NOZIONI ELEMENTARI DI ALGEBRA

Si presentano qui alcune nozioni di base di Algebra, sia a scopo di ripasso, sia per introdurre i concetti che saranno poi sviluppati nei capitoli seguenti. Alcune di queste nozioni sono impartite anche nei corsi paralleli di Analisi Matematica e Geometria, ma può essere utile per gli allievi vederle da vari punti di vista.

Prerequisiti: gli insiemi numerici e le nozioni di algebra classica contenute nei programmi della scuola superiore[1].

Contenuto:

§ 1 Insiemi, tavole di verità, operazioni sugli insiemi, relazioni, funzioni, relazioni d'equivalenza e d'ordine.

§ 2 Strutture algebriche: operazioni, proprietà, tipi elementari di strutture algebriche, esempi.

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

[1] Si veda anche il documento "Prerequisiti"

§ 1 – INSIEMI, RELAZIONI E FUNZIONI

Si può introdurre "ingenuamente" l'insiemistica dicendo che il termine *insieme* è sinonimo di collezione, raccolta, ecc. Ci si accorge ben presto di cadere però in alcune contraddizioni, come fu scoperto da subito, alla fine del 1800. Di qui la necessità di trattare la teoria degli insiemi secondo lo stesso schema seguito per esempio dalla geometria razionale e che comprende alcuni passi che riassumiamo per semplicità nell'elenco seguente.

- **Termini primitivi:** *insieme, elemento, appartenenza*. Tali termini vengono rappresentati con i seguenti simboli: gli insiemi con lettere maiuscole, tipo A, B, X,...; gli elementi con lettere minuscole: a, b, x, y,...; l'appartenenza dell'elemento x all'insieme X, con la scrittura $x \in X$; la non appartenenza, con $x \notin X$.

- **Assiomi o postulati:** si tratta di affermazioni (proposizioni) concernenti i termini primitivi (o altri termini da essi derivati), ammesse vere all'inizio della teoria, la cui funzione è tra l'altro quella di definire implicitamente i termini primitivi stessi. Per esempio, il *postulato di estensione* recita:

"*due insiemi cui appartengano gli stessi elementi sono lo stesso insieme*".

- **Definizione di nuovi termini:** ogni termine nuovo che viene introdotto deve essere specificato solo mediante termini già noti. Per esempio: dati due insiemi A e B, si dice che B è sottoinsieme di A, e si scrive $B \subseteq A$, se ogni elemento x appartenente a B appartiene anche ad A.

- **Dimostrazione di teoremi:** una proposizione (= affermazione) è vera se è dedotta, mediante le regole della logica, dai postulati e dai teoremi precedentemente dimostrati. Non si tratta quindi di sperimentare (come in Fisica), di votare (come per le Leggi) o esibire documenti (come in Storia). Per esempio, l'affermazione:

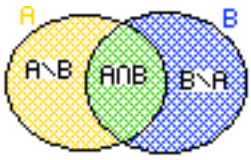
"*Se A e B sono due insiemi e si ha* $A \subseteq B$ *e* $B \subseteq A$, *allora* $A = B$"

si può dimostrare mediante l'assioma di estensione nel modo seguente: da $A \subseteq B$, per definizione di sottoinsieme, segue che ogni elemento x appartenente ad A appartiene anche a B; da $B \subseteq A$ segue analogamente che ogni elemento di B

appartiene anche ad A; pertanto per ogni elemento x si ha che $x \in A$ se e solo se $x \in B$; dal postulato di estensione segue allora $A=B$.

Il postulato di estensione ci consente di descrivere un insieme mediante l'elenco dei suoi elementi (se possibile), raccolti entro due parentesi graffe; per esempio $A = \{\text{Carlo, Anna, Luca}\}$. In generale però un tale elenco non è possibile, ed allora si ricorre ad una proprietà posseduta da tutti e soli gli elementi dell'insieme; per esempio, $A = \{x \mid x \text{ è un cittadino italiano}\}$.
Quest'ultima procedura non sempre è atta a definire un insieme, ma la proprietà scelta deve essere compatibile con gli assiomi. Non vi sono invece problemi se gli oggetti x fra i quali scegliere quelli che soddisfano una data proprietà fanno già parte di un insieme. Più chiaramente, se P(x) è una certa proprietà ed X è un insieme, la scrittura $\{x \in X \mid P(x) \text{ è vera}\}$ definisce sempre un insieme, un sottoinsieme di X.

Una rappresentazione grafica degli insiemi è costituita dai ben noti "diagrammi di Venn". Essi possono costituire un mezzo per comunicare, illustrare le varie nozioni, non per dimostrare teoremi.



Ora, un elenco di procedure che definiscono nuovi insiemi ottenuti a partire da insiemi dati. Si tenga presente che in alcuni casi è un postulato che il risultato sia un insieme.

- *Unione*. Siano A e B due insiemi. Poniamo $A \cup B = \{x \mid x \in A \text{ oppure } x \in B\}$.
- *Intersezione*. Siano A e B due insiemi. Poniamo $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$.
- *Differenza*. Siano A e B due insiemi. Poniamo $A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}$.
- *Differenza simmetrica*. Siano A e B due insiemi. Poniamo $A \Delta B = (A \setminus B) \cup (B \setminus A)$.
- *Insieme delle parti*. Sia X un insieme. Poniamo $\wp(X) = \{A \mid A \subseteq X\}$.
- *Complementare*. Dati un insieme X ed un suo sottoinsieme A, chiamiamo complementare di A in X l'insieme $A' = X \setminus A$.

Indichiamo infine con $\varnothing$ *l'insieme vuoto*, cioè privo di elementi. L'articolo "lo" è giustificato dal postulato di estensione: c'è un solo insieme vuoto.

Un procedimento per definire insiemi e per dimostrare l'eguaglianza di insiemi è costituito dalle tavole di verità. Esse sono relative al calcolo proposizionale e servono per calcolare il valore di verità di una proposizione ottenuta da proposizioni date mediante i connettivi logici "oppure", "e", "implica" ecc. Relativamente agli insiemi, le tavole di verità servono a verificare la proposizione "$x\in X$" per un dato elemento x ed un dato insieme X. Indichiamo con V la verità di tale proposizione e con F la sua falsità. La tavola seguente dimostra il seguente teorema:

"Per ogni coppia di insiemi A e B si ha $A\Delta B = A\cup B\setminus A\cap B$",

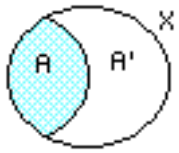
mostrando che per ogni x si ha $x\in A\Delta B$ se e solo se $x\in A\cup B\setminus A\cap B$. (Si noti che si dovrebbe scrivere $(A\cup B)\setminus(A\cap B)$, ma si può convenire che $\cup$ ed $\cap$ abbiano la precedenza su $\setminus$).

$x\in A$	$x\in B$	$x\in A\cup B$	$x\in A\cap B$	$x\in A\setminus B$	$x\in B\setminus A$	$x\in A\Delta B$	$x\in A\cup B\setminus A\cap B$
V	V	V	V	F	F	**F**	**F**
V	F	V	F	V	F	**V**	**V**
F	V	V	F	F	V	**V**	**V**
F	F	F	F	F	F	**F**	**F**

In modo analogo (ma con 8 righe) si possono dimostrare le seguenti proprietà:
Siano A, B, C tre insiemi. Allora $A\cup(B\cup C)=(A\cup B)\cup C$, $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$, $A\cap(B\Delta C)=(A\cap B)\Delta(A\cap C)$, ecc.

Un altro esempio: sia X un insieme, siano $A\subseteq X$ ed A' il complementare di A in X. Questa volta supponiamo in partenza $x\in X$, per cui avremo:

$x\in A$	$x\in A'$	$x\in A\cup A'$	$x\in A\cap A'$
V	F	**V**	**F**
F	V	**V**	**F**



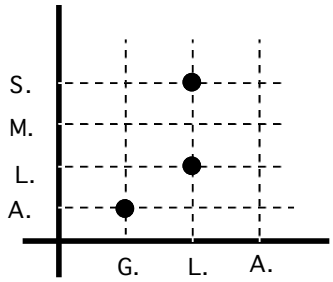
Si ha quindi $A\cap A' = \emptyset$ e $A\cup A' = X$. Due insiemi si dicono *disgiunti* se hanno intersezione vuota. Un sottoinsieme ed il suo complementare sono sempre disgiunti.

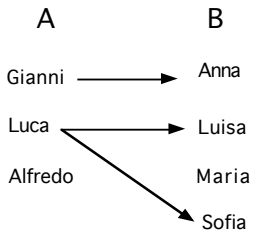
Siano A e B due insiemi e siano $a\in A$ e $b\in B$. Chiamiamo *coppia ordinata* (a,b) l'insieme {{a},{a,b}}. Con questa definizione si ha $(a,b)=(c,d)\Leftrightarrow\begin{cases}a=c\\b=d\end{cases}$. In

particolare $(a,b) = (b,a) \Leftrightarrow a = b$. In modo analogo si definiscono le terne ordinate: siano A, B, C tre insiemi e siano a∈A, b∈B, c∈C; si pone $(a,b,c) = ((a,b),c)$.

L'insieme A×B = {(a,b) | a∈A, b∈B} si chiama *prodotto cartesiano* di A e B. Chiamiamo *relazione* tra A e B ogni terna (A, B, ℜ) dove ℜ è un sottoinsieme del prodotto cartesiano A×B. Per semplicità di linguaggio, se non ci sono ambiguità, spesso viene chiamata relazione l'insieme ℜ.

Rappresentazioni grafiche delle relazioni sono i grafici cartesiani e i diagrammi a frecce. Per esempio, dati gli insiemi A = {Gianni, Luca, Alfredo} e B = {Luisa, Anna, Maria, Sofia}, la relazione ℜ = {(Gianni, Anna), (Luca, Luisa), (Luca, Sofia)} si può rappresentare come nella figura seguente.





Il rappresentare le coppie ordinate (a,b) mediante frecce a→b è usato soprattutto in un particolare tipo di relazioni: le funzioni (o applicazioni) tra insiemi.

Funzioni. Dati due insiemi A e B si chiama *funzione* da A a B, e si denota con f:A→B, una relazione f⊆A×B tale che per ogni x∈A esiste uno ed un solo y∈B tale che (a,b)∈f. Si scrive di solito f:a→b oppure b = f(a) anziché (a,b)∈f.

Per indicare le funzioni, si usano lettere minuscole o talora maiuscole, latine o greche (f, g, F, Φ, σ, ...). Se f:A→B, l'insieme A si dice *dominio* e l'insieme B si dice *codominio* di f. L'insieme $\{b \in B \mid \exists a \in A, f(a) = b\}$ si chiama *immagine di f*, e si denota con Im f o con f(A).

ESEMPIO 1.1. Indichiamo con **Z** l'insieme dei numeri interi relativi e con **Q** l'insieme dei numeri razionali relativi. Siano ora date le seguenti relazioni:

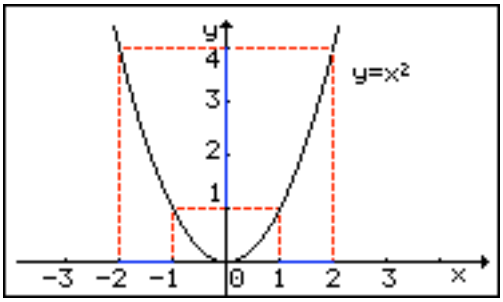
$F_1 = \{(x,y) \mid x,y \in \mathbf{Z},\ x = |y|\}$ (dove |y| indica il valore assoluto di y).

$F_2 = \{(x,y) \mid x,y \in \mathbf{Z},\ y = |x|\}$.

$F_3 = \{(x,y) \mid x \in \mathbf{Q},\ y \in \mathbf{Z},\ \exists q \in \mathbf{Z},\ q \neq 0,\ x = y/q\}$.

Di queste tre relazioni, F_2 è una funzione, mentre F_1 non lo è perché esistono degli $x \in \mathbf{Z}$ che non hanno un corrispondente y: per esempio $x = -1$ non è il valore assoluto di alcun $y \in \mathbf{Z}$. Neppure F_3 è una funzione, poiché ogni numero razionale si può rappresentare con infinite frazioni diverse, quindi ad ogni $x \in \mathbf{Q}$ corrispondono mediante F_3 infiniti numeri interi e non uno solo. Per esempio, ad $x = \frac{1}{2}$ corrisponde non solo 1, ma anche 2, perché per $q = 4$ si ha $\frac{2}{4} = \frac{1}{2} = x$,ecc.

Sia $f:A \to B$ una funzione e siano $C \subseteq A$, $D \subseteq B$. Indichiamo con $f(C)$ l'insieme $\{b \in B \mid \exists a \in C,\ f(c) = b\}$, che si può descrivere anche come $\{f(c) \mid c \in C\}$, e che si chiama *immagine di C in B tramite f*. In particolare, come già detto, $f(A)$ si chiama immagine di f, e si denota spesso con Im f. L'insieme $\{a \in A \mid f(a) \in D\}$ è un sottoinsieme di A detto *controimmagine di D in A tramite f*, e si denota spesso con $f^{-1}(D)$, anche se talora questo simbolo può assumere significati diversi, come vedremo. Nell'esempio a lato c'è la funzione $f : \mathbf{R} \to \mathbf{R}$, $f(x) = x^2$. L'immagine dell'intervallo $[1,2]$ è l'intervallo $[1,4]$, mentre la controimmagine dell'intervallo $[1,4]$ è $[-2,-1] \cup [1,2]$. Si ha poi $\text{Im } f = [0,+\infty[$.



Date due funzioni $f:A \to B$ e $g:A \to B$, aventi quindi lo stesso dominio A e lo stesso codominio B, si ha $f = g$ quando (come insiemi di coppie ordinate) esse posseggono gli stessi elementi. Si ricava allora che $f = g$ se e solo se per ogni $x \in A$ si ha $f(x) = g(x)$.

Siano ora A e B due insiemi. Dal punto di vista "insiemistico" le classi di funzioni più notevoli sono le seguenti:

funzioni iniettive. Una funzione $f:A \to B$ si dice iniettiva, e si scrive $f : A \xrightarrow{1\text{–}1} B$, se per ogni $y \in B$ esiste al massimo un $x \in A$ tale che $y = f(x)$;

funzioni suriettive. Una funzione $f:A \to B$ si dice suriettiva, e si scrive $f : A \xrightarrow{su} B$, se per ogni $y \in B$ esiste almeno un $x \in A$ tale che $y = f(x)$;

funzioni biiettive (o biiezioni). Una funzione f:A→B si dice biiiettiva, e si scrive $f : A \xrightarrow[su]{1\text{–}1} B$, se per ogni y∈B esiste uno ed un solo x∈A tale che y = f(x).
Una funzione biiettiva è pertanto iniettiva e suriettiva.

Una definizione equivalente di funzione iniettiva è la seguente: f:A→B è iniettiva se e solo se per ogni x_1 ed x_2∈A, se $f(x_1) = f(x_2)$ allora $x_1 = x_2$. Per dimostrare che una data funzione è iniettiva si fa generalmente uso di quest'ultima definizione.

Per quanto riguarda le funzioni suriettive, si può dire che una funzione f:A→B è suriettiva se e solo se la sua immagine f(A) coincide col codominio B.

ESEMPI 1.2.

1.2.A. - Sia f:**Z**→**Z** così definita: per ogni x∈**Z** sia f(x) = 2x. Allora f è una funzione iniettiva. Infatti se $f(x_1) = f(x_2)$ allora $2x_1 = 2x_2$, quindi $2x_1-2x_2 = 0$, da cui $2(x_1-x_2) = 0$ e, per la legge di annullamento del prodotto, essendo $2 \neq 0$ deve essere $x_1-x_2 = 0$, ossia $x_1 = x_2$. Questa funzione non è suriettiva. Infatti la sua immagine f(**Z**) contiene solo i numeri pari.

1.2.B. - Sia g:**Q**→**Z** così definita: per ogni x∈**Q** sia g(x) il massimo intero minore o uguale ad x. Per esempio g(-5/4) = -2. Questa funzione è suriettiva, poiché per ogni y∈**Z** esiste certamente almeno un x∈**Q** tale che y = g(x): per esempio il numero razionale rappresentato dalla frazione apparente y/1: g(y/1) = y. La funzione g non è iniettiva: per esempio, g(5/4) = 1 = g(6/5), ma 6/5 e 5/4 non sono lo stesso numero razionale.

1.2.C. - Sia X un insieme qualsiasi e sia id_X:X→X così definita: per ogni x∈X sia $id_X(x) = x$. Questa funzione si chiama *identità su X* ed è una biiezione.

Data una relazione $\mathfrak{R}$ tra due insiemi A e B, si può definire una nuova relazione tra B ed A, detta *trasposta* di $\mathfrak{R}$ ed indicata con $\mathfrak{R}^t$, nel modo seguente:

$$\mathfrak{R}^t = \{(b,a) \mid (a,b) \in \mathfrak{R}\}.$$

Se in particolare consideriamo una funzione f:A→B, la relazione trasposta in generale non è una funzione. Se però f è una biiezione allora la trasposta non solo è una funzione, ma è addirittura una biiezione. Essa si denota con f^{-1} e viene chiamata *funzione inversa* di f. Un nome tradizionale per le biiezioni è

corrispondenza biunivoca, termine che sottintende proprio questa possibilità di definire l'inversa di f. Se invece f non è una biiezione allora la sua trasposta non è mai una funzione.

Siano A, B, C tre insiemi e siano $f:A\to B$ e $g:B\to C$ due funzioni. Definiamo una funzione, che denoteremo con $g\circ f$, tra A e C nel modo seguente: per ogni $x\in A$ sia $y = f(x)$ e sia $z = g(y)$; poniamo $g\circ f(x) = z$, ovvero $g\circ f(x) = g(f(x))$.

$$\begin{array}{ccccc} x & \xrightarrow{f} & y & \xrightarrow{g} & z \\ \downarrow & & & & \uparrow \\ & & g\circ f & & \end{array}$$

ESEMPIO 1.3. Siano $\mathbf{N} = \{0, 1, 2, \ldots\}$ l'insieme dei numeri naturali, $f:\mathbf{N}\to\mathbf{N}$ e $g:\mathbf{N}\to\mathbf{N}$ così definite: $f(x) = x^2+1$, $g(x) = 2x+3$. Allora:

$$g\circ f(x) = g(f(x)) = 2f(x)+3 = 2(x^2+1)+3 = 2x^2+5.$$

In questo particolare caso, i tre insiemi A, B, C della definizione coincidono con **N**, quindi si può calcolare anche $f\circ g$. Si ha:

$$f\circ g(x) = (2x+3)^2+1 = 4x^2+12x+10.$$

Si noti che $f\circ g \neq g\circ f$.

PROPOSIZIONE 1.4. Siano A, B, C, D quattro insiemi e siano $f:A\to B$, $g:B\to C$, $h:C\to D$. Si ha $(h\circ g)\circ f = h\circ(g\circ f)$.

Dimostrazione. Per ogni $x\in A$ siano $y = f(x)$, $z = g(y)$, $t = h(z)$. Allora:

$$((h\circ g)\circ f)(x) = (h\circ g)(f(x)) = (h\circ g)(y) = h(g(y)) = h(z) = t.$$

Analogamente:

$$(h\circ(g\circ f))(x) = h((g\circ f)(x)) = h(z) = t.$$

Perciò per ogni $x\in A$ si ha $((h\circ g)\circ f)(x) = ((h\circ(g\circ f))(x)$, dunque $(h\circ g)\circ f = h\circ(g\circ f)$.

PROPOSIZIONE 1.5. Siano A, B, C tre insiemi.

a) Se $f : A \xrightarrow[\text{su}]{1\text{–}1} B$ allora $f^{-1}\circ f = id_A$, $f\circ f^{-1} = id_B$.

b) Se $f : A \xrightarrow[\text{su}]{1\text{–}1} B$ e $g : B \xrightarrow[\text{su}]{1\text{–}1} C$ allora $g\circ f : A \xrightarrow[\text{su}]{1\text{–}1} C$.

c) Se $f:A\to B$ allora $id_B\circ f = f$ e $f\circ id_A = f$.

Dimostrazione a) per ogni a∈A, posto b = f(a) si ha $f^{-1}(b) = a$, dunque,

$$f^{-1} \circ f(a) = f^{-1}(f(a)) = f^{-1}(b) = a = id_A(a) \Rightarrow f^{-1} \circ f = id_A$$

Allo stesso modo si dimostra che $f \circ f^{-1} = id_B$.

b) Essendo g suriettiva, per ogni c∈C esiste b∈B tale che g(b) = c. Poiché anche f è suriettiva, esiste a∈A tale che f(a) = b. Allora $g \circ f(a) = c$ e quindi $g \circ f$ è suriettiva. Se si ha anche $g \circ f(a') = c$, allora

$$g(f(a')) = c = g(b) \Rightarrow f(a') = b = f(a) \Rightarrow a' = a.$$

Perciò $g \circ f$ è anche iniettiva.

c) Per ogni a∈A, posto b = f(a) si ha

$$id_B \circ f(a) = id_B(f(a)) = id_B(b) = b = f(a) \Rightarrow id_B \circ f = f$$

Analogamente si dimostra che $f \circ id_A = f$.

Definiamo ora due tipi importanti di relazioni tra un insieme e se stesso, le relazioni d'equivalenza e le relazioni d'ordine.

Relazioni d'equivalenza. Sia A un insieme. Sia $\Re$ una relazione su A, ossia un sottoinsieme di A×A. Scriviamo $x\Re y$ anziché $(x,y)\in\Re$. Ciò posto, $\Re$ si dirà *relazione d'equivalenza* se possiede le seguenti tre proprietà:

a) *Riflessiva*: per ogni x∈A si ha $x\Re x$.

b) *Simmetrica*: per ogni x,y∈A, se $x\Re y$ allora anche $y\Re x$.

c) *Transitiva*: per ogni x, y, z∈A, se $x\Re y$ ed $y\Re z$ allora anche $x\Re z$.

Per le relazioni d'equivalenza si usano spesso notazioni particolari: ≅, ~, ≡, =. Data nell'insieme A una relazione d'equivalenza ~, si chiama *classe d'equivalenza* dell'elemento x∈A l'insieme $[x]_\sim = \{y\in A \mid x\sim y\}$. Questo insieme $[x]_\sim$ non è vuoto perché, per la proprietà riflessiva, esso contiene per lo meno x stesso.
L'insieme delle classi d'equivalenza si chiama *insieme quoziente* di A rispetto a ~ e si denota con A/~. Una proprietà notevole delle classi d'equivalenza è la seguente:

PROPOSIZIONE 1.6. Siano dati un insieme A ed una relazione d'equivalenza ~ su A,

a) Per ogni $x, y \in A$ si ha $[x]_\sim = [y]_\sim$ se e solo se $x \sim y$.

b) Per ogni $x, y \in A$, se $[x]_\sim \neq [y]_\sim$ allora $[x]_\sim \cap [y]_\sim = \emptyset$.

Dimostrazione. a) Se $[x]_\sim = [y]_\sim$ allora certamente $y \in [x]_\sim$, quindi $x \sim y$. Viceversa, supponiamo che sia $x \sim y$ e dimostriamo che $[x]_\sim = [y]_\sim$. Per questo proviamo dapprima che $[x]_\sim \subseteq [y]_\sim$. Sia $z \in [x]_\sim$: allora $x \sim z$. Essendo poi per ipotesi $x \sim y$, per la proprietà simmetrica si ha anche $y \sim x$. Per la proprietà transitiva, da $y \sim x$ e $x \sim z$ segue $y \sim z$. Pertanto $z \in [y]_\sim$. Abbiamo quindi provato che ogni elemento $z \in [x]_\sim$ appartiene anche a $[y]_\sim$, dunque $[x]_\sim \subseteq [y]_\sim$. Viceversa, sia $z \in [y]_\sim$: allora $y \sim z$ ed essendo per ipotesi $x \sim y$, per la proprietà transitiva si ha $x \sim z$, quindi $z \in [x]_\sim$. Dunque $[y]_\sim \subseteq [x]_\sim$. Avendo già provato che $[x] \subseteq [y]_\sim$, si ha quindi $[x]_\sim = [y]_\sim$.
b) Siano $x, y \in A$ tali che $[x]_\sim \neq [y]_\sim$. Se per assurdo vi fosse un elemento $z \in [x]_\sim \cap [y]_\sim$ allora $x \sim z$ e $y \sim z$, dunque $x \sim y$ e allora $[x]_\sim = [y]_\sim$.

L'insieme quoziente $A/\sim$ è quindi una *partizione* dell'insieme A, ossia un insieme di sottoinsiemi non vuoti di A tali che a due a due hanno intersezione vuota e ogni $x \in A$ appartiene ad uno (ed uno solo) di essi.

ESEMPI 17.

1.7.A. - Nell'insieme dei poligoni del piano sono note varie relazioni d'equivalenza: la congruenza, la similitudine, l'equiscomponibilità, l'equivalenza (nel senso dell'avere la stessa area).

1.7.B. - Nell'insieme delle rette del piano la relazione di parallelismo in senso debole, secondo la quale due rette sono parallele se coincidono oppure se non hanno punti comuni, è una relazione d'equivalenza. Le classi d'equivalenza si chiamano *fasci di rette parallele* o anche *punti impropri* del piano e l'insieme quoziente si chiama *retta impropria*. Nasce di qui la geometria proiettiva, che considera accanto ai punti e alle rette del piano anche i punti e la retta impropri: in essa due rette hanno sempre uno ed un solo punto in comune, proprio o improprio. Si può osservare che la proprietà transitiva della relazione di parallelismo è equivalente al postulato euclideo delle parallele, nel senso che, se assunta come postulato, da essa discende che per ogni punto del piano passa una ed una sola parallela ad una retta data.

1.7.C. - In ogni insieme A sono relazioni d'equivalenza sia il prodotto cartesiano $A\times A$, sia l'identità id_A. Per la proprietà riflessiva, ogni altra relazione d'equivalenza contiene id_A come sottoinsieme.

1.7.D. - Nell'insieme $\mathbf{Z}$ dei numeri interi relativi fissiamo un numero m e definiamo la seguente relazione: per ogni $x,y\in\mathbf{Z}$, diciamo che x è congruo ad y modulo m, e scriviamo $x \equiv y \pmod m$, se x-y è multiplo di m, ossia esiste $q\in\mathbf{Z}$ tale che $x-y = mq$. Non è difficile provare che la congruenza modulo m è una relazione d'equivalenza:

proprietà riflessiva: per ogni $x\in\mathbf{Z}$ si ha $x-x = 0 = m\cdot 0$, dunque $x \equiv x \pmod m$.

Proprietà simmetrica: se $x \equiv y \pmod m$ allora $x-y = mq$, ma allora $y-x = m(-q)$, quindi anche $y \equiv x \pmod m$.

Proprietà transitiva: se $x \equiv y \pmod m$ ed $y \equiv z \pmod m$ allora $x-y = mq$ e $y-z = mq'$, quindi $y = z+mq'$ e, sostituendo, si ricava $x-(z+mq') = mq$, da cui $x-z = m(q+q')$, ossia $x \equiv z \pmod m$.

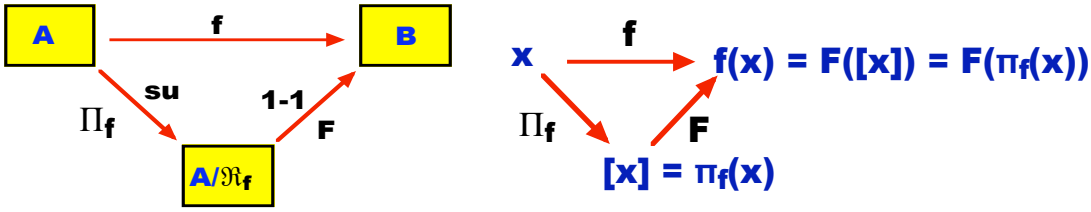
Denotiamo con $[x]_m$ le classi d'equivalenza e con $\mathbf{Z}_m$ l'insieme quoziente.

Se $m = 0$ allora si ha: $x \equiv y \pmod 0$ se e solo se $x-y = 0\cdot q$, ossia se e solo se $x = y$. Dunque la congruenza modulo 0 è l'identità. La congruenza modulo 1 è il prodotto cartesiano $\mathbf{Z}\times\mathbf{Z}$. Negli altri casi vediamo quante sono le classi. Innanzitutto osserviamo che se a ed m sono numeri interi e a è multiplo di m allora a è multiplo anche di -m. Pertanto la congruenza modulo m e la congruenza modulo -m coincidono. Supponiamo quindi $m > 0$. Sappiamo che per ogni $x\in\mathbf{Z}$ esistono $q, r\in\mathbf{Z}$ tali che $x = mq+r$, con $0 \le r < m$. Allora si ha $x-r = mq$, quindi $x \equiv r \pmod m$ e allora $[x]_m = [r]_m$. Allora si ha $\mathbf{Z}_m = \{[0]_m, [1]_m,..., [m-1]_m\}$. Le classi indicate entro le graffe sono tutte distinte; se infatti si ha $0 \le r < s < m$ non può accadere che sia $s-r = mq$, poiché $0 < s-r < s < m$. Allora $\mathbf{Z}_m$ ha esattamente m elementi. In particolare, $\mathbf{Z}_2$ ha due soli elementi: $[0]_2$, costituita dai numeri pari e $[1]_2$, costituita dai numeri dispari.

1.7.E. Dati due insiemi A e B ed $f:A\to B$, in A è definita la relazione $\Re_f$ seguente: per ogni $x_1, x_2\in A$ poniamo $x_1 \Re_f x_2$ se $f(x_1) = f(x_2)$. E' immediato provare che $\Re_f$ è una relazione d'equivalenza. la funzione $\pi:A\to A/\Re_f$, $\pi(x) = \left[x\right]_{\Re_f}$, è suriettiva. La funzione $F:A/\Re_f\to B$, definita da $F\left(\left[x\right]_{\Re_f}\right) = f(x)$, è ben definita, ed è iniettiva:

$$F([x]_{\Re_f}) = F([x']_{\Re_f}) \Leftrightarrow f(x) = f(x') \Leftrightarrow x \Re_f x' \Leftrightarrow [x]_{\Re_f} = [x']_{\Re_f};$$

ha poi per immagine Im f, quindi $F : A/\Re_f \xrightarrow[\text{su}]{1\text{–}1} \text{Im}\, f$, e $f = F \circ \pi$.



Viceversa, data in un insieme A una relazione d'equivalenza ~, si definisca la funzione $\pi: A \to A/\sim$ nel modo seguente: per ogni $x \in A$ sia $\pi(x) = [x]_\sim$. Allora $\Re_\pi = \sim$.

Relazioni d'ordine. Sia A un insieme. Una relazione $\Re \subseteq A \times A$ si dice *relazione d'ordine* su A se possiede le seguenti proprietà:

a) *Riflessiva*: per ogni $x \in A$ si ha $x \Re x$.

b) *Antisimmetrica*: per ogni $x,y \in A$, se $x \Re y$ e $y \Re x$ allora $x = y$.

c) *Transitiva*: per ogni $x, y, z \in A$, se $x \Re y$ ed $y \Re z$ allora anche $x \Re z$.

Una relazione d'ordine si dice *totale* se possiede inoltre la seguente proprietà:

d) *Dicotomia*: per ogni $x, y \in A$ si ha $x \Re y$ oppure $y \Re x$.

Se $\Re$ non possiede questa proprietà, viene detta *ordine parziale*. I simboli usati per le relazioni d'ordine sono di solito: $\leq$, $\subseteq$, $|$, $\Rightarrow$, ecc.

Se A è un insieme e $\leq$ è una relazione d'ordine su A allora la coppia $(A, \leq)$ si chiama *insieme ordinato* o anche *poset* (partially ordered set).

Sia $(A, \leq)$ un insieme ordinato e sia $B \subseteq A$. Si chiama *maggiorante di B* ogni elemento $y \in A$ tale che per ogni $x \in B$ sia $x \leq y$. Si chiama *estremo superiore* di B un maggiorante x_0 di B tale che per ogni altro maggiorante y di B sia $x_0 \leq y$. Si vede subito che se l'estremo superiore esiste allora è unico e si denota con *sup B*. Analogamente sono definiti i minoranti di B e l'*estremo inferiore inf B*. Se sup B esiste ed appartiene a B allora esso si chiama *massimo* di B e si denota con *max B*. Analogamente, se inf $B \in B$ esso si chiama *minimo* di B e si denota con *min B*.

ESEMPI 1.8.

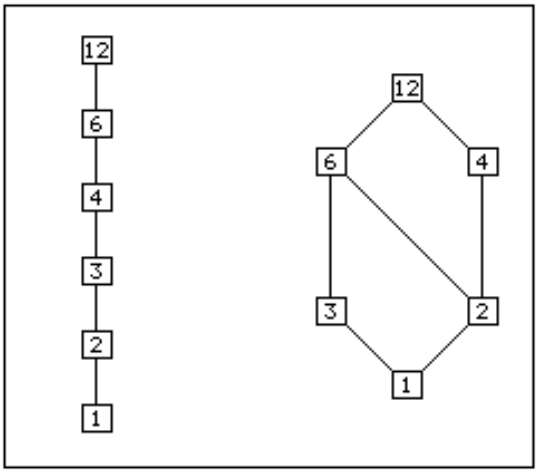
1.8.A. - Indichiamo con $\leq$ l'usuale ordinamento di $\mathbf{N}$, definito nel modo seguente: se $x,y\in\mathbf{N}$ poniamo $x \leq y$ se esiste $d\in\mathbf{N}$ tale che $y = x+d$. Allora $(\mathbf{N}, \leq)$ è un insieme totalmente ordinato. Ogni sottoinsieme non vuoto di $\mathbf{N}$ ha minimo. Il minimo di $\mathbf{N}$ è lo zero; invece, $\mathbf{N}$ non ha estremo superiore.

1.8.B. - In $\mathbf{N}$ poniamo $x|y$ (e diciamo che x divide y) se esiste $q\in\mathbf{N}$ tale che $y = xq$. Allora $(\mathbf{N}, |)$ è un insieme parzialmente ordinato. $\mathbf{N}$ ha massimo 0 e minimo 1 e per ogni coppia di elementi $x, y\in\mathbf{N}$ si ha;

$$\sup\{x,y\} = \mathrm{mcm}(x,y), \qquad \inf\{x,y\} = \mathrm{MCD}(x,y).$$

1.8.C. - Sia X un insieme. Allora $(\wp(X), \subseteq)$ è un insieme parzialmente ordinato. Il massimo di $\wp(X)$ è X ed il minimo è l'insieme vuoto. Per ogni coppia di elementi $A, B\in\wp(X)$ si ha $\sup\{A,B\} = A\cup B$ e $\inf\{A,B\} = A\cap B$.

1.8.D. - Nell'insieme $\mathbf{Z}$ dei numeri interi relativi chiamiamo *positivi* lo zero ed i numeri preceduti dal segno +. Definiamo poi la relazione $\leq$ ponendo, per ogni $x,y\in\mathbf{Z}$, $x \leq y$ se y-x è positivo. Allora $(\mathbf{Z}, \leq)$ è un insieme totalmente ordinato e $\leq$ è il consueto ordinamento di $\mathbf{Z}$.



Nel caso finito è possibile rappresentare un poset $(X, \leq)$ mediante un *diagramma di Hasse*. Esso è basato sulla relazione seguente, detta di *copertura*: $\forall x, y \in X$, $x \prec y$ se $x < y$ e non esiste $z\in X$, $x < z < y$. Nel diagramma gli elementi di X sono rappresentati mediante punti, con le condizioni seguenti: se $x < y$ allora x è più in basso di y e una linea collega x ed y se $x \prec y$. In figura i diagrammi di Hasse dell'insieme dei divisori di 12 ordinato sia mediante l'ordine naturale di $\mathbf{N}$ sia mediante la relazione "è divisore di".

§ 2 – OPERAZIONI E STRUTTURE ALGEBRICHE

Una *operazione binaria (interna)* in un insieme non vuoto X è una applicazione (o funzione) da X×X ad X. Per indicare una operazione si usano i simboli +, × , ·, *, ° ecc. Di solito nelle considerazioni "astratte" si adopera il simbolo · ; in tal caso il risultato dell'operazione sulla coppia (x,y) è detto prodotto ed è indicato con x · y o più brevemente con xy.

La *struttura algebrica* più semplice è una coppia $(X, \cdot)$ formata da un insieme X (non vuoto), detto *sostegno della struttura*, e dall'operazione binaria · su X.

Se X è un insieme finito con n elementi, per definire una operazione si può costruire una tabella, simile alla tavola pitagorica, che contiene i risultati.

ESEMPIO 2.1. Sia $X = \{1,2,3\}$. La tabella

$*$	1	2	3
1	1	2	2
2	1	3	1
3	2	3	1

definisce una operazione in X. In essa per esempio: $2*3=1$, $2*1=1$, ecc. Ognuna delle 9 caselle interne della tavola contiene uno ed uno solo dei 3 elementi di X. Ne segue che sull'insieme X si possono definire ben $3^9 = 19.683$ operazioni diverse!

Naturalmente non tutte le operazioni definibili in un insieme saranno in qualche modo interessanti. Ciò che le rende tali è la presenza di particolari proprietà. Vediamo un elenco delle proprietà più comuni. Scriveremo spesso, come detto sopra, ab in luogo di a · b.

1. *Proprietà associativa*: per ogni a, b, c∈X si ha a(bc)=(ab)c.
2. *Proprietà commutativa*: per ogni a,b∈X si ha ab=ba.
3. *Elemento neutro*: esiste un elemento e∈X tale che:
   per ogni a∈X, a · e = e · a = a .
4. *Elementi simmetrici* (se c'è un elemento neutro e):
   per ogni a∈X esiste a'∈X tale che a · a' = a'· a = e.
5. *Leggi di cancellazione*:
   destra: da ab = cb segue a = c;
   sinistra: da ab = ac segue b = c.

6. Esistenza di *operazioni inverse*:
   destra: per ogni a,b∈X esiste uno ed un solo x∈X tale che $ax = b$;
   sinistra: per ogni a,b∈X esiste uno ed un solo y tale che $ya = b$.
7. *Proprietà di idempotenza*: per ogni a∈X si ha $a \cdot a = a$.
8. *Elemento assorbente*: esiste u∈X tale che, per ogni a∈X, $a \cdot u = u \cdot a = u$.

La lista si potrebbe allungare. Le proprietà elencate si trovano negli esempi più importanti, ma non contemporaneamente. Il primo passo è scoprire quali di queste proprietà possano coesistere, quali si escludano a vicenda, quali siano conseguenza di altre.

Alcune relazioni tra queste proprietà si scoprono facilmente perché sono conseguenza immediata delle definizioni. Per esempio in una struttura $(X, \cdot)$ c'è al massimo un elemento neutro: difatti dati due elementi neutri e_1 ed e_2, si ha $e_1 \cdot e_2 = e_2$, poiché e_1 è elemento neutro, ma anche $e_1 \cdot e_2 = e_1$ poiché anche e_2 è elemento neutro, dunque per l'unicità del prodotto si ha $e_1 = e_2$. Per questo è possibile usare l'articolo determinativo "lo". L'elemento neutro di solito viene indicato con 1_X.

Allo stesso modo si prova che c'è al più un elemento assorbente. Inoltre, vedremo nel capitolo dei gruppi che, se l'operazione è associativa, ogni elemento ha un solo simmetrico. Si potrebbe dimostrare che la presenza delle proprietà 1, 3, 4 implica la presenza delle 5, 6 e (se X ha più di un elemento) l'assenza delle 7, 8, mentre la 2 può valere o no. Per altro le 5, 6 non implicano la 4, ecc.

Alcuni esempi di strutture algebriche note chiariranno meglio la situazione; indichiamo con **N, Z, Q, R, C** rispettivamente gli insiemi dei numeri naturali (compreso lo zero), interi relativi, razionali, reali, complessi, che qui sono dati per noti e per i quali si rinvia al capitolo sugli insiemi numerici. Le dimostrazioni di queste affermazioni si vedranno più avanti.

ESEMPI 2.2

2.2.A. - (**N**, +) ha le proprietà 1, 2, 3, 5. L'elemento neutro è lo zero.

2.2.B. - (**Z**,+), (**Q**,+), (**R**,+) hanno le proprietà 1, 2, 3, 4, 5, 6. L'elemento neutro è lo zero, ogni elemento x ha il simmetrico -x, detto *opposto* di x.

2.2.C. - (**N**, ·) ha le proprietà 1, 2, 3, 8. L'elemento neutro è 1, l'elemento assorbente è lo zero.

2.2.D. - (**N**, MCD), dove MCD indica il massimo comune divisore, ha le proprietà 1, 2, 3, 7, 8. L'elemento neutro è lo zero, l'elemento assorbente è 1.

2.2.E. - Sia $\wp(X)$ l'insieme dei sottoinsiemi di un insieme X e sia $\cup$ l'unione insiemistica: $(\wp(X),\cup)$ possiede le proprietà 1, 2, 3, 7, 8. L'elemento neutro è il vuoto, l'elemento assorbente è X.

Alcune delle proprietà di una struttura $(X,*)$ con X finito, si possono leggere direttamente sulla tavola:

a) La proprietà commutativa si traduce nella simmetria della tavola rispetto alla diagonale che esce dal vertice in alto a sinistra (diagonale principale).
b) L'elemento neutro dà luogo ad una riga e ad una colonna (nella stessa posizione) uguali rispettivamente alla riga sopra la tavola ed alla colonna a sinistra della tavola.
c) La legge di cancellazione assicura che in ogni riga e colonna ogni elemento compaia una volta sola.
d) Ogni elemento ha un simmetrico se e solo se in ogni riga e colonna compare l'elemento neutro e se le posizioni da esso occupate sono simmetriche rispetto alla diagonale principale.
e) L'idempotenza si traduce nel fatto che la diagonale principale è uguale alla colonna a sinistra della tavola.
f) L'elemento assorbente ha solo se stesso nella sua riga e nella sua colonna.

Invece, la proprietà associativa, che è la più importante, non è leggibile sulla tavola, dato che coinvolge tre elementi e non due.

La parte dell'algebra che studia le proprietà generali delle strutture algebriche si chiama "Algebra universale". Essa prende in considerazione anche operazioni con un numero di fattori diverso da due; per esempio le operazioni *ternarie* che operano su tre fattori, e così via. Si definisce poi operazione *unaria* su X ogni funzione da X ad X ed operazione *zeroaria* ogni elemento di X (per es. l'elemento neutro). Chiameremo sinteticamente *operazione finitaria* su X una operazione n-aria, con n intero ≥ 0. Una struttura algebrica è una sequenza formata da un insieme e da una o più operazioni finitarie: $\left(X, f_1, f_2, \ldots, f_r\right)$.

Vediamo ora una breve lista delle più comuni specie di strutture algebriche e per ciascuna alcuni esempi ed alcune nozioni. Le dimostrazioni si

vedranno nei capitoli sui gruppi e sugli anelli. Osserviamo che, quando non vi sia pericolo di ambiguità, una struttura algebrica $(X, f_1, f_2, \dots, f_r)$ viene denotata anche solo con X.

Semigruppo $(S,\cdot)$: l'operazione $\cdot$ è associativa.
Un esempio è $(\{n \in \mathbf{N} \mid n \text{ pari}\}, \cdot)$. I semigruppi sono importanti soprattutto in Analisi Funzionale. Una nozione che si può introdurre in un semigruppo è quella di *potenza*. Sia $(S,\cdot)$ un semigruppo e sia $x \in S$. Poniamo $x^1 = x$ e per ogni altro $n \in \mathbf{N}$, $n>1$, poniamo: $x^n = x^{n-1} \cdot x$. Valgono per queste potenze le due proprietà seguenti, che dimostreremo poi nel capitolo dei gruppi:
per ogni $m,n \in \mathbf{N}$, $m,n \geq 1$, e per ogni $x \in S$ si ha $x^m \cdot x^n = x^{m+n}$ e $(x^m)^n = x^{mn}$.
Inoltre, se $xy = yx$ allora per ogni $n \in \mathbf{N}$ si ha $(xy)^n = x^n y^n$.
Se l'operazione è indicata con + allora si usa il termine *multipli* anziché potenze e in tal caso si scrive nx anziché x^n. Le due proprietà precedenti in questa notazione diventano:

$$mx + nx = (m+n)x, \quad m(nx) = (mn)x, \quad n(x+y) = nx + ny$$

Monoide $(M,\cdot,1_M)$: l'operazione $\cdot$ è associativa ed 1_M ne è l'elemento neutro. Un esempio è $(\mathbf{N},+,0)$, un altro è $(\mathbf{N},\cdot,1)$. Vediamo altri due esempi:

ESEMPI 2.3

2.3.A - *I monoidi di parole*: sia A un insieme finito di oggetti che chiameremo *lettere*; con esse formiamo delle sequenze finite, le *parole* nell'*alfabeto* A. Consideriamo anche la *parola vuota*, indicata per esempio con ø. Sia F_A l'insieme delle parole nell'alfabeto A, compresa la parola vuota, e definiamo in esso la seguente operazione: date due parole w_1 e w_2, attacchiamo la seconda dietro alla prima ottenendo una nuova parola formata dalla sequenza delle lettere della prima e della seconda. Per esempio, se w_1="abra" e w_2="cadabra", la parola ottenuta è w="abracadabra". Indichiamo con $*$ questa operazione, detta *concatenazione di parole*: essa possiede la proprietà associativa e la parola vuota è il suo elemento neutro. Pertanto $(F_A, *, ø)$ è un monoide, detto *monoide delle parole nell'alfabeto* A. Tale monoide ha in ogni caso infiniti elementi. Si osservi che ogni parola w ha una *lunghezza* $\ell(w)$ data dal numero delle sue lettere. In particolare, $\ell(\varnothing) = 0$, e inoltre $\ell(w_1 * w_2) = \ell(w_1) + \ell(w_2)$.

2.3.B - *I monoidi di funzioni*: sia X un insieme non vuoto e sia X^X l'insieme delle funzioni da X in sé; definiamo in X^X la seguente operazione $\circ$, detta composizione di funzioni: siano $f, g \in X^X$; per ogni $x \in X$ siano $y = f(x)$ e $z = g(y)$: poniamo

$(g\circ f)(x) = z$. Si può dimostrare che questa operazione è associativa e che ha per elemento neutro la *funzione identità* id_X che ad ogni $x\in X$ associa se stesso. Il monoide $(X^X, \circ, id_X)$ si chiama *monoide delle funzioni* di X. Se X ha n elementi, dal calcolo combinatorio (v. § 3) sappiamo che esso possiede n^n elementi.

Una proprietà dei monoidi è l'unicità dell'eventuale simmetrico di un elemento: se x ha due simmetrici x' ed x'' si ha:

$$x'=x'\cdot 1_M = x'\cdot (x\cdot x'') = (x'\cdot x)\cdot x'' = 1_M\cdot x'' = x'', \text{ cioè } x' = x''.$$

In un monoide si può inoltre ampliare la nozione di potenza ponendo $x^0=1_M$. Le proprietà delle potenze enunciate per i semigruppi continuano a valere anche se qualche esponente è nullo.

Gruppo $(G,\cdot,1_G,')$: l'operazione $\cdot$ è associativa, 1_G è l'elemento neutro e ogni elemento x ha *il* simmetrico x' (con l'apice ' indichiamo qui la funzione, cioè l'operazione unaria, che ad ogni x associa il suo simmetrico x').
Se l'operazione $\cdot$ possiede anche la proprietà commutativa il gruppo si dice *abeliano*. Di solito nei testi di algebra un gruppo è indicato soltanto con $(G,\cdot)$. Esempi di gruppi abeliani sono (usando la scrittura abbreviata): $(\mathbf{Z},+)$, $(\mathbf{Q},+)$, $(\mathbf{Q}^*,\cdot)$ dove con $\mathbf{Q}^*$ indichiamo l'insieme dei numeri razionali non nulli e con $\cdot$ l'usuale moltiplicazione. Il gruppo $(\{1,-1\},\cdot)$ (sempre indicando con $\cdot$ l'usuale moltiplicazione) è un esempio di gruppo finito con 2 elementi. Vedremo esempi di gruppi nel capitolo apposito. Qui vediamo una macchina per fabbricarne.

ESEMPIO 2.4. In un monoide $(M,\cdot,1_M)$ consideriamo l'insieme M^* costituito dagli elementi che hanno l'inverso rispetto al prodotto. Per ogni $x, y\in M^*$, detti x' ed y' gli inversi, si ha $(xy)' = y'x'$; infatti, $(xy)(y'x') = x(yy')x' = x\cdot 1_M\cdot x' = xx' = 1_M$. Analogamente, $(y'x')(xy) = 1_M$. Pertanto, $xy\in M^*$. Ne segue che la moltiplicazione, che è associativa in M, ristretta ad M^* è una operazione in M^* ed è associativa.
Poi, $1_M \in M^*$ perché 1_M è inverso di se stesso. Infine, se $x\in M^*$ ha per inverso x', allora x' ha per inverso x, quindi anche $x'\in M^*$. Dunque, $\left(M^*,\cdot\right)$ è un gruppo, detto *gruppo delle unità del monoide*.

Nel caso del monoide $(X^X, \circ, id_X)$ delle funzioni dall'insieme X a se stesso, il monoide delle untà è costituito dalle funzioni biiettive da X a se stesso, dette *permutazioni* di X. Tale gruppo si chiama *gruppo simmetrico* su X e si denota con S_X. Sarà studiato in dettaglio nel capitolo dei gruppi.

Anello $(A,+,\cdot,1_A)$: $(A,+)$ è un gruppo abeliano; $(A,\cdot,1_A)$ è un monoide e valgono le due *proprietà distributive* (destra e sinistra) di $\cdot$ rispetto a $+$, ossia:

per ogni $a, b, c \in A$, $(a+b)c = ac+bc$ e $a(b+c) = ab+ac$.

Se l'operazione $\cdot$ è commutativa l'anello si dice *commutativo*. $(\mathbf{Z},+,\cdot,1)$ è un anello commutativo. Vedremo altri esempi e proprietà nel capitolo apposito sugli anelli.

In un anello $(A,+,\cdot,1_A)$ si ha sempre $x\cdot 0_A = 0_A\cdot x = 0_A$, ossia lo zero è *elemento assorbente*. Un anello si dice *integro* se vale la *legge di annullamento del prodotto*: $x\cdot y = 0_A$ solo se $x = 0_A$ oppure $y = 0_A$. Un anello commutativo ed integro è detto dominio d'integrità, ed un esempio è $(\mathbf{Z},+,\cdot,1)$.

Gli elementi di un anello che hanno l'inverso rispetto alla moltiplicazione si dicono *elementi unitari* e costituiscono il gruppo delle unità del monoide $(A,\cdot,1_A)$: si denota con A^* ed è detto *gruppo delle unità* dell'anello. Nel caso di $\mathbf{Z}$ gli elementi unitari sono solo 1 e -1.

Lo zero non è mai invertibile, perciò al massimo si ha $A^* = A \setminus \{0_A\}$: se ciò accade, l'anello si chiama *corpo* e, se è commutativo, si chiama *campo*. Sono campi $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$.

Reticolo $(R, \vee, \wedge)$, dove $\vee$ e $\wedge$ sono operazioni binarie associative, commutative e tali che per ogni $a, b \in R$ si ha:

$a\vee a = a = a\wedge a$ (*idempotenza* delle due operazioni)

$a\vee(a\wedge b) = a = a\wedge(a\vee b)$ (*legge di assorbimento*).

Due esempi di reticoli costruiti sull'insieme dei numeri naturali sono:

- $(\mathbf{N}, \text{MCD}, \text{mcm})$, in cui le due operazioni hanno anche elementi neutri (0 e 1 rispettivamente) e le due operazioni sono anche distributive l'una rispetto all'altra;
- $(\mathbf{N}, \max, \min)$, dove $\max\{a, b\}$ e $\min\{a, b\}$ indicano rispettivamente il più grande ed il più piccolo fra a e b. In quest'ultimo, solo max ha elemento neutro, lo zero.

Gli (eventuali) elementi neutri di $\vee$ ed $\wedge$ si indicano con 0_R ed 1_R rispettivamente. Un reticolo si dice *complementato* se ha gli elementi neutri e per ogni elemento x esiste un elemento x' tale che $x\vee x' = 1_R$, $x\wedge x' = 0_R$.

Un reticolo si dice *distributivo* se le due operazioni sono distributive l'una rispetto all'altra. Se è anche complementato, ogni suo elemento ha un solo complemento.

Un reticolo si dice infine *algebra di Boole* se è distributivo e complementato, e si indica in tal caso con $(A, \vee, \wedge, 0_A, 1_A, ')$. Per esempio, se X è un insieme e $\wp(X)$ è l'insieme dei suoi sottoinsiemi, $\left(\wp(X), \cup, \cap, \varnothing, X, '\right)$ è un'algebra di Boole (indicando qui con Y' il complementare di un sottoinsieme Y di X). Un altro esempio è fornito dall'insieme $D = \{1, 2, 3, 5, 6, 10, 15, 30\}$ dei divisori di 30: indicando con x' il quoziente 30/x, si ha che (D, MCD, mcm, 30, 1, ') è un'algebra di Boole. Si può dimostrare che un'algebra di Boole finita ha 2^n elementi, per un $n \in \mathbf{N}$ opportuno.

In un'algebra di Boole $(A, \vee, \wedge, 0_A, 1_A, ')$ definiamo la seguente operazione, detta *differenza simmetrica*: $x+y = (x \wedge y') \vee (x' \wedge y)$: si può dimostrare che (A, +) è un gruppo abeliano e che $(A, +, \wedge, 1_A)$ è un anello, detto *anello di Boole*. In esso ogni elemento è opposto di se stesso ed è il quadrato di se stesso, ossia A è idempotente. Inversamente, da ogni anello di Boole si può costruire un'algebra di Boole ponendo:

$$x \wedge y = x \cdot y, \; x \vee y = x + y + x \cdot y, \; x' = 1_A + x.$$

In un reticolo $(R, \vee, \wedge)$ poniamo: $x \leq y$ se $x \wedge y = x$. Si può dimostrare che la relazione $\leq$ è un ordine in R, tale che per ogni $a,b \in R$ si ha

$$\begin{cases} \sup(a, b) = a \vee b \\ \inf(a, b) = a \wedge b \end{cases}.$$

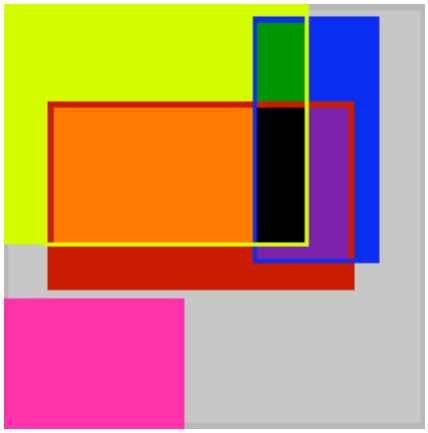
Per esempio, in (N, mcm, MCD) la relazione d'ordine associata è "a è divisore di b"; in $\left(\wp(X), \cup, \cap\right)$ la relazione è "A è sottoinsieme di B". Inversamente, ogni insieme ordinato $(R, \leq)$ nel quale per ogni coppia {x, y} di elementi esistono l'estremo superiore ed inferiore, è un reticolo in cui $x \vee y = \sup\{x, y\}$ ed $x \wedge y = \inf\{x, y\}$. In particolare, ogni insieme totalmente ordinato è un reticolo ed è distributivo.

§ 3 – CALCOLO COMBINATORIO ELEMENTARE

Problema A. In un gruppetto di amici, nove sono tifosi del **Bologna**, sette della **Virtus**, quattro stravedono per **Valentino Rossi**, tre **non s'interessano di sport**. Quanti sono questi amici in tutto?

Problema B. Un consiglio comunale è composto da nove consiglieri del **partito A**, sette del **partito B**, quattro del **partito C**, tre del **partito D**. Quanti sono in tutto i consiglieri?

Che differenza c'è tra i due problemi?



problema A

problema B

Nel caso B si ha una ***partizione*** dell'insieme, nel caso A no.

Il problema generale affrontato dal Calcolo Combinatorio è la determinazione del numero di elementi di cert insiemi finiti conoscendo il numero d'elementi di certi altri insiemi finiti. Nella figura precedente ci sono due di questi problemi: uno ha l'ovvia risposta "23 consiglieri", mentre l'altro è mal posto per mancanza di sufficenti informazioni, quindi è senza risposta.

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

PROPOSIZIONE 3.1 In ogni insieme U di insiemi, l'equipotenza è una relazione d'equivalenza.

Dimostrazione. Per ogni A, B, C appartenenti ad 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 $A \cong C$.

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

Se $X = \emptyset$ poniamo $|X| = 0$; se $X \cong I_n$ poniamo $|X| = n$. $|X|$ si chiama *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 $|A| \le n$.

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

b) Se $X = \emptyset$ allora $A = \emptyset$. Sia $X \neq \emptyset$; $|X| = n$ significa che esiste $f : I_n \xrightarrow{1\text{–}1\ su} X$. Consideriamo l'immagine $f^{-1}(A) \subseteq I_n$ 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, $|A| \le n$.

Qui vedremo alcuni problemi classici in una formulazione che fa uso della teoria degli insiemi e in particolare del teorema visto nell'esempio 1.7.E..

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 $\varphi : I_k \xrightarrow{1-1\ su} A$, $\psi : I_n \xrightarrow{1-1\ su} B$. Definiamo ora una funzione $\Phi : I_{k+n} \xrightarrow{1-1\ su} A \cup B$ ponendo, per ogni $i \in I_{k+n}$,

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

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 $A_1, \dots, A_r$ 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 teor. 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 teor. 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 $|A| = \sum_{i=1}^{m} |C_i| \ge \sum_{i=1}^{m} 1 = m = |\wp|$. 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 $f(x) = f(y)$. Per 1.7.E, essendo f suriettiva esiste una biiezione F tra l'insieme quoziente $A/\Re_f$, che è una partizione di A, e B. 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) $|A \setminus C| = k-r$.

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

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 $|A \setminus C| = |A| - |C| = k-r$.

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

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

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

PROBLEMA II. Siano A e B insiemi finiti. Calcolare $|A \times B|$.

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

Dimostrazione. Se A oppure B è vuoto allora è banale. Altrimenti osserviamo che $A \times B = \bigcup_{a \in A} (\{a\} \times B)$, 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 $b, b' \in B$, quindi $(\{a\} \times B) \cap (\{a'\} \times B) = \varnothing$. Inoltre, per ogni $a \in A$, 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:

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

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

COROLLARIO 3.8. Il principio di moltiplicazione. Se $A_1, \ldots, A_k$ 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 $k \geq 3$, 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. La proprietà espressa dal corollario 3.8 è nota come il *principio di moltiplicazione*: dati gli insiemi *finiti* $A_1, A_2, \ldots, A_k$, rispettivamente con n_1, ... , n_k elementi, ci sono in tutto $\prod_{i=1}^{k} n_i$ *liste* (o *n-uple ordinate*) distinte, ossia il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$ ha $n_1 \cdot n_2 \cdot \cdots \cdot n_k$ elementi distinti. In altre parole, 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). Un esempio è dato dalle colonnine del totocalcio: ci sono 13 caselle, per ciascuna delle quali sono a disposizione i tre simboli 1, 2, x. Allora esistono $3^{13} = 1.594.323$ colonnine distinte.

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

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

Dimostrazione. Sia $A = \{a_1, a_2, \dots, a_k\}$. 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 $(f(a_1), f(a_2), \dots, f(a_r))$.

Quest'ultimo oggetto è un elemento del prodotto cartesiano B^k. Inversamente, dato un qualunque elemento $(b_1, b_2, \dots, b_k) \in B^k$, 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 $(f(a_1), f(a_2), \dots, f(a_r)) \in B^k$ 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.

NOTA. Di norma in un linguaggio non tutte le parole possibili hanno un significato. In natura esiste una specie di linguaggio che usa solo quelle 4 lettere (dette *basi azotate*: adenina, citosina, guanina e timina) per scrivere parole di 3 lettere, (dette *aminoacidi*), ma ne usa solo 20, con le quali forma "frasi" chiamate *proteine*.

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 $n^{(n^2)}$. 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.

a) Se esiste $f : A \xrightarrow{1-1} B$ allora $|A| \leq |B|$.

b) Se $A \subseteq B$ allora $|A| \leq |B|$.

Dimostrazione. a) Poiché f è iniettiva esiste $g:B\to A$ tale che $g \circ f = id_A$: basta infatti fissare $\bar{a} \in A$ e porre $g : b \mapsto \begin{cases} a & \text{se } f(a) = b \\ \bar{a} & \text{se } b \notin f(A) \end{cases}$. Allora g è una funzione, è suriettiva e, per il corollario 3.5, $|A| \leq |B|$.

b) La funzione $i : A\to B$ tale che $i(a) = a$ per ogni $a \in A$ (funzione *inclusione* di A in B, ossia restrizione ad A dell'identità di B) è 1-1.

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 $k \leq n$. 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)!·n. Il simbolo n! si legge "n *fattoriale* ". Si osservi che n! = $D_{n,n}$.

ESERCIZIO 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 $1 \le k \le n$.

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 C l'insieme dei sottoinsiemi di X aventi k elementi. Se k = 0 allora C = {ø} e $C_{n,0} = 1$ per ogni n∈**N**. Se k > n allora $C_{n,k} = 0$ per il lemma 3.12. Sia 0 < k ≤ n e sia D l'insieme delle funzioni iniettive da $I_k = \{1, 2, \ldots, k\}$ ad X. Ad ogni f∈D associamo la sua immagine Im(f), che ovviamente appartiene a C. Otteniamo una funzione F: D→C, che è suriettiva, poiché dire che A⊆X ha k elementi significa proprio dire che esiste $f : I_k \xrightarrow[\text{su}]{1-1} A$ e quindi esiste $\varphi : I_k \xrightarrow{1-1} X$ tale che φ(i) = f(i) per ogni i; l'immagine di φ è $\varphi(I_k) = f(I_k) = A$ e allora F(φ) = A. Ogni classe [φ] della relazione $\Re_F$ è costituita dalle $\phi : I_k \xrightarrow[\text{su}]{1-1} A = \mathrm{Im}(\varphi)$, il cui numero è $D_{k,k} = k!$ Dunque, le classi della relazione $\Re_F$ hanno ciascuna k! elementi e sono tante quanti sono i sottoinsiemi con k elementi di X, ossia sono $C_{n,k} = |C| = |\mathrm{Im}(F)|$. Pertanto: $D_{n,k} = |D| = |C| \cdot k! = C_{n,k} \cdot k!$, 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 ≤ 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. a) Basta ricordare che $0! = 1$, perciò $\binom{n}{0} = \binom{n}{n} = \frac{n!}{0! \cdot n!} = 1$.

NOTA. Sia X un insieme con n elementi. Una dimostrazione combinatoria si basa sul fatto che $\binom{n}{0}$ 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) $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{(n-(n-k))! \cdot (n-k)!} = \binom{n}{n-k}$.

NOTA. Una dimostrazione combinatoria anche in questo caso: 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) $\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)! \cdot (n-k)!} + \frac{(n-1)!}{k! \cdot (n-1-k)!} = \frac{(n-1)! \cdot k + (n-1)! \cdot (n-k)}{k! \cdot (n-k)!} =$

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

NOTA. Anche in questo caso c'è una dimostrazione combinatoria: 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∈**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 ≥ 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 $\binom{n}{k}$.

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

PROBLEMA VI. Sia X un insieme con n elementi. Calcolare il numero π(n) di **partizioni** di X.

Sia $X = \{x_1,..., x_n\}$. Se $\pi = \{B_1,..., B_k\}$ è una partizione con k elementi, la chiamiamo π *k-partizione* di X. Sia $v_{n,k}$ il numero di k-partizioni di X. Si ha subito $v_{n,1} = v_{n,n} = 1$, inoltre

$$\pi(n) = \sum_{k=1}^{n} v_{n,k}\,.$$

Supposto n > 1, poniamo $X^* = X\setminus\{x_n\}$. Sia $\pi = \{B_1,..., B_k\}$ una k-partizione di X. Allora $x_n \in B_i$ per un certo $i \in \{1, ... , k\}$. Distinguiamo due casi:

a) $B_i = \{x_n\}$. Allora $\pi^* = \{B_1,..., B_{i-1}, B_{i+1},..., B_n\}$ è una (k-1)-partizione di X^*.

Inversamente da ogni (k-1)-partizione π^* di X^* si ottiene una ed una sola k-partizione π di X aggiungendole $\{x_n\}$. Pertanto X ha $v_{n-1,k-1}$ k-partizioni di questo tipo.

b) B_i contiene altri elementi oltre x_n. Sia $B'_j = B_j$ per ogni $j \neq i$ e sia $B'_i = B_i\setminus\{x_n\}$. L'insieme $\pi' = \{B_1',...,B_k'\}$ è una k-partizione di X^*. Inversamente, ogni k-partizione di X^* produce k diverse k-partizioni di X di questo secondo tipo aggiungendo l'elemento x_n ad uno qualunque dei B_i', i = 1,...,k. Pertanto X ha $k\cdot v_{n-1,k}$ k-partizioni di questo tipo.

In definitiva, $v_{n,k} = v_{n-1,k-1} + k\cdot v_{n-1,k}$ per ogni k = 1,..., n.

Si può allora costruire un triangolo, simile a quello di Tartaglia, per calcolare $v_{n,k}$ per ogni n, k e quindi per calcolare π(n): nella prima riga c'è $v_{1,1}$, nella seconda $v_{2,1}$ e $v_{2,2}$ e così via.

n \ k	1	2	3	4	5	6	7	8	9	π(n)
1	1									1
2	1	1								2
3	1	3	1							5
4	1	7	6	1						15
5	1	15	25	10	1					52
6	1	31	90	65	15	1				203
7	1	63	301	350	140	21	1			877
8	1	127	966	1701	1050	266	28	1		4140
9	1	255	3025	7770	6951	2640	462	36	1	21147

Esercizio 3.18. Determinare le cinque partizioni dell'insieme $X = \{1,2,3\}$.