∈M(H) si avesse anche x+1∈M(H) allora, per il principio d'induzione, M(H) = **N** e H sarebbe vuoto, assurdo. Dunque, esiste x_0∈M(H) tale che x_0+1∈H. Ne segue che x_0+1 è il minimo cercato: infatti ogni altro h∈H è maggiore di x_0, quindi per 1.7.b) è anche h ≥ x_0+1.

PROPOSIZIONE 1.9. - Dati due numeri naturali a, b, con b ≠ 0, esistono due numeri naturali q, r, univocamente determinati, tali che $\begin{cases} a = b\cdot q + r \\ 0 \le r < b \end{cases}$.

Dimostrazione: se a < b allora q = 0 ed r = a. Se a ≥ b sia $M = \{x \in \mathbf{N} \mid \exists k \in \mathbf{N},\ x = a - b \cdot k\}$: non è vuoto perché a∈M, perciò ha minimo r ≥ 0. Allora esiste q tale che $r = a - b \cdot q$, e si ha r < b, altrimenti s = r–b = a-(q+1)b∈M e s < r, assurdo. Se poi si ha anche $a = b \cdot q' + r'$, con per esempio r' < r, allora:

$$b \cdot q + r = b \cdot q' + r' \Rightarrow r - r' = b \cdot (q' - q), \text{ con } q'\text{-}q \geq 1.$$

Ma si ha contemporaneamente $r - r' < r < b \leq b \cdot (q' - q)$, assurdo. Dunque si ha l'unicità di q ed r.

I numeri q ed r si chiamano rispettivamente *quoziente* e *resto* di a diviso b. Questa "operazione" è detta *divisione euclidea* o *divisione col resto* in **N**.

Dati a, b∈$\mathbf{N}^+$, se esiste q∈**N** tale che a·q = b allora q si dice *quoto* di "b diviso a" e si pone b:a = q. Questa operazione si chiama spesso *divisione esatta* di a per b. In particolare, b:b = 1. Si osservi che si ha la divisione esatta fra a e b se e solo se la divisione euclidea dà resto nullo. In tal caso, il quoto coincide col quoziente. Torneremo più avanti su questo algoritmo.

NOTA. Poiché per ogni a ≠ 0 risulta a·0 = 0, si può definire il quoto di 0 diviso a ponendo 0:a = 0. Non ha senso invece la scrittura 0:0, in quanto per ogni q∈**N** si ha 0·q = 0.

L'ordine dalla divisibilità. Eseguendo una 'traduzione' in notazione moltiplicativa delle nozioni precedenti, introduciamo un ordine in $\mathbf{N}^+$. Definiamo la relazione | (*divide*) in $\mathbf{N}^+$ ponendo:

per ogni a, b∈$\mathbf{N}^+$, a | b se esiste q∈$\mathbf{N}^+$ tale che a·q = b.

Sostituendo ≤ con | e 0 con 1 nella proposizione 1.6, mediante le proprietà della moltiplicazione si provano subito le seguenti proprietà:

PROPOSIZIONE 1.10. - Proprietà della relazione |:

a) *Proprietà riflessiva*: per ogni a∈$\mathbf{N}^+$ si ha a|a.

b) *Proprietà antisimmetrica*: per ogni a,b∈$\mathbf{N}^+$, se a|b e b|a allora a = b.

c) *Proprietà transitiva:* per ogni a, b, c∈$\mathbf{N}^+$, se a|b e b|c allora a|c.

Non vale invece la dicotomia: per esempio 2 non divide 3 e 3 non divide 2. Queste proprietà ci dicono che ($\mathbf{N}^+$, |) è un insieme *parzialmente ordinato*. Inoltre, poiché per ogni $n\in\mathbf{N}^+$ si ha $1\cdot n = n$ allora $1 \mid n$. Dunque 1 è il minimo. Non c'è invece massimo, poiché per ogni $n\in\mathbf{N}^+$ si ha per esempio $n \mid 2n$.

L'ordinamento | di $\mathbf{N}^+$ è legato all'ordinamento $\leq$ dalla relazione seguente:

PROPOSIZIONE 1.11. - Per ogni $a, b\in\mathbf{N}^+$, se $a \mid b$ allora $a \leq b$. Inversamente, se $a < b$ allora b non divide a.

Dimostrazione. Sia $b = aq$ e procediamo per induzione rispetto a q. Se $b = a\cdot 1$ allora $a = b$, quindi $a \leq b$. Supponiamo vero il teorema per $q = n$ (ipotesi induttiva) e proviamolo per $q = n+1$. Sia $b = a(n+1) = an+a$: per ipotesi induttiva e per la proposizione 1.7 si ha:

$$a \leq an = an + 0 \leq an+a = b,$$

da cui segue $a \leq b$. Inversamente, se $a < b$ e se fosse $b \mid a$ allora $b \leq a$, assurdo.

NOTA. Volendo estendere l'ordinamento | a tutto $\mathbf{N}$, si deve porre necessariamente $n \mid 0$ per ogni $n\in\mathbf{N}$, in particolare, $0 \mid 0$. Infatti per ogni $n\in\mathbf{N}$ esiste almeno un elemento $q\in\mathbf{N}$, tale che $nq = 0$: è ovviamente $q = 0$ (e non è richiesta l'unicità di q). Pertanto ($\mathbf{N}$, |) oltre al minimo, uguale ad 1, possiede anche il massimo, lo zero.

Potenze. Per ogni $a\in\mathbf{N}^+$ e per ogni $n\in\mathbf{N}$ si definisce ricorsivamente la *potenza* a^n nel modo seguente:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \end{cases}.$$

In particolare si ha $a^1 = a$. Per le potenze valgono le seguenti proprietà, che si dimostrano per induzione rispetto ad n:

PROPOSIZIONE 1.12. - Per ogni $a, b\in\mathbf{N}^+$ e per ogni $m, n\in\mathbf{N}$ si ha:

a) $a^m \cdot a^n = a^{m+n}$

b) $(a^m)^n = a^{mn}$

c) $(ab)^n = a^n b^n$

NOTA. Mentre le prime proprietà dipendono solo dalla definizione di potenza e dalla proprietà associativa della moltiplicazione, la terza dipende in modo essenziale dalla proprietà commutativa: $(ab)^2 = abab = aabb = a^2b^2$.

Quanto sopra detto per le potenze si può ripetere per l'addizione. Osserviamo che in notazione additiva la potenza di base a ed esponente n si scrive *na* anziché a^n, e si ha:

$$\begin{cases} 0a = 0 \\ (n+1)a = na + a \end{cases}.$$

Il numero *na* si chiama *multiplo naturale* di a.

PROPOSIZIONE 1.13. - Altre proprietà di multipli e potenze.

a) Per ogni n, h, k∈**N**, n ≠ 0, si ha h < k se e solo se hn < kn. In particolare, l'unico multiplo di n che sia minore di n è lo zero.

b) Per ogni n, h, k∈$\mathbf{N}^+$, n ≠ 1, si ha h < k se e solo se $n^h < n^k$ (o equivalentemente se e solo se n^h divide "propriamente" n^k). In particolare, l'unica potenza di n che sia minore di n (cioè divisore proprio di n) è 1.

Riprendiamo il discorso sui numeri naturali e sul modo di rappresentarli, ossia sui *sistemi di numerazione*. Nella storia ci sono stati vari approcci. Il più antico consiste nel rappresentare i numeri naturali come file finite di *tacche*:

1 = I 2 = II 3 = III e così via.

Lo *zero* è l'assenza di tacche. E' un metodo che dal punto di vista teorico permette di capire facilmente le operazioni ed il confronto.

- L'*ordinamento* è evidente: si sovrappongono le due file di tacche e quella che "sporge" è maggiore dell'altra.
- *Addizionare* non è altro che concatenare:

  III+IIII = IIIIIII

  e così ogni numero è somma di tanti 1 quante sono le sue tacche.
- *Sottrarre* è eliminare dal minuendo tante tacche quante sono espresse dal sottraendo, purché sia minore o uguale al minuendo:

  IIIII - II = III

- *Moltiplicare* è addizionare successivamente lo stesso numero di tacche:

$$||| \times || = ||+||+|| = ||||||$$

- *Dividere* è sottrarre successivamente il divisore dal dividendo, finché possibile: il *quoziente* è il numero delle sottrazioni, il *resto* è quel che rimane alla fine.

Le proprietà sono quasi immediate. In particolare, persino uno scoglio concettuale come la divisione per zero è facile: sottrarre zero tacche da un numero dato non lo cambia mai, si può proseguire all'infinito e non si ha un quoziente ed un resto, perciò non ha senso dividere per zero.

Questo metodo si pensa sia stato il primo ad essere utilizzato nella storia della rappresentazione dei numeri: infatti il più antico ritrovamento consiste in un osso di lupo, risalente a 30.000 anni fa circa, con incise una successione di tacche a distanza all'incirca costante l'una dall'altra e con una tacca più lunga in corrispondenza di cinque tacche corte.

Tuttavia, questo approccio non è soddisfacente per un uso pratico: i numeri come tacche diventano presto ingestibili e le esigenze di calcolo e di introduzione di nuovi insiemi di numeri (per misurare e non solo per contare) richiedono una razionalizzazione dei numeri naturali ed una loro diversa rappresentazione. Parliamo allora in generale di sistemi di numerazione.

Per *sistema di numerazione* si intende l'insieme dei simboli e delle regole che consentono di rappresentare graficamente i numeri e di leggerli. Un sistema di numerazione è quindi una sequenza di nomi di numeri, o numerali, utilizzata per *enumerare*, ossia per attribuire ad ogni elemento di un insieme finito un nome, che dipende dall'ordine con il quale prendiamo in considerazione tale elemento.

Gli aspetti di un sistema di numerazione, che vengono valutati per determinarne la "qualità", sono:

1) *Motivazione*: è una proprietà non matematica, che dipende dagli usi, dalle abitudini. Il nostro sistema a base 10 non è particolarmente motivato, a differenza del sistema unario delle tacche.
2) *Astrattezza*: proprietà fondamentale, dato che vengono trattati numeri che sono entità astratte.
3) *Organicità*: un sistema è organico se con un metodo semplice e composto da poche regole riesce a rappresentare tutti i numeri (naturali).

4) *Efficienza computazionale*: un sistema è efficiente quando permette, non solo di menzionare i numeri, ma anche di utilizzarli nel calcolo delle comuni operazioni con facilità. Il sistema posizionale da noi utilizzato ha avuto successo grazie alla sua straordinaria efficienza nel calcolo rispetto ai sistemi fino a quel momento utilizzati.

La sequenza dei nomi che costituisce un sistema di numerazione si può pensare che debba essere infinita, data l'infinità dei numeri. Sin dai primi tentativi di enumerazione, l'uomo ha capito la necessità di attribuire nomi ai numeri seguendo regole e non in modo arbitrario, ed ha escogitato nel corso della storia diversi metodi di rappresentazione dei numeri attraverso la scrittura. Dividiamo tali metodi in due categorie principali: i *metodi senza base* e quelli *con base*.

Del primo tipo è il metodo delle tacche, già visto, ma anche il rappresentare ogni numero con un simbolo diverso e senza nessi logici fra i simboli. Quest'ultimo metodo è sicuramente inefficiente perché privo di organicità e perché non permette le fasi di memorizzazione e trasmissione del processo del contare.

Nei metodi con base rappresentiamo numeri che sappiamo essere decomponibili in una somma di q_n unità u_n, q_{n-1} unità u_{n-i}, ..., q_0 unità u_0. Ricordiamo solo i due seguenti:

1) I numeri romani

Questo metodo fu introdotto per evitare di scrivere successivamente più di 3 simboli uguali. Per fare questo furono introdotti simboli per le potenze di 10 ed altri simboli per "unità intermedie", e una notazione sottrattiva. Il suo supporto grafico è costituito da 7 lettere dell'alfabeto latino :

I = 1, V = 5, X =10, L = 50, C = 100 , D = 500 M = 1000.

Per rappresentare un numero venivano scritte le lettere in ordine decrescente dei loro valori, che venivano sommati, ma per evitare la ripetizione di 4 lettere uguali fu inventata la seguente regola: se una lettera di valore inferiore è collocata alla sinistra di una lettera di valore superiore, i due valori vanno sottratti; se è collocata alla destra i due valori vanno sommati. In questo modo otteniamo ad esempio: XL = 40 e LX = 60. L'efficienza computazionale è bassissima e la rappresentazione di numeri altri assai complicata.

2) Rappresentazione di posizione (RP)

La logica che sta alla base di questo metodo è la seguente: stabilita una convenzione per la scrittura, i diversi addendi $q_i u_i$ vengono rappresentati per lo stesso valore di q_i, con lo stesso simbolo e il valore di u_i viene indicato solo attraverso la posizione del corrispondente simbolo per q_i occupata nella stringa di simboli che costituisce la rappresentazione del numero. Questo metodo poteva creare degli errori causati dal dovere lasciare uno spazio vuoto in corrispondenza di un moltiplicatore assente. Questo problema fu risolto con l'introduzione di un simbolo speciale chiamato *zero*, sia all'interno delle sequenze (*zero intercalare*) sia alla fine di esse (*zero finale*). Questo metodo è utilizzato da quasi tutti i popoli, facendo riferimento alla base 10 e usando attualmente i simboli 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 come cifre, combinate secondo le seguenti regole:

- i primi nove interi positivi sono rappresentati da 1, 2, 3, 4, 5, 6, 7, 8, 9
- il successivo di 9 si scrive 10
- il successivo rappresentato da n cifre si scrive nel seguente modo: se l'ultima cifra non è 9 si sostituisce questa con la sua successiva; se l'ultima cifra è 9 si sostituisce 9 con 0 e l'intero rappresentato dalle n-1 prime cifre col suo successivo.

Questo metodo ha origini indo-arabiche ed è usato non tanto per la motivazione dei simboli, quanto per la sua sistematicità e per la sua elevata efficienza computazionale. I sistemi posizionali si sono sviluppati gradualmente, in concomitanza con l'uso di "unità di ordine superiore" (decine, centinaia, dozzine, lustri...) rese necessarie dall'espansione del sistema dei numerali verso numeri sempre più grandi.

NOTA. Sembra che il metodo posizionale risalga circa al 600 d. C. Circa nel 750 d.C. il persiano al-Khowarizmi tradusse in arabo il libro indiano che spiegava l'aritmetica decimale. Il metodo posizionale fu poi introdotto in Europa da Leonardo Fibonacci, che ne espose le caratteristiche nel suo celebre "Liber Abaci" (1202), traduzione latina del libro arabo di al-Khowarizmi. Nel "Liber Abaci" il termine arabo *as-sifr* fu latinizzato in *zephirum*, da cui deriva l'italiano *zefiro*, corretto in *zeuero*, e infine in *zero.* Da esso derivano anche l'italiano *cifra*, il francese *chiffre*, il tedesco *ziffer,* per indicare tutti i simboli da 0 a 9 e non solo lo zero.

Nella scuola elementare si imparano le tecniche per eseguire le operazioni sui numeri naturali scritti in base 10. Successivamente, nella scuola media, si impara

talora ad usare la base 2, a causa della scrittura binaria usata nell'informatica. Quest'ultima usa solo i simboli 1 e 0, sostituibili con ON/OFF o con V/F (vero o falso). Una tabella di confronto per i primi dodici numeri naturali scritti nei vari sistemi di numerazione è interessante:

tacche		I	II	III	IIII	IIIII	IIIIII	IIIIIII	IIIIIIII	IIIIIIIII	IIIIIIIIII	IIIIIIIIIII	IIIIIIIIIIII
Romani		I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
2	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100
10	0	1	2	3	4	5	6	7	8	9	10	11	12

ESEMPIO 4.3. Algoritmo di passaggio dalla base 10 alla base 2: si divide il numero per 2 e si trascrivono quoziente e resto; si ripete col quoziente come dividendo. I resti concatenati in ordine inverso danno il numero in base 2.

numero dec.	547	273	136	68	34	17	8	4	2	1
quoziente	273	136	68	34	17	8	4	2	1	0
resto	1	1	0	0	0	1	0	0	0	1

Il numero in base 2 è allora 1000100011 (= $2^9 + 2^5 + 2 + 1$)

NOTA. Interessante come attività scolastica, interdisciplinare ed interclasse, è anche il confronto dei nomi dei numeri nelle varie lingue, perché può coinvolgere gli insegnanti di lingua straniera e di lingue classiche, gli allievi di provenienza estera; può essere spunto per ricerche su Internet o su enciclopedie su lingue sempre più attuali come lo spagnolo, l'arabo, il russo o il cinese.

§ 2. Numeri cardinali

Si tratta di un argomento profondo e complesso, forse il cuore della teoria degli insiemi. Qui è accennato solo come possibile approccio ai numeri naturali, poiché riprende, dal punto di vista superiore, quello che gli insegnanti delle scuole dell'infanzia ed elementari propongono ai bambini, mediante figure di oggetti da confrontare: due uova, due conigli, due automobili, ... per formare il concetto di numero 2.

Due insiemi A e B si dicono *equipotenti* se esiste una biiezione $f : A \xrightarrow{1\text{–}1}{su} > B$. Se A è equipotente a B scriviamo per brevità $A \cong B$.

PROPOSIZIONE 2.1. - In ogni insieme $\mathscr{U}$ di insiemi, l'equipotenza è una relazione d'equivalenza.

Dimostrazione. Per ogni A, B, C appartenenti ad $\mathscr{U}$, si ha:

- proprietà riflessiva: poiché $id_A : A \xrightarrow{1\text{–}1}{su} > A$, allora $A \cong A$.
- proprietà simmetrica: sia $A \cong B$, allora esiste $f : A \xrightarrow{1\text{–}1}{su} > B$. Ne segue $f^{-1} : B \xrightarrow{1\text{–}1}{su} > A$, quindi $B \cong A$.
- proprietà transitiva: siano $A \cong B$, $B \cong C$; esistono allora $f : A \xrightarrow{1\text{–}1}{su} > B$ e $g : B \xrightarrow{1\text{–}1}{su} > C$, da cui segue $g \circ f : A \xrightarrow{1\text{–}1}{su} > C$ e quindi $A \cong C$.

Le classi d'equivalenza si chiamano *numeri cardinali*. La classe dell'insieme A, ossia il suo numero cardinale, la denoteremo con $|A|$.

Supponiamo ora che l'insieme $\mathscr{U}$ sia *chiuso* rispetto all'unione, all'intersezione, all'inclusione, al prodotto cartesiano e contenga l'insieme vuoto e l'insieme $\{\varnothing\}$. Poniamo dapprima $0 = |\varnothing|$ e $1 = |\{\varnothing\}|$. Allora, $0 \neq 1$ perché $\varnothing$ e $\{\varnothing\}$ non sono equipotenti. Definiamo ora le operazioni di *addizione* e *moltiplicazione* in $\mathscr{U}$. Siano A e B due insiemi e siano $A' = A \times \{0\}$, $B' = B \times \{1\}$. I due insiemi A' e B' sono equipotenti ad A e B rispettivamente, e sono disgiunti, ossia $A' \cap B' = \varnothing$. Poniamo:

$$|A| + |B| = |A' \cup B'|, \quad |A| \cdot |B| = |A \times B|$$

Le due definizioni sono ben poste. Infatti, siano $C \cong A$, $D \cong B$. Allora sicuramente $C \times D \cong A \times B$. Inoltre, posto $C' = C \times \{0\}$, $D' = D \times \{1\}$, si ha $C' \cup D' \cong A' \cup B'$.

Queste operazioni sono inoltre associative, commutative, la moltiplicazione è distributiva rispetto all'addizione. Inoltre, $0 = |\varnothing|$, ossia lo *zero*, è l'elemento neutro dell'addizione ed è elemento assorbente della moltiplicazione. Infine, $1 = |\{\varnothing\}|$, ossia l'*uno*, è l'elemento neutro della moltiplicazione.

Si può anche definire un ordine tra i numeri cardinali. Enunciamo dapprima il seguente teorema:

TEOREMA 2.2 (Cantor – Bernstein). - Siano A e B due insiemi. Se esistono $f : A \xrightarrow{1-1} B$ e $g : B \xrightarrow{1-1} A$, allora A e B sono equipotenti.

Osserviamo poi che: dati quattro insiemi A, A', B, B', $A \cong A'$, $B \cong B'$, ed esiste $f : A \xrightarrow{1-1} B$, allora esiste anche $f' : A' \xrightarrow{1-1} B'$. Infatti, siano $\alpha : A \xrightarrow[su]{1-1} > A'$, $\beta : B \xrightarrow[su]{1-1} > B'$, allora $f' = \beta \circ f \circ \alpha^{-1}$ è iniettiva.

Ne segue la possibilità di definire $|A| \le |B|$ se esiste $f : A \xrightarrow{1-1} B$, e questa è una relazione d'ordine. In più, è *totale*: infatti, si può dimostrare che dati due insiemi A e B, se non esiste $f : A \xrightarrow{1-1} B$ allora esiste $g : B \xrightarrow{1-1} A$; pertanto, se non si ha $|A| \le |B|$, allora necessariamente $|B| \le |A|$.

Concludiamo osservando che se per il nostro insieme universo $\mathscr{U}$ si ha $A \in \mathscr{U} \Rightarrow \wp(A) \in \mathscr{U}$, allora a partire da $\mathscr{U}$ si trovano numeri cardinali grandi a piacere. Infatti, un teorema di Cantor afferma che $\forall A,\ A \in \mathscr{U} \Rightarrow |A| < |\wp(A)|$.

Seguendo Dedekind, un insieme A si dice *infinito* se è equipotente ad un suo sottoinsieme proprio. Se non è infinito, si dice *finito*. Ogni insieme equipotente ad A è infinito o finito come A. Pertanto, possiamo parlare di numeri cardinali finiti. Il vuoto è un insieme finito (non è equipotente ad un sottoinsieme proprio perché non ne ha), quindi 0 è un cardinale finito, e così pure 1 è finito. Si ha poi:

a) Somma e prodotto di cardinali finiti sono cardinali finiti.

b) Se n è un cardinale finito, anche n+1 lo è.

c) Se m ed n sono finiti, $n \neq 0$, allora $m+n \neq m$.

d) I numeri cardinali finiti costituiscono un insieme, che denoteremo con **N**, e che chiameremo insieme dei numeri naturali.

e) **N** non è un insieme finito, poiché posto $\sigma(n) = n+1$, si ha $\sigma : \mathbf{N} \xrightarrow{1-1} \mathbf{N} \setminus \{0\}$.

f) La terna $(\mathbf{N}, 0, \sigma)$ soddisfa gli assiomi di Peano e quindi è un modello dei numeri naturali.

Gli insiemi equipotenti ad **N** si dicono *numerabili*. Si può dimostrare che un insieme è infinito se e solo se contiene un sottoinsieme numerabile. Allora ogni numero cardinale infinito è maggiore di $|\mathbf{N}|$. Quest'ultimo numero cardinale si denota con $\aleph_0$ (che si legge Aleph zero).

ESEMPI 2.3. – a) L'insieme **Z** degli interi relativi è numerabile.

Risposta. Una funzione biiettiva da **Z** ad **N** è la seguente:

$f(x) = \begin{cases} 2x & \text{se } x \geq 0 \\ -1-2x & \text{se } x < 0 \end{cases}$. Per esempio,

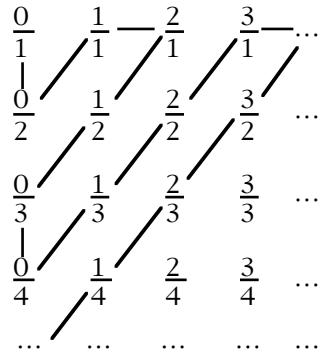
x	0	1	2	3	…	–1	–2	–3	–4	…
f(x)	0	2	4	6	…	1	3	5	7	…

Per dimostrare che è suriettiva, si osservi che per ogni n∈**N**, se n è pari allora $n = 2n' = f(n'),\ n' \geq 0$. Se è dispari, allora $n = 2n' - 1 = -1 - 2(-n') = f(-n'),\ n' > 0$. Per l'iniettività si osservi che l'immagine dei negativi è l'insieme dei dispari, quella dei positivi o nulli è l'insieme dei pari. Se quindi x, y sono tali che f(x) = f(y), allora x ed y sono entrambi ≥ 0 o entrambi < 0.

Ora, sui ≥ 0: 2x = 2y ⇒ x = y; sui negativi, -1-2x = -1-2y ⇒ x = y, perciò f è anche iniettiva.

b) L'insieme **Q** dei numeri razionali è numerabile.

Risposta. Poiché **Q** contiene **N** allora |**Q**| ≥ $\aleph_0$. Per la disuguaglianza inversa si parte col costruire una funzione iniettiva dall'insieme **N** all'insieme delle frazioni $\frac{m}{n}$, con m ed n numeri naturali e n ≠ 0. (si veda la figura seguente). L'insieme di queste frazioni è dunque numerabile. Ogni numero razionale "assoluto" è identificabile con una frazione ridotta ai minimi termini, perciò l'insieme dei numeri razionali assoluti è equipotente ad un sottoinsieme dell'insieme delle frazioni, ed è di conseguenza numerabile a sua volta. Ossia, esiste una funzione biiettiva $g : \mathbf{N} \to \mathbf{Q}^+ \cup \{0\}$.



n	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$f(n)$	$\frac{0}{1}$	$\frac{0}{2}$	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{1}{2}$	$\frac{0}{3}$	$\frac{0}{4}$	$\frac{1}{3}$	$\frac{2}{2}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{3}{2}$	$\frac{2}{3}$	...

Con uno scambio eventuale tra lo zero di **Q** e g(0), possiamo ricondurci al caso di $g(0) = 0$.

Si può allora costruire una funzione biiettiva Γ : **N** → **Q**, ponendo, per ogni n∈**N**,

$$\begin{cases} \Gamma(2n) = g(n) \\ \Gamma(2n+1) = -g(n) \end{cases}$$

e ciò prova che **Q** è numerabile.

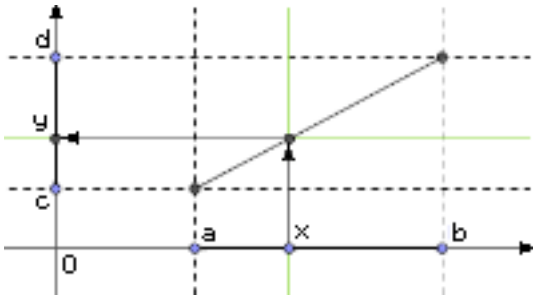
c) L'insieme **R** dei numeri reali non è numerabile.

Risposta. Poiché **R** contiene **N** allora |**R**| ≥ $\aleph_0$. Mostriamo che non vale l'uguaglianza. Per cominciare, osserviamo che l'insieme $\{0\} \cup \left\{ \frac{1}{n} \;\middle|\; n \in \mathbf{N}^+ \right\}$ è equipotente ad **N** ed è incluso nell'intervallo $[0,1[$ di **R**. Pertanto, questo intervallo è almeno numerabile. Supponiamo che lo sia, cioè che sia data una $f : \mathbf{N} \xrightarrow[\text{su}]{1\text{-}1} [0,1[$. A meno di uno scambio, supponiamo $f(0) = 0$. Rappresentiamo gli elementi di $[0,1[$ in base 10 come al solito, ossia con numeri decimali del tipo $0, c_1 c_2 c_3 \cdots$ Ognuno di questi numeri è il corrispondente tramite f di un numero naturale. Ma ora mostriamo che non è vero, parafrasando Cantor, costruendo cioè un numero diverso da ogni f(n).

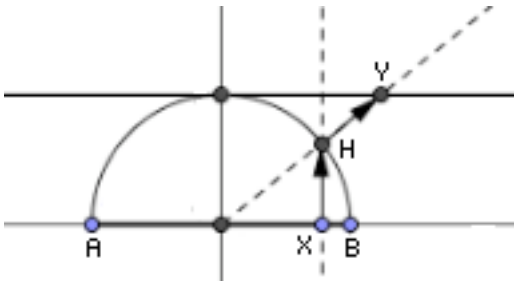
Sia x = $0, c_1 c_2 c_3 \cdots$ il nostro numero da costruire. Per ogni n∈**N**, n > 0, poniamo:

$$c_n = \begin{cases} 2 & \text{se la n-esima cifra decimale di } f(n) \text{ è } 1 \\ 1 & \text{altrimenti} \end{cases}$$

In tal modo, il nostro numero x sarà non nullo, quindi ≠ f(0), e differirà da ogni altro f(n) per la n-esima cifra decimale, ed allora x∉f(**N**). D'altra parte, essendo un numero decimale del tipo 0,… si ha x∈$[0,1[$ = f(**N**), quindi abbiamo una contraddizione. Ne segue che una tale f non esiste, ed allora $[0,1[$ non è numerabile. Ne segue che anche **R** non è numerabile.



d) Due intervalli chiusi e limitati $[a,b]$ e $[c,d]$ di **R** sono equipotenti.
Ne segue anche l'equipotenza di intervalli limitati ma non necessariamente chiusi.
La figura è eseguita col software Geogebra e qualche manipolazione.



e) Un segmento aperto $]A,B[$ è equipotente ad una semicirconferenza aperta di diametro AB e ad una retta.
Ne segue l'equipotenza fra rette e segmenti, e fra **R** ed ogni suo intervallo.

f) **R** ed $\mathbf{R}^2$ sono equipotenti. Lo stesso Peano mostrò infatti che esiste una funzione suriettiva dall'intervallo $[0,1]$ di R al quadrato $[0,1]\times[0,1]$ di $\mathbf{R}^2$. Ne segue che esiste una funzione iniettiva da $[0,1]\times[0,1]$ a $[0,1]$ e, valendo ovviamente il viceversa, i due insiemi sono equipotenti. Ne segue che anche **R** ed $\mathbf{R}^2$ sono equipotenti.

NOTA. Il numero cardinale dell'insieme **R** è denotato con *c* ed è detto *potenza del continuo*. Tra $\aleph_0$ e *c* ci sono altri numeri cardinali? La risposta non segue dagli altri assiomi della teoria degli insiemi, ma può diventare a sua volta un assioma da aggiungere agli altri: se ne può fare a meno, o si può postulare l'esistenza o postulare la non esistenza (*ipotesi del continuo*), senza per questo cadere in contraddizioni.

Certamente questi esempi sono interessanti ed istruttivi, ma coinvolgono nozioni molto delicate, che non sono trattabili compiutamente a livello elementare. Il concetto di numero cardinale finito è sfuggente; il fatto che i cardinali finiti siano un insieme non è ovvio. Il fatto che non esista l'"insieme di tutti gli insiemi", costringe a considerare un insieme *universo*, i cui elementi siano insiemi, che sia abbastanza grande da contenere tutti i possibili cardinali finiti: esiste?

§ 3. – Calcolo combinatorio

In questa sezione vediamo gli insiemi finiti con l'impostazione opposta a quella della sezione precedente: si suppongono noti i numeri naturali e si usano per contare gli elementi di certi insiemi finiti, ossia esploriamo il *calcolo combinatorio* elementare. Il problema generale è la determinazione del numero di elementi di certi insiemi finiti conoscendo il numero d'elementi di certi altri insiemi finiti. Ricordiamo che due insiemi A e B si dicono *equipotenti* se esiste una biiezione $f : A \xrightarrow[su]{1-1} B$. L'equipotenza possiede le proprietà riflessiva, simmetrica e transitiva. Se A è equipotente a B scriviamo $A \cong B$.

Siano $n \in \mathbf{N}$, $n > 0$, ed $\mathbf{N}_n = \{i \in \mathbf{N} \mid 1 \le i \le n\}$. Sia poi X un insieme. Diremo che X è *finito* se $X = \varnothing$ oppure se esiste $n \in \mathbf{N}$ tale che $\mathbf{N}_n \cong X$.

LEMMA 3.1. Per ogni $m, n \in \mathbf{N}$, non nulli, se $\mathbf{N}_m$ ed $\mathbf{N}_n$ sono equipotenti allora $n = m$.

Dimostrazione. Procediamo per induzione rispetto ad m. Siano $\mathbf{N}_m$ ed $\mathbf{N}_n$ equipotenti e sia $f : \mathbf{N}_m \xrightarrow[su]{1-1} \mathbf{N}_n$. Se m = 1, allora n = 1, altrimenti $\mathbf{N}_n = \{k \in \mathbf{N} \mid 1 \le k \le n\} \supset \{f(1)\}$, e viceversa. Sia m > 1 (quindi n > 1), sia vero il lemma per m-1 e dimostriamo che è vero anche per m.

Sia $u = f^{-1}(n) \in \mathbf{N}_m$. Poniamo $g : \mathbf{N}_{m-1} \to \mathbf{N}_n$, $g(k) = \begin{cases} f(k) & k < u \\ f(k+1) & k \ge u \end{cases}$. Allora:

$$\mathrm{im}(g) = \mathrm{im}(f) \setminus \{f(u)\} = \mathbf{N}_n \setminus \{n\} = \mathbf{N}_{n-1}$$

Inoltre, g è iniettiva. Infatti, $\forall h,k \in \mathbf{N}_{m-1}$, se g(h) = g(k) allora:

- Se sono entrambi minori di u, si ha f(h) = f(k) quindi h = k.
- Se sono entrambi maggiori di u, allora f(h+1) = f(k+1) implica h+1 = k+1 ossia h = k.
- Altrimenti, se k < u ≤ h, allora f(k) = f(h+1) implica $k = h+1 > h > k$, assurdo.

Pertanto, $g : \mathbf{N}_{m-1} \xrightarrow[su]{1-1} \mathbf{N}_{n-1}$.

L'ipotesi induttiva implica allora m-1 = n-1, ossia m = n.

Questo lemma giustifica la seguente definizione. Siano X un insieme ed n un numero naturale non nullo. Se $X = \varnothing$ poniamo $|X| = 0$. Sia $X \neq \varnothing$; se X è equipotente ad $\mathbf{N}_n$ poniamo $|X| = n$. Chiameremo $|X|$ *numero di elementi* di X.

PROPOSIZIONE 3.2. Sia X un insieme finito, |X| = n.

a) Ogni insieme Y equipotente ad X ha lo stesso numero n di elementi.

b) Per ogni $A \subseteq X$ si ha $|A| \leq n$.

Dimostrazione. a) Se X è vuoto, anche Y è vuoto, quindi |X| = |Y| = 0. Sia X non vuoto; |X| = n significa che esiste $f : \mathbf{N}_n \xrightarrow[su]{1-1} X$. $X \cong Y$ significa che esiste $g : X \xrightarrow[su]{1-1} Y$, allora $g \circ f : \mathbf{N}_n \xrightarrow[su]{1-1} Y$ e quindi |Y| = n.

b) Se X = ø allora A = ø. Sia X ≠ ø; |X| = n significa che esiste $f : \mathbf{N}_n \xrightarrow[su]{1-1} X$. Consideriamo l'immagine $f^{-1}(A) \subseteq \mathbf{N}_n$ di A rispetto alla biiezione inversa. Allora $|A| = |f^{-1}(A)|$ e $f^{-1}(A)$ è costituito da numeri naturali distinti compresi tra 1 ed n, quindi sono al massimo n. Pertanto, $|A| \leq n$.

Qui vedremo alcuni problemi classici in una formulazione che fa uso della teoria degli insiemi.

PROBLEMA I. Siano A e B insiemi finiti, e sia $A \cap B = \varnothing$. Calcolare $|A \cup B|$.

TEOREMA 3.3. - In queste ipotesi si ha $|A \cup B| = |A| + |B|$.

Dimostrazione. Poniamo |A| = k, |B| = n. Se k = 0 oppure n = 0 allora è banale. Altrimenti esistono $\varphi : \mathbf{N}_k \xrightarrow[su]{1-1} A$, $\psi : \mathbf{N}_n \xrightarrow[su]{1-1} B$. Definiamo ora una funzione $\Phi : \mathbf{N}_{k+n} \xrightarrow[su]{1-1} A \cup B$ ponendo, per ogni $i \in I_{k+n}$,

$$\Phi(i) = \begin{cases} \varphi(i) & \text{se } i \leq k \\ \psi(i-k) & \text{se } i > k \end{cases}$$

Poiché φ e ψ sono funzioni e $A \cap B = \varnothing$, anche Φ è una funzione ed è anche una biiezione.

COROLLARIO 3.4 - **Principio di addizione.** - Siano $A_1, \ldots, A_r$ insiemi finiti a due a due disgiunti. Allora $\left|\bigcup_{i=1}^{r} A_i\right| = \sum_{i=1}^{r} |A_i|$.

Dimostrazione. Per induzione su r, se r = 2 è vero per il teorema 3.3. Supponiamo il teorema vero per r (≥ 2) e proviamo che di conseguenza è vero per r+1.

Posto $B = \bigcup_{i=1}^{r} A_i$, si ha $B \cap A_{r+1} = \varnothing$ e $|B| = \sum_{i=1}^{r} |A_i|$, dunque per il teorema 3.3 si ha

$$|B \cup A_{r+1}| = \sum_{i=1}^{r} |A_i| + |A_{r+1}| = \sum_{i=1}^{r+1} |A_i|.$$

NOTA. La proprietà espressa dal Corollario 3.4 è detta *principio di addizione*. Se in un insieme A consideriamo una partizione $\wp = \{C_1, \dots, C_m\}$, allora A è unione disgiunta delle componenti $C_1, \dots, C_m$. Ne segue $|A| = \left| \bigcup_{i=1}^{m} C_i \right| = \sum_{i=1}^{m} |C_i|$. In particolare, poiché ogni componente ha almeno un elemento, allora $|A| = \sum_{i=1}^{m} |C_i| \geq \sum_{i=1}^{m} 1 = m = |\wp|$. Di conseguenza, se A è un insieme con n elementi e $\wp = \{C_1, \dots, C_m\}$ è una partizione di A con m < n blocchi, allora esiste $i \in \{1, 2, \dots, r\}$ tale che $|C_i| > 1$. Questa proprietà è detta *principio dei cassetti*.

COROLLARIO 3.5. Siano A e B insiemi finiti. Se esiste $f : A \xrightarrow{su} B$ allora $|A| \geq |B|$.

Dimostrazione. Consideriamo la relazione di equivalenza $\Re_f$ in A, associata ad f, secondo la quale sono in relazione due elementi x ed y se f(x) = f(y). Essendo f suriettiva esiste una biiezione F tra l'insieme quoziente $A/\Re_f$, che è una partizione di A, e il codominio B, che associa ad ogni classe $[a]_{\Re_f}$ l'elemento $f(a)$. Dunque, $|A/\Re_f| = |B|$. Per quanto precede, però, $|A| \geq |A/\Re_f|$, perciò $|A| \geq |B|$.

COROLLARIO 3.6. Siano $|A| = k$, $|B| = n$, $C \subseteq A$, $|C| = r$.

a) $|A \setminus C| = k\text{-}r$.

b) Sia $C = A \cap B$, allora $|A \cup B| = k+n\text{-}r$.

Dimostrazione. a) La coppia $\{C, A \setminus C\}$ è una partizione di A, quindi per il principio di addizione si ha $|A| = |C| + |A \setminus C|$, da cui segue |A\C| = |A|-|C| = k-r.

b) La terna $\{C, A \setminus C, B \setminus C\}$ è una partizione di A∪B, quindi

$$|A \cup B| = |A \cap B| + |A \setminus C| + |B \setminus C| = r + (k - r) + (n - r) = k + n - r$$

Denotiamo con A×B il prodotto cartesiano di A per B, cioè l'insieme di tutte le coppie ordinate (a, b), con a∈A e b∈B.

PROBLEMA II. Siano A e B insiemi finiti. Calcolare |A×B|.

TEOREMA 3.7. Si ha $|A\times B| = |A|\cdot|B|$.

Dimostrazione. Se A oppure B è vuoto allora è banale. Altrimenti osserviamo che $A\times B = \bigcup_{a\in A}\left(\{a\}\times B\right)$, e che tutti gli insiemi $\{a\}\times B$ sono a due a due disgiunti ed equipotenti a B. Infatti, $a\neq a' \Rightarrow (a,b)\neq(a',b')$ per tutti i b, b'∈B, quindi $\left(\{a\}\times B\right)\cap\left(\{a'\}\times B\right)=\varnothing$. Inoltre, per ogni a∈A, la funzione $f_a : B\to\{a\}\times B$, $f_a : b\mapsto(a,b)$, risulta biiettiva, perciò $\{a\}\times B$ è equipotente a B. Per il corollario 3.4 si ha quindi:

$$|A\times B| = \left|\bigcup_{a\in A}\left(\{a\}\times B\right)\right| = \sum_{a\in A}|\{a\}\times B| = \sum_{a\in A}|B| = |A|\cdot|B|$$

perché somma di $|A|$ addendi uguali a $|B|$.

Il prodotto cartesiano degli insiemi $A_1, A_2, \ldots, A_n$, $n>2$ è definito induttivamente: $A_1\times\ldots\times A_n = (A_1\times\ldots\times A_{n-1})\times A_n$. I suoi elementi sono detti *liste* o *n-uple ordinate*, e denotati con $(a_1, a_2, \ldots, a_n)$.

COROLLARIO 3.8. Il principio di moltiplicazione. Se A_1, ..., A_k sono insiemi finiti, allora $|A_1\times\ldots\times A_k| = \prod_{i=1}^{k}|A_i|$.

Dimostrazione. Procediamo per induzione rispetto a k. Per k = 2 l'asserto è il teorema 3.7. Sia k ≥ 3, allora si ha $A_1\times\ldots\times A_k = (A_1\times\ldots\times A_{k-1})\times A_k$. Per ipotesi induttiva, $|A_1\times\ldots\times A_{k-1}| = \prod_{i=1}^{k-1}|A_i|$ e, per il teorema 3.7, si ottiene:

$$|A_1\times\ldots\times A_k| = |(A_1\times\ldots\times A_{k-1})\times A_k| = \left(\prod_{i=1}^{k-1}|A_i|\right)\cdot|A_k| = \prod_{i=1}^{k}|A_i|$$

NOTA. Il *principio di moltiplicazione* afferma che se per la lista $(a_1, a_2, \ldots, a_n)$ ci sono: n_1 possibilità per a_1, n_2 possibilità per a_2, e così via, in tutto ci sono $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ liste distinte. In particolare, se A_1, … , A_k sono tutti uguali ad un insieme A con n elementi, ci sono in tutto n^k liste distinte (k = lunghezza della lista, n = numero di scelte per ogni casella).

PROBLEMA III. Siano A e B insiemi finiti non vuoti. Calcolare $|B^A|$, ovvero il numero di funzioni f:A→B.

TEOREMA 3.9. Risulta $|B^A| = |B|^{|A|}$.

Dimostrazione. Sia $A = \{a_1, a_2, \ldots, a_k\}$. Ogni f:A→B si può rappresentare mediante la tabella

x	f(x)
a_1	$f(a_1)$
a_2	$f(a_2)$
…	…
a_k	$f(a_k)$

, ossia, in definitiva, mediante la lista $(f(a_1), f(a_2), \ldots, f(a_r))$. Quest'ultimo oggetto è un elemento del prodotto cartesiano B^k. Inversamente, dato un qualunque elemento $(b_1, b_2, \ldots, b_k) \in B^k$, la tabella

x	y
a_1	b_1
a_2	b_2
…	…
a_k	b_k

definisce una funzione f:A→B. Allora la corrispondenza Φ che ad ogni funzione f:A→B associa la lista $(f(a_1), f(a_2), \ldots, f(a_r)) \in B^k$ è una biiezione da B^A a B^k. Quest'ultimo ha $|B|^k = |B|^{|A|}$ elementi, quindi risulta proprio $|B^A| = |B|^{|A|}$.

ESEMPI 3.10.

3.10.A. - Quante parole di 3 lettere si possono scrivere con l'alfabeto $\{a, c, g, t\}$?

Ogni parola è una lista di lettere. Nel nostro caso, le lettere sono tre, e per ciascuna ci sono 4 possibilità, quindi $4 \cdot 4 \cdot 4 = 4^3 = 64$ parole.

3.10.B. - Sia |A| = n. Quante operazioni diverse, ossia funzioni $* : A \times A \to A$, si possono definire su A? Poiché $|A \times A| = n^2$, le operazioni possibili sono $n^{\left(n^2\right)}$. Per esempio, se n = 2, ci sono $2^4 = 16$ operazioni distinte.

COROLLARIO 3.11. Sia U un insieme finito, |U| = n; allora $|\wp(U)| = 2^n$.

Dimostrazione. Sia X⊆U; definiamo la seguente funzione associata ad X, detta *funzione caratteristica* di X: $\varepsilon_X : U \to \{0,1\}$, $\varepsilon_X : x \mapsto \begin{cases} 0 & \text{se } x \notin X \\ 1 & \text{se } x \in X \end{cases}$.

Definiamo ora la funzione $\varepsilon : \wp(U) \to \{0,1\}^U$, $\varepsilon : X \mapsto \varepsilon_X$. Tale funzione è una biiezione, e allora dal teorema 3.8 segue l'asserto.

PROBLEMA IV. Siano A e B due insiemi finiti non vuoti. Calcolare il numero delle funzioni iniettive $f : A \xrightarrow{1-1} B$.

Se |A| = k e |B| = n tale numero si denota con $D_{n,k}$ e viene anche chiamato *numero delle disposizioni senza ripetizioni* di n oggetti a k a k. Il problema si può porre anche per |A| = 0: in tal caso fra A e B vi è solo la *funzione vuota*, che è iniettiva. Pertanto $D_{n,0} = 1$ per ogni $n \geq 0$.

LEMMA 3.12. Siano A e B insiemi finiti. Se esiste $f : A \xrightarrow{1-1} B$ allora $|A| \leq |B|$.

Dimostrazione. Poiché f è iniettiva allora la co-restrizione di f ad f(A) ⊆ B è biiettiva da A ad f(A). Pertanto, A è equipotente ad f(A). Allora, $|A| = |f(A)| \leq |B|$.

TEOREMA 3.13. Risulta $D_{n,k} = \begin{cases} 0 & \text{se } k > n \\ \prod_{i=0}^{k-1} (n-i) & \text{se } 0 \leq k \leq n \end{cases}$.

Dimostrazione. Sia |B| = n. Se |A| = k > n, allora per il lemma si ha $D_{n,k} = 0$. Sia k ≤ n. Ogni $f : A \xrightarrow{1-1} B$ si può rappresentare mediante la lista $(f(a_1), f(a_2), \ldots, f(a_r))$, dove gli elementi sono tutti distinti. Allora, mentre $f(a_1)$ è un elemento qualunque di B, $f(a_2) \in B \setminus f(a_1)$, che ha n-1 elementi, $f(a_3) \in B \setminus \{f(a_1), f(a_2)\}$, che ha n-2 elementi, e così via. La conclusione segue ora dal principio di moltiplicazione.

Poniamo $0! = 1$, e per ogni $n > 0$ poniamo $n! = (n-1)!\cdot n$. Il simbolo $n!$ si legge "n *fattoriale* ".

PROPOSIZIONE 3.14. – a) Sia X un insieme finito non vuoto, $|X| = n$. Sia S_X l'insieme delle permutazioni su X. Allora $|S_X| = n!$

b) Risulta $D_{n,k} = \frac{n!}{(n-k)!}$ per ogni $0 \le k \le n$.

Dimostrazione. a) Le permutazioni di X sono biiezioni da X a se stesso, perciò ce ne sono $D_{n,n}$. Quest'ultimo numero coincide proprio con n!

b) Si ha $D_{n,k} = \frac{D_{n,k}\cdot(n-k)!}{(n-k)!} = \frac{n!}{(n-k)!}$.

PROBLEMA V. Sia X un insieme finito con n elementi. Trovare il numero $C_{n,k}$ di sottoinsiemi di X aventi k elementi. Tale numero è anche chiamato numero delle *combinazioni senza ripetizione* di n oggetti a k a k.

TEOREMA 3.15. Si ha $C_{n,0} = 1$, e, per $0 \le k < n$, $C_{n,k} = D_{n,k}/k!$

Dimostrazione. Sia $\mathscr{C}$ l'insieme dei sottoinsiemi di X aventi k elementi. Se k = 0 allora $\mathscr{C} = \{\emptyset\}$ e $C_{n,0} = 1$ per ogni $n \in \mathbf{N}$. Se $k > n$ allora $C_{n,k} = 0$ per il lemma 3.12.

Sia $0 < k \le n$ e sia $\mathscr{D}$ l'insieme delle funzioni iniettive da $\mathbf{N}_k = \{1, 2, \dots, k\}$ ad X. Ad ogni $f \in \mathscr{D}$ associamo la sua immagine Im(f), che ovviamente appartiene a $\mathscr{C}$. Otteniamo una funzione $F: \mathscr{D} \to \mathscr{C}$.

F è suriettiva, poiché dire che $A \subseteq X$ ha k elementi significa proprio dire che esiste $f : \mathbf{N}_k \xrightarrow[\text{su}]{1-1} A$ e quindi esiste $\varphi : \mathbf{N}_k \xrightarrow{1-1} X$ tale che $\varphi(i) = f(i)$ per ogni i; l'immagine di φ è $\varphi(\mathbf{N}_k) = f(\mathbf{N}_k) = A$ e allora $F(\varphi) = A$. Le funzioni $\phi : \mathbf{N}_k \xrightarrow{1-1} X$ tali che $F(\phi) = F(\varphi)$ hanno A per immagine, quindi sono del tipo $\phi : \mathbf{N}_k \xrightarrow[\text{su}]{1-1} A = \mathrm{Im}(\varphi)$, e ce ne sono $D_{k,k} = k!$

Dunque, posto $\phi \mathfrak{R}_F \varphi \Leftrightarrow F(\phi) = F(\varphi)$ le classi di questa relazione d'equivalenza hanno ciascuna k! elementi, e sono tante quanti sono i sottoinsiemi A con k elementi di X; ossia, ce ne sono $C_{n,k} = |\mathscr{C}| = |\mathrm{Im}(F)|$. Pertanto: $D_{n,k} = |\mathscr{D}| = |\mathscr{C}|\cdot k! = C_{n,k}\cdot k!$, da cui segue l'asserto.

Poniamo $\binom{n}{k} = C_{n,k} = \frac{n!}{k!\cdot(n-k)!}$. Questo simbolo si chiama *coefficiente binomiale*, ed è un **numero intero.**

PROPOSIZIONE 3.16. Siano n, k due numeri interi ≥ 0 e sia $k \leq n$.

a) $\binom{n}{0} = \binom{n}{n} = 1$.

b) $\binom{n}{k} = \binom{n}{n-k}$.

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

Dimostrazione. Sia X un insieme con n elementi.

a) $\binom{n}{0}$ è il numero di sottoinsiemi di X con 0 elementi, ossia vuoti, e ce n'è uno solo. Analogamente, di sottoinsiemi di X con n elementi c'è solo X.

b) Per ogni sottoinsieme di X con k elementi c'è il complementare con n-k elementi. Pertanto,

$$\binom{n}{k} = \binom{n}{n-k}.$$

c) Si fissi un elemento x di X. Ogni sottoinsieme Y di X con k elementi è di uno dei due tipi seguenti:

- Y non contiene x: è un sottoinsieme con k elementi di X\{x}, che ha n-1 elementi; di questi Y quindi ce ne sono $\binom{n-1}{k}$;
- Y contiene x: allora Y\{x} è un sottoinsieme con k-1 elementi di X\{x}, che ha n-1 elementi; di questi Y quindi ce ne sono $\binom{n-1}{k-1}$

In totale quindi ci sono $\binom{n-1}{k} + \binom{n-1}{k-1}$ sottoinsiemi Y con k elementi.

Le proprietà a) e c) consentono di costruire un noto triangolo, detto in Italia "Triangolo di Tartaglia", in Francia "Triangolo di Pascal" e così via, ma pare fosse noto anche agli antichi cinesi. Perciò è preferibile chiamarlo *triangolo aritmetico*. Il termine all'incrocio della riga n-esima con la colonna k-esima è $\binom{n}{k}$, ed è ottenuto sommando i termini $\binom{n-1}{k-1}$ ed $\binom{n-1}{k}$, che lo sovrastano nella riga precedente. La somma dei

termini della riga n-esima dà il numero di sottoinsiemi di un insieme con n elementi, che sappiamo essere 2^n.

n \ k	0	1	2	3	4	5	6	7	2^n
0	1								$1 = 2^0$
1	1	1							$2 = 2^1$
2	1	2	1						$4 = 2^2$
3	1	3	3	1					$8 = 2^3$
4	1	4	6	4	1				$16 = 2^4$
5	1	5	10	10	5	1			$32 = 2^5$
6	1	6	15	20	15	6	1		$64 = 2^6$
7	1	7	21	35	35	21	7	1	$128 = 2^7$

COROLLARIO 3.17. - *Formula di Newton* - Siano x e y due numeri reali ed $n \in \mathbf{N}$. Allora $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

Dimostrazione. Se n = 0 oppure n = 1 il risultato è immediato.

Sia $n \geq 2$: $(x+y)^n = (x+y)(x+y)\cdots(x+y)$, e lo sviluppo del secondo membro è la somma dei monomi ottenuti scegliendo un termine da ogni fattore x+y, dunque ogni tal monomio è del tipo $x^{n-k}y^k$, ed è ottenuto scegliendo y da k degli n fattori x+y ed x dagli altri n-k. Pertanto per ognuno degli $\binom{n}{k}$ insiemi di k fattori x+y vi è un monomio $x^{n-k}y^k$; riducendo i termini simili, il coefficiente di questo monomio diviene $\binom{n}{k}$.

NOTA. Posto x = y = 1, dalla formula di Newton si riottiene il numero 2^n di sottoinsiemi di un insieme con n elementi.

Esempio 3.18. Il numero di possibili sestine nel superenalotto si ottiene considerando che da un insieme di n = 90 numeri sostanzialmente se ne estraggono k = 6, distinti. Allora il numero cercato è:

$$C_{90,6} = \binom{90}{6} = \frac{90!}{6!\cdot 84!} = \frac{90\cdot 89\cdot 88\cdot 87\cdot 86\cdot 85}{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 622.614.630.$$

§ 4. Estendere l'insieme dei numeri naturali

Un *monoide* $(M,\cdot,1_M)$ è costituito da un insieme sostegno M, da un'operazione binaria $\cdot$ associativa di cui 1_M è l'elemento neutro. Il monoide si dice *commutativo* se l'operazione $\cdot$ è commutativa, e *regolare* se inoltre valgono le leggi di cancellazione. In tal caso, non deve possedere elemento assorbente. Se ogni suo elemento possiede l'inverso, il monoide prende il nome di *gruppo*.

ESEMPI 4.1.

4.1.a) Sull'insieme **N** dei numeri naturali sono definite le due operazioni di addizione e di moltiplicazione, che con le loro proprietà lo convertono in due monoidi $(\mathbf{N},+,0)$ e $(\mathbf{N},\cdot,1)$, entrambi commutativi, ma mentre il primo è regolare, il secondo no, per la presenza dello zero. Se lo togliamo, otteniamo il monoide $(\mathbf{N}^+,\cdot,1)$, che è a sua volta commutativo e regolare. In entrambi i casi il solo elemento invertibile è l'elemento neutro. Questi due monoidi non sono isomorfi: quello additivo è costituito dai multipli di 1 ossia è *generato da un solo elemento*; quello moltiplicativo non è costituito dalle potenze di un solo elemento, ma dai prodotti delle potenze degli infiniti numeri primi (*infinitamente generato*).

4.1.b) Altre due operazioni notevoli inducono su **N** la struttura di monoide: il *massimo comune divisore* MCD ed il *minimo comune multiplo* mcm. Per ogni coppia (a,b) di numeri naturali, MCD(a,b) è il "più grande" dei divisori comuni, nel senso che è il divisore comune che è multiplo di ogni altro divisore comune. Si tratta di una operazione associativa e commutativa, il cui elemento neutro è lo zero, mentre 1 è elemento assorbente, perché è divisore di tutti. Pertanto, $(\mathbf{N},\mathrm{MCD},0)$ è un monoide commutativo, ma non regolare. Analogamente, mcm(a,b) è il "più piccolo" dei multipli comuni, nel senso che è il multiplo comune che è divisore di ogni altro multiplo comune. Si tratta di una operazione associativa e commutativa, il cui elemento neutro è 1, mentre lo zero è elemento assorbente, essendo multiplo di tutti gli altri. Pertanto, $(\mathbf{N},\mathrm{mcm},1)$ è un monoide commutativo, ma non regolare. Entrambe le operazioni sono anche idempotenti, dato che MCD(a,a) = mcm(a,a) = a. . In entrambi i monoidi il solo elemento invertibile è l'elemento neutro.

La regolarità è una proprietà importante per un monoide, perché consente di immergere il monoide in un gruppo.

TEOREMA 4.2. *Simmetrizzazione di un monoide commutativo regolare.* Sia $(M, *, 1_M)$ un monoide commutativo regolare, allora esiste un gruppo abeliano G, contenente un sottomonoide M' isomorfo ad M e tale che per ogni g∈G esistono a,b∈M' tali che $g = a * b^{-1}$.

Dimostrazione. Si consideri il prodotto cartesiano M×M, i cui elementi sono le coppie ordinate (a, b), con a, b∈M. Si definisca in M×M la seguente operazione:

(a, b)*(c, d) = (a*c, b*d).

Non è difficile provare che essa possiede la proprietà associativa ed ha elemento neutro (1_M, 1_M). Si ha così il monoide (M×M, *, (1_M, 1_M)), che è a sua volta commutativo e regolare.

Si definisca ora in M×M la seguente relazione: (a, b) ~ (a', b') se a*b' = b*a'.

Non è difficile provare che ~ è una relazione d'equivalenza in M×M, ossia che possiede le proprietà riflessiva, simmetrica e transitiva.

Si denoti con [a, b] la *classe d'equivalenza* di (a, b), costituita da tutte le coppie equivalenti ad (a, b). Si tenga presente che se (a, b) ~ (a', b') allora [a, b] = [a', b']; inoltre, due classi distinte hanno sempre intersezione vuota.

A titolo di esempio, una coppia (c, d) è equivalente alla la coppia (1_M, 1_M) se e solo se $c * 1_M = d * 1_M$, ossia se e solo se c = d. Pertanto [1_M, 1_M] = {(a, a) | a∈M} = [a, a] per ogni a∈M.

Denotiamo con G l'insieme M×M/~ delle classi, ossia l'*insieme quoziente*.

La proprietà da sottolineare è la seguente: la relazione ~ è *compatibile* con *:

(a, b) ~ (a', b') e (c, d) ~ (c', d') ⇒ (a*c, b*d) ~ (a'*c', b'*d').

E' allora possibile definire tra le classi la seguente operazione:

[a, b] * [c, d] = [a*c, b*d],

sicuri che il risultato non dipende dalle particolari coppie prescelte per rappresentare le classi d'equivalenza, ma solo dalle classi stesse. Si verifica facilmente che questa operazione in G è associativa, commutativa ed ha elemento neutro [1_M, 1_M]. Inoltre, ogni classe [a, b] possiede l'inversa: è la classe [b, a], infatti,

[a, b] * [b, a] = [a*b, b*a] = [a*b, a*b] = [1_M, 1_M] = 1_G.

Pertanto, (G, *) è un gruppo *abeliano* (ossia con la proprietà commutativa)

Si verifica poi che il sottoinsieme M' costituito dalle classi del tipo [a, 1_M] è un *sottomonoide* del gruppo G e che è isomorfo ad M: l'isomorfismo è la funzione $a \mapsto [a, 1_M]$. Gli elementi di M' si possono identificare allora con quelli di M, cioè per ogni a∈M si pone a = [a, 1_M].

Si osservi che ora per ogni g = [a, b]∈G, si ha [a, b] = [a, 1_M]*[b, 1_M]$^{-1}$, ma allora si può scrivere, in G, [a, b] = a*b^{-1} (o anche = a:b). Ossia, ogni elemento di G è *quoto* di due elementi di M.

La necessità di cercare estensioni dell'insieme dei numeri naturali nasce dall'impossibilità di risolvere in generale le equazioni $a + x = b$ e $a \cdot x = b$. La prima è

formulata nel monoide additivo di (**N**, +, 0), ed ha soluzione se e solo se $a \leq b$; la seconda, escludendo il caso di a e b nulli, lo è nel monoide $\left(\mathbf{N}^+, \cdot, 1\right)$, ed ha soluzione se e solo se a divide b. Con la tecnica della simmetrizzazione dei monoidi commutativi regolari si trova per entrambe le equazioni nuovi insiemi numerici in cui si possono risolvere, ma non lo stesso insieme per entrambe.

Nel caso di (**N**, +, 0) la relazione ~ diventa: (a,b) ~ (c,d) se a+d = b+c. L'operazione tra le coppie è: (a,b)+(c,d) = (a+c, b+d). Il suo elemento neutro è la coppia (0, 0). Poiché si sta parlando in termini di addizione, si parla di *opposto* e non di inverso, e anziché $[a, b]^{-1}$ si scrive -[a, b] = [b, a]. Identifichiamo **N** con il sottoinsieme {[x,0] | x∈**N**}. Allora si ha la seguente proprietà:

ogni elemento [a, b] o appartiene ad **N** o è l'opposto di un elemento di **N**. (*)

Infatti, se $a \geq b$ si ha [a, b] = [a-b, 0], risultando a+0 = b+(a-b).
Se invece a < b, essendo a+(b-a) = b+0, si ha [a, b] = [0, b-a] = -[b-a, 0].
Pertanto la classe [a,b] può essere denotata con il numero naturale a-b quando $a \geq b$, e con -(b-a) quando a < b. Per esempio, [7, 3] = 4, [6, 8] = -2.
Si ha così che il gruppo quoziente è sostanzialmente il gruppo additivo $(\mathbf{Z}, +)$ dei numeri interi relativi. In questo gruppo si ha $a + x = b \Leftrightarrow x = b + \left(-a\right)$

NOTA. Questa costruzione di **Z**, pur così astratta, presenta alcuni vantaggi: le definizioni e le dimostrazioni sono dirette e generali e non è necessario esaminare sottocasi. Essa consentirebbe di definire in **Z** anche la moltiplicazione e l'ordinamento, a partire da quelli di **N**, ma non in modo abbastanza elementare. Si otterrebbe l'anello **Z** e, da questo, con un procedimento generale derivato dalla simmetrizzazione dei monoidi regolari, al campo razionale **Q**. Questa è la via seguita nei corsi universitari. Nei corsi d'Algebra della scuola secondaria non viene però mai seguita.

Nel caso del monoide $\left(\mathbf{N}^+, \cdot, 1\right)$, le coppie (a, b) di elementi di $\mathbf{N}^+$ sono dette *frazioni* e sono scritte nella forma $\frac{a}{b}$. La relazione ~ è in questo caso: $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c$. L'operazione tra le frazioni è: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$. L'elemento neutro è la

frazione $\frac{1}{1}$. Il gruppo quoziente è il gruppo moltiplicativo $\mathbf{Q}^+$ dei "numeri razionali assoluti" (non nulli). L'inverso di $\left[\frac{a}{b}\right]$ è $\left[\frac{b}{a}\right]$. Il sottomonoide corrispondente ad $\mathbf{N}^+$ è $\left\{\left[\frac{a}{1}\right] \,\middle|\, a \in \mathbf{N}^+\right\}$. Identificando a con $\left[\frac{a}{1}\right]$, si ha $\left[\frac{a}{b}\right] = a \cdot b^{-1}$, quindi ogni elemento di $\mathbf{Q}^+$ è *quoto* di due elementi di $\mathbf{N}$. Gli elementi di $\mathbf{Q}^+$ si denotano comunque con $\frac{a}{b}$ anziché con $\left[\frac{a}{b}\right]$ o con ab^{-1}.

Poiché la relazione d'ordine | ("è divisore di") in $\mathbf{N}^+$ non è totale, non vale in $\mathbf{Q}^+$ una proprietà analoga a (*). Infatti per esempio $\frac{2}{3}$ non è un numero naturale e neppure il reciproco di un numero naturale, perché 2 non divide 3 e 3 non divide 2. In questo gruppo, si ha $a \cdot x = b \Leftrightarrow x = a^{-1} \cdot b$. Abbiamo così risolto anche la seconda equazione, ma non nello stesso ambiente, perché i due gruppi $(\mathbf{Z}, +)$ e $(\mathbf{Q}^+, \cdot)$ sono diversi e non sono neppure isomorfi, dato che il primo è ciclico ed il secondo non lo è.

NOTA. Questa costruzione di $\mathbf{Q}^+$ consente di definire agevolmente anche l'addizione, dapprima tra le frazioni ponendo $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ e, poiché anche questa operazione risulta compatibile con la relazione d'equivalenza ~, in seguito anche tra le classi di frazioni, cioè tra numeri razionali assoluti. Considerando anche le frazioni $\frac{0}{b}$, $b \neq 0$, il quoziente $\mathbf{N} \times \mathbf{N}^+/\sim$ con l'addizione quoziente è un monoide commutativo regolare. La simmetrizzazione di tale monoide è il gruppo additivo ($\mathbf{Q}$, +) dei numeri razionali. Esso diviene infine un *campo* estendendo convenientemente anche la moltiplicazione. Questa via è sostanzialmente seguita nei corsi di Aritmetica della scuola secondaria. E' astratta come la precedente, le dimostrazioni non sono facilissime (ma quasi sempre sono omesse), tuttavia la scrittura $\frac{a}{b}$, cui si è abituati fin dalle scuole elementari, la rende abbastanza accessibile.