Appunti per gli studenti di Matematica Discreta (A-L)- Cdl Informatica, Bari

A. Lotta

A.A. 2022-23

COPPIE ORDINATE

Considerati due oggetti qualsiasi, è possibile formare l'insieme

$$\{a, b\}$$

che contiene esattamente a e b. Si noti che, se $a = b$, allora

$$\{a, b\} = \{a\} = \{b\}.$$

Tale insieme può essere utile per raggruppare coppie di oggetti tra loro in base ad un certo criterio, ovvero trattare una certa relazione tra oggetti. Volendo considerare relazioni di natura qualsiasi, bisogna notare che questo modo di procedere ha un problema; infatti, in ogni caso si ha:

$$\{a, b\} = \{b, a\},$$

ovvero l'ordine con cui si considerano i due oggetti per formare tale insieme non è rilevante, ciò significa che c'è una simmetria intrinseca nel modo in cui raggruppiamo oggetti. Tenendo conto di ciò, chiameremo l'insieme $\{a, b\}$ la *coppia non ordinata* formata da a e b.

In molte situazioni concrete è importante invece tener conto dell'ordine in cui gli oggetti sono considerati nel momento in cui essi vengono confrontati in base ad un determinato criterio. Per questo scopo, si utilizzano le coppie ordinate.

Se a e b sono oggetti qualsiasi, il simbolo

$$(a, b)$$

denota la **coppia ordinata** avente a come prima coordinata (primo elemento) e b come seconda coordinata (secondo elemento).
Due coppie ordinate (a, b) e (a', b') si definiscono *uguali* se e solo se:

$$a = a' \text{ e } b = b'.$$

Quindi in generale

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

Non si deve confondere (a, b) con l'insieme $\{a, b\}$.

Es.: Si considerino gli elementi 1 e -1 dell'insieme $\mathbb{Z}$; allora

- $(-1, 1) \neq (1, -1)$
- $\{-1, 1\} = \{1, -1\}$.

- La coppia $(-1, -1)$ ha l'elemento -1 sia come prima che come seconda coordinata.

Si osservi che l'insieme $\{-1, -1\}$ è costituito dal solo elemento -1: pertanto $\{-1, -1\} = \{-1\}$.

PRODOTTO CARTESIANO DI INSIEMI

Definizione: Siano A e B due insiemi. Si dice **prodotto cartesiano** (o semplicemente prodotto) di A per B l'insieme di **tutte** le coppie ordinate (a, b) la cui prima coordinata a appartiene ad A e la cui seconda coordinata b appartiene a B.

Il prodotto cartesiano di A per B si denota col simbolo

$$A \times B.$$

Dunque

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

Notazione: Nel caso in cui $A = B$, il prodotto $A \times A$ viene anche denotato con A^2.

Osserviamo che, per ogni insieme A risulta:

$$A \times \emptyset = \emptyset = \emptyset \times A.$$

Attenzione: in generale $A \times B \neq B \times A$.

Es. Siano $A = \{3, 4, 7\}$ e $B = \{a, b\}$. Allora

$$\begin{aligned}
A \times B &= \{(3, a), (3, b), (4, a), (4, b), (7, a), (7, b)\} \\
B \times A &= \{(a, 3), (a, 4), (a, 7), (b, 3), (b, 4), (b, 7)\} \\
A \times A &= \{(3, 3), (3, 4), (3, 7), (4, 3), (4, 4), (4, 7), (7, 3), (7, 4), (7, 7)\} \\
B \times B &= \{(a, a), (a, b), (b, a), (b, b)\}.
\end{aligned}$$

RELAZIONI

Definizione: Siano A e B due insiemi. Una *relazione* o *corrispondenza da A in B* è un qualsiasi **sottoinsieme** di $A \times B$.

Nel caso in cui A=B, una relazione da A ad A prende il nome di *relazione su A*.

Attenzione: Se $A \neq B$, una relazione da A a B non è una relazione da B in A!

Esempio: Siano $A = \{1, 2, 5, 7, 8\}$ e $B = \{a, b, r, s\}$.

Sono relazioni:

$$\{(1, a), (1, s), (5, b), (8, s), (2, r)\} \quad \text{da } A \text{ in } B$$
$$\{(2, a), (5, s)\} \quad \text{da } A \text{ in } B$$
$$\{(a, 1)\} \quad \text{da } B \text{ in } A$$

Non sono invece relazioni, nè da A a B, nè da B in A, gli insiemi:

$$\{(a, 1), (8, s), (2, r)\}$$
$$\{(2, 5), (7, s)\}.$$

Esempio: Si consideri la seguente relazione su $\mathbb{N}$:

$$\leq = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \exists t \in \mathbb{N} \text{ tale che } m = n + t\}.$$

Questa è l'usuale *relazione d'ordine* su $\mathbb{N}$, con la quale siamo abituati a *confrontare* tra loro i numeri naturali.

Sia $\mathcal{R}$ una relazione da un insieme A ad un insieme B, cioè $\mathcal{R} \subseteq A \times B$. Allora, invece di scrivere $(a, b) \in \mathcal{R}$, si usa scrivere

$$a \,\mathcal{R}\, b.$$

Questa scrittura si legge "a è nella relazione $\mathcal{R}$ con b".

Qualora $(a, b) \notin \mathcal{R}$, si usa la notazione

$$a \;\not\mathcal{R}\; b$$

che si può leggere "a non è in relazione con b."

Es: Sia $A = \{1, 2, 3, 4, 5\}$. Allora

$$\mathcal{R} = \{(1, 1), (1, 3), (4, 5), (2, 3)\}$$

è una relazione su A; per tale relazione possiamo scrivere:

$$1 \,\mathcal{R}\, 1,\ 1 \,\mathcal{R}\, 3, 4 \,\mathcal{R}\, 5$$

e

$$1 \;\not\mathcal{R}\; 2.$$

Osservazione: Giacchè *ogni* sottoinsieme $\mathcal{R}$ di $A \times B$ è una relazione dall'insieme A all'insieme B, non si escludono i casi estremi, ossia:

- $\mathcal{R} = \emptyset$: nessun elemento di A è in relazione con elementi di B;
- $\mathcal{R} = A \times B$: ogni elemento di A è in relazione con ogni elemento di B.

La notazione appena introdotta permettere di maneggiare le relazioni in modo più snello e intutivo; nella pratica, per definire una certa relazione da A in B si esplicita il criterio secondo il quale è vero o no che $a \,\mathcal{R}\, b$. Ciò significa isolare il sottoinsieme di $A \times B$ costituito da tutte e solo le coppie (a, b) per le quali tale criterio risulta soddisfatto, e fare questo significa definire una relazione in accordo con la definizione rigorosa che è stata data.

Ad esempio, si può definire una relazione $\mathcal{R}$ su $\mathbb{Z}$ dichiarando:

$$a \,\mathcal{R}\, b \iff a - b \text{ è pari.}$$

Si tratta di un modo più snello di porre

$$\mathcal{R} := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} |\ a - b \text{ è pari}\}.$$

In base alla definizione data abbiamo ad esempio $3 \,\mathcal{R}\, 5$, mentre $2 \;\not\mathcal{R}\; 5$.

RELAZIONI SIMMETRICHE

Definizione: Una relazione $\mathcal{R}$ su un insieme A si dice *simmetrica* se per ogni $a, b \in A$, se è vero che $a \mathcal{R} b$, allora è vero anche che $b \mathcal{R} a$.

In simboli, la condizione di simmetria per una relazione $\mathcal{R}$ è:

$$\forall a, b \in A \qquad a \mathcal{R} b \Rightarrow b \mathcal{R} a.$$

Es: La relazione $\mathcal{R}$ su $\mathbb{Z}$ definita con il criterio seguente è simmetrica:

$$a \mathcal{R} b \iff a^2 = b^2.$$

Es: La relazione su $\mathbb{N} \times \mathbb{N}$ definita da:

$$(a, b) \mathcal{R} (c, d) \iff a + b = c + d$$

è simmetrica.

Un esempio di relazione *non* simmetrica è l'usuale relazione $\leq$ con cui vengono confrontati numeri (naturali, interi, razionali, reali).

Si può osservare che assegnare una relazione simmetrica su un insieme equivale di fatto ad assegnare un insieme di coppie non ordinate (sebbene la definizione coinvolga coppie ordinate). Ciò è dovuto alla condizione aggiuntiva di simmetria. Ad esempio, se si considera su $A = \{1, 2, 3, 4, 5\}$ l'insieme

$$\{\{1, 3\}, \{2, 5\}, \{1\}\},$$

ad esso corrisponde un'unica relazione simmetrica $\mathcal{R}$, ricostruibile a partire da tale dato, ponendo:

$$\mathcal{R} = \{(1, 3), (3, 1), (2, 5), (5, 2), (1, 1)\}.$$

In generale, ogni coppia non ordinata $\{a, b\}$ nell'insieme assegnato genera le due coppie (a, b) e (b, a) che devono essere entrambe incluse nella costruenda relazione simmetrica.
Viceversa, ad ogni relazione simmetrica si può associare un insieme di coppie non ordinate, semplicemente sostituendo (a, b) con $\{a, b\}$; così facendo non viene persa alcuna informazione, a patto di ricordare che la relazione originaria soddisfa la condizione di simmetria.

RELAZIONI FUNZIONALI E APPLICAZIONI

Definizione: Siano A e B due insiemi non vuoti e sia f una relazione da A a B. Si dice che f è una *relazione funzionale* o *funzione* o anche *applicazione da A in B* se verifica la seguente condizione:

per ogni $a \in A$ esiste uno ed un solo elemento $b \in B$ tale che

$$a\, f\, b.$$

In altri termini, si richiede che *ciascun $a \in A$ sia in relazione con uno ed un solo elemento $b \in B$.*

Si fissi l'attenzione sul fatto che per ogni $a \in A$ devono essere soddisfatte due condizioni: esistenza di b in relazione con esso ed unicità di tale oggetto verificante tale proprietà.

Per ogni fissato $a \in A$, l'unico elemento $b \in B$ per cui $a\, f\, b$ si denota con

$$f(a)$$

e viene chiamato **valore della funzione f in a**, o anche **immagine di a mediante f**.

Dunque, per ogni $a \in A$ e $b \in B$, per definizione abbiamo

$$b = f(a) \iff a\, f\, b.$$

Per esprimere il fatto che b è l'immagine di a, si usa anche la notazione:

$$f : x \mapsto b.$$

Es: Dati $A = \{1, 2, 3, 4, 5\}$ e $B = \{5, 6, 7, 9, 11\}$ si consideri la relazione f da A in B:

$$f = \{(1, 5), (2, 6), (2, 9), (3, 11), (5, 9)\}.$$

Questa relazione *non* è una funzione. Infatti, vi sono le seguenti due eccezioni alle condizioni richieste:

-l'elemento 2 è in relazione con *due* elementi di B (compare in due coppie);

–l'elemento 4 *non* è in relazione con alcun elemento di B (non compare in alcuna coppia).

Invece

$$g = \{(1, 5), (2, 6), (3, 11), (5, 9), (4, 9)\}$$

è un'applicazione.

Attenzione: Il fatto che 4 e 5 siano in relazione con lo stesso elemento 9 di B **non** è vietato dalla definizione! Dunque in tal caso $g(4) = 9 = g(5)$.

Per indicare che una relazione $f \subset A \times B$ dall'insieme A nell'insieme B è un'applicazione si usa la notazione:

$$f : A \to B.$$

Def: Data un'applicazione $f : A \to B$, l'insieme A è detto **insieme di partenza** dell'applicazione f, oppure **dominio**, mentre B è detto **insieme di arrivo** di f.

Nota importante: Si è soliti definire un'applicazione $f : A \to B$ stabilendo una legge che determina, **in modo univoco**, per ogni $x \in A$ chi è $f(x)$. La relazione corrispondente è quindi ricostruibile come $\{(x, f(x)) | x \in A\}$. Tale procedimento è implicito e nella pratica si identifica l'applicazione f con la legge stessa che la determina.

Esempio Possiamo definire un'applicazione $f : \mathbb{Z} \to \mathbb{Z}$ ponendo:

$$\forall x \in \mathbb{Z} \quad f(x) := 2x$$

Si tratta di una funzione, perchè per ogni intero x, l'intero $2x$ esiste sempre ed è univocamente determinato da x. In questo caso f altri non è che la relazione

$$f = \{\, (x, 2x) \mid x \in \mathbb{Z} \,\}.$$

Abbiamo ad esempio

$$f(-4) = -8,\ f : 5 \mapsto 10.$$

Esempio: La legge $f : \mathbb{Q} \to \mathbb{Q}$ data da

$$x \mapsto \frac{1}{x}$$

non definisce un'applicazione perchè 0 non ha immagine! Infatti, l'espressione $1/x$ perde di significato per $x = 0$.

Invece, se si sceglie come primo insieme $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, allora si può definire l'applicazione $g : \mathbb{Q}^* \to \mathbb{Q}$ tale che

$$\forall x \in \mathbb{Q}^* \quad g(x) = \frac{1}{x}.$$

COMPOSIZIONE DI APPLICAZIONI

Definizione: Siano A, B e C insiemi e siano $f : A \to B$ e $g : B \to C$ applicazioni, tali che il dominio di g coincida con l'insieme di arrivo di f.
Si dice *applicazione composta* di f e g e si denota con $g \circ f$, l'applicazione

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

definita ponendo

$$(g \circ f)(a) = g(f(a)) \qquad \text{per ogni } \ a \in A. \tag{$*$}$$

Talvolta $g \circ f$ viene denotata con gf e chiamata *applicazione prodotto* di f per g.

Nota: La notazione $g \circ f$ è corente col fatto che f è la **prima** applicazione ad essere usata nel calcolare l'immagine di un elemento di A.
Spesso per indicare l'applicazione composta $g \circ f$ si fa uso del seguente diagramma:

$$A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C$$

Es: Sia $f : \mathbb{N} \to \mathbb{N}$ definita da $f(x) = 2x$ per ogni $x \in \mathbb{N}$, e sia $g : \mathbb{N} \to \mathbb{Z}$ definita da $g(x) = -x^2$ per ogni $x \in \mathbb{N}$.
Allora ha senso considerare $g \circ f : \mathbb{N} \to \mathbb{Z}$ e risulta

$$(g \circ f)(x) = g(f(x)) = g(2x) = -(2x)^2 = -4x^2.$$

Es: Consideriamo le applicazioni $f : \mathbb{Z} \to \mathbb{Z}$ definita da $f(x) = x^2$ e $g : \mathbb{Z} \to \mathbb{Z}$ definita da $g(x) = 2$ per ogni $x \in \mathbb{Z}$. In tal caso si possono considerare entrambe le applicazioni composte $f \circ g$ e $g \circ f$. Determinandole esplicitamente, risulta:

$$(g \circ f)(x) = g(f(x)) = g(x^2) = 2$$

e

$$(f \circ g)(x) = f(g(x)) = f(2) = (2)^2 = 4,$$

per ogni $x \in \mathbb{Z}$.

APPLICAZIONI INGETTIVE

Definizione: Un'applicazione $f : A \to B$ si dice *ingettiva* o *ingezione* se elementi distinti del dominio hanno sempre immagini distinte mediante f.

Dunque f è ingettiva se per ogni $a, a' \in A$, $a \neq a'$ si ha sempre $f(a) \neq f(a')$, ovvero in modo più formale, se è soddisfatta la condizione seguente:

$$\forall a, a' \in A : \qquad a \neq a' \Rightarrow f(a) \neq f(a').$$

Nota importante: La stessa proprietà si può anche formulare:

$$\textit{per ogni } a, a' \in A, \textit{ se } f(a) = f(a') \textit{ allora } a = a',$$

ovvero, in modo più formale:

$$\forall a, a' \in A : \qquad f(a) = f(a') \Rightarrow a = a'.$$

Es: Dati $A = \{1, 2, 3\}$ e $B = \{4, 5, 7, 9, 10\}$, l'applicazione $f : A \to B$ tale che

$$f(1) = 4,\ f(2) = 5,\ f(3) = 10$$

è ingettiva, mentre l'applicazione $g : A \to B$

$$g(1) = 4,\ g(2) = 5,\ g(3) = 4$$

non è ingettiva avendosi $g(1) = g(3)$.

Es: Sia $f : \mathbb{N} \to \mathbb{Z}$ l'applicazione data da

$$f(n) = -3n + 2.$$

Essa è ingettiva. Infatti, siano $n, n' \in \mathbb{N}$ tali che $f(n) = f(n')$. Allora

$$-3n + 2 = -3n' + 2$$

da cui deduciamo

$$-3n = -3n'$$

e quindi

$$n = n'.$$

Es: Sia $f : \mathbb{Z} \to \mathbb{N}$ l'applicazione tale che

$$f(x) = x^2 \qquad \text{per ogni } \; x \in \mathbb{Z}.$$

f non è ingettiva. Infatti, ad esempio, risulta $f(2) = f(-2)$.

Es: : Non esiste alcuna applicazione ingettiva $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3\}$.

Il motivo risiede nel fatto che l'insieme di partenza contiene 5 elementi distinti; le corrispondenti immagini non possono essere tutte distinte, perchè l'insieme di arrivo $\{1, 2, 3\}$ non potrebbe contenerle tutte.

Tale osservazione ovviamente può essere generalizzata e verrà formalizzata in seguito come *principio dei cassetti*; in maniera informale, sappiamo che se si vogliono conservare delle camicie in una cassettiera che ha a disposizione meno cassetti rispetto alle camicie, non è possibile farlo in modo che le camicie occupino cassetti tutti diversi (alla fine dovrà esserci almeno un cassetto contenente due o più camicie).

IMMAGINI DI INSIEMI MEDIANTE APPLICAZIONI

Definizione: Si consideri un'applicazione $f : A \to B$. Dato un sottoinsieme $X \subset A$, si chiama **immagine di X mediante** f il sottoinsieme di B, denotato con

$$f(X)$$

costituito da tutte le immagini $f(x)$ al variare di $x \in X$. In simboli:

$$f(X) := \{\, f(x) \mid x \in X \,\}.$$

L'immagine di A stesso, ovvero $f(A)$, si chiama **immagine dell'applicazione** f. Tale insieme talvolta si denota anche con $\mathrm{Im}(f)$.

Es: Consideriamo l'appicazione $f : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ tale che

$$1 \mapsto c, \quad 2 \mapsto b, \ 3 \mapsto c, \ 4 \mapsto a.$$

Allora l'immagine $f(X)$ di $X = \{1, 3, 4\}$ è $f(X) = \{a, c\}$.
Si noti che l'immagine di f è $\{a, b, c\}$; essa non contiene l'elemento d: l'applicazione non assume mai d come valore.

APPLICAZIONI SURGETTIVE

Definizione: Un'applicazione $f : A \to B$ si dice *surgettiva* o *surgezione* se la sua immagine coincide con l'intero insieme di arrivo, cioè se:

$$f(A) = B.$$

Dunque affinchè un'applicazione sia surgettiva è richiesto che *ogni* $b \in B$ sia della forma $b = f(a)$ per *almeno un* elemento $a \in A$.

In simboli, la condizione di surgettività è:

$$\forall b \in B \ \exists a \in A : \ b = f(a).$$

Es: Dati $A = \{1, 2, 3\}$ e $B = \{0, 5\}$, l'applicazione $f : A \to B$ tale che

$$f(1) = 0, \ f(2) = 0, \ f(3) = 5$$

è surgettiva.

Nessuna applicazione $g : B \to A$ è surgettiva, perchè $Im(g) = \{g(0), g(5)\}$ può essere costituito da al più due elementi distinti, per cui certamente $Im(g) \neq A$.

Es: L'applicazione $f : \mathbb{N} \to \mathbb{Z}$ definita da:

$$f(n) = -n$$

non è surgettiva. Infatti, ad esempio, non esiste alcun $n \in \mathbb{N}$ tale che $f(n) = 1$. In effetti, l'immagine di f è costituita da tutti e soli i numeri interi ≤ 0.

BIGEZIONI

Definizione: Un'applicazione si dice **bigettiva** o **bigezione** o anche **corrispondenza biunivoca** se è ingettiva ed è surgettiva.

Mettendo insieme le caratterizzazioni delle applicazioni ingettive e surgettive discusse in precedenza, otteniamo che *un'applicazione $f : A \to B$ è bigettiva se e solo per ogni $b \in B$ esiste uno ed un solo $a \in A$ tale che $f(a) = b$.*
In simboli, la condizione in esame è:

$$\forall b \in B \ \exists!\ a \in A : \ b = f(a).$$

Es: L'applicazione $f : \mathbb{Z} \to \mathbb{Z}$ definita da

$$f(x) = 4 - x \qquad \text{per ogni } \ x \in \mathbb{Z}$$

è una bigezione. Infatti:

f è ingettiva: per ogni $x, y \in \mathbb{Z}$ se $f(x) = f(y)$, allora si ha:

$$4 - x = 4 - y$$

da cui $x = y$.
f è surgettiva: dato un qualsiasi $y \in \mathbb{Z}$ esiste $x \in \mathbb{Z}$ tale che $f(x) = y$; infatti l'equazione

$$4 - x = y$$

ammette l'unica soluzione intera $x = 4 - y$.

Es: L'applicazione $f : \mathbb{Q} \to \mathbb{Q}$ definita da:

$$f(x) = \frac{4}{x^2 + 1} \qquad \text{per ogni } \ x \in \mathbb{Q}$$

non è bigettiva, anzi non è ingettiva e non è surgettiva. Infatti, per ogni x risulta $f(x) = f(-x)$ per cui f non è ingettiva. Inoltre, osservato che $\frac{4}{x^2+1}$ è un numero *positivo* qualunque sia $x \in \mathbb{Q}$, certamente $f(\mathbb{Q}) \neq \mathbb{Q}$.

PREIMMAGINI

Sia $f : A \to B$ un'applicazione.

Def: Se $b \in B$, ogni elemento a di A tale che $f(a) = b$ si dice *una preimmagine* dell'elemento b. L'insieme di tutte le preimmagini di b si denota con $f^{-1}(b)$ (può essere vuoto).

È importante fissare l'attenzione sui seguenti fatti:

- assegnato $a \in A$, l'**immagine** di a tramite f è **unica**;
- un elemento qualsiasi $b \in B$ può avere **nessuna, una o più preimmagini** in A.

Inoltre, dalle definizioni segue:

- Una funzione $f : A \to B$ è ingettiva se e solo se ogni $b \in B$ ha nessuna o esattamente una preimmagine $a \in A$.

- Una funzione $f : A \to B$ è surgettiva se e solo se ogni $b \in B$ ha almeno una preimmagine $a \in A$.

- Una funzione $f : A \to B$ è bigettiva se e solo se ogni $b \in B$ ha esattamente una preimmagine $a \in A$.

BIGEZIONE INVERSA

Definizione: Sia $f : A \to B$ una bigezione.
Si chiama *inversa* di f l'applicazione $f^{-1} : B \to A$ che associa ad ogni $y \in B$ la sua **unica** preimmagine in A.

Quindi per ogni b in B, si ha che $f^{-1}(b)$ è l'unico elemento di A per cui

$$f(b) = a.$$

Nota: In termini della definizione originaria di funzione come relazione, abbiamo

$$f^{-1} = \{(b, a) \in B \times A |\, f(a) = b\}.$$

Esempio: L'applicazione $f : \mathbb{Q} \to \mathbb{Q}$ definita da:

$$f(x) = \frac{3x - 1}{2} \qquad \text{per ogni } \; x \in \mathbb{Q}$$

è una bigezione.

Per verificarlo, basta controllare che ogni $y \in \mathbb{Q}$ ha un'unica preimmagine $x \in \mathbb{Q}$; ciò si traduce nel controllare che l'equazione

$$f(x) = y$$

ovvero

$$\frac{3x - 1}{2} = y$$

ammette una ed una sola soluzione razionale. Risolvendo l'equazione otteniamo

$$3x - 1 = 2y$$

$$3x = 2y + 1$$

$$x = \frac{2y + 1}{3}.$$

La soluzione ottenuta esiste ed è univocamente determinata in $\mathbb{Q}$, qualsiasi sia y, e quindi l'applicazione è bigettiva.

L'inversa di f è data dunque da $f^{-1} : \mathbb{Q} \to \mathbb{Q}$ tale che:

$$f^{-1}(y) = \frac{2y + 1}{3}.$$

In base alla definizione di inversa e di preimmagine di un elemento $y \in \mathbb{Q}$, notiamo che possiamo procedere alla verifica che la funzione appena determinata è l'inversa di f, andando a controllare che valga:

$$f(f^{-1}(y)) = y$$

sempre per un y qualsiasi. In effetti:

$$f\left(\frac{2y + 1}{3}\right) = \frac{3(\frac{2y+1}{3} - 1)}{2} = \frac{6y}{6} = y.$$

Esempio: Gli insiemi $\mathbb{Z}$ ed $\mathbb{N}$ sono in corrispondenza biunivoca:

$$\begin{array}{ccccccc} 0 & -1 & 1 & -2 & 2 & -3 & 3\cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & 3 & 4 & 5 & 6\cdots \end{array}$$

Le bigezioni illustrate si possono esprimere in maniera analitica: le frecce dall'alto verso il basso rappresentano la funzione $f : \mathbb{Z} \to \mathbb{N}$ definita da:

$$\forall n \in \mathbb{Z} \quad f(n) = \begin{cases} 2n & \text{se } n \geq 0 \\ -2n-1 & \text{se } n < 0. \end{cases}$$

Le frecce dal basso verso l'alto illustrano invece il modo in cui opera la funzione inversa $f^{-1} : \mathbb{Z} \to \mathbb{N}$ che è data da:

$$\forall k \in \mathbb{N} \quad f^{-1}(k) = \begin{cases} \frac{k}{2} & \text{se } k \text{ è pari} \\ -\frac{k+1}{2} & \text{se } k \text{ è dispari.} \end{cases}$$

AVVERTENZA SULLA NOTAZIONE RELATIVA ALL'INVERSA DI UNA FUNZIONE

Per una funzione bigettiva $f : A \to B$, il simbolo f^{-1} denota la funzione inversa; pertanto la scrittura $f^{-1}(b)$ denota l'immagine di b mediante tale funzione inversa.

La stessa notazione però viene anche utilizzata per denotare l'insieme $f^{-1}(b) \subset A$ delle preimmagini dello stesso b (ricordarsi che questa notazione è ammissibile anche se la funzione non è bigettiva).

Il legame tra le due cose è che l'insieme $f^{-1}(b)$ delle preimmagini ha un solo elemento, che è proprio l'immagine $f^{-1}(b)$ mediante f^{-1}. Ciò in simboli andrebbe scritto:

$$f^{-1}(b) = \{f^{-1}(b)\}$$

il che risulta corretta solo se intendiamo in modo diverso il significato dei simboli $f^{-1}(b)$ al primo e al secondo membro (insieme delle preimmagini al primo, immagine nel secondo).

Nella pratica, è di solito chiaro del contesto, oppure è a cura di chi usa tali simboli spiegarlo, a quale dei due significati di $f^{-1}(b)$ si sta facendo riferimento.

COMPOSIZIONE DI INGEZIONI E DI SURGEZIONI

Teorema: *Siano $f : A \to B$ e $g : B \to C$ applicazioni. Sussistono le seguenti proprietà:*

i) Se f e g sono ingettive, anche $g \circ f$ è ingettiva;

ii) Se f e g sono surgettive, anche $g \circ f$ è surgettiva;

iii) Se f e g sono bigettive, anche $g \circ f$ è bigettiva.

Dimostrazione: i) Supposto che f e g siano entrambe ingettive, siano $a, b \in A$ e supponiamo che

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

Vogliamo dedurne che $a = b$. Infatti, la relazione precedente implica che

$$g(f(a)) = g(f(b)).$$

Quindi, per l'ingettività di g otteniamo che

$$f(a) = f(b)$$

ed utilizzando l'ingettività di f segue

$$a = b.$$

Poichè ciò vale per arbitrari elementi a, b di A, resta verificato che $g \circ f$ è ingettiva.
ii) Supposto che f e g siano entrambe surgettive, si vuol provare che per ogni $c \in C$ esiste $a \in A$ tale che

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

Sia quindi $c \in C$ un elemento qualsiasi. Poichè g è surgettiva, esiste $b \in B$ tale che

$$g(b) = c.$$

Ora, $b \in B$ e anche f è surgettiva, per cui esiste $a \in A$ tale che

$$f(a) = b.$$

Allora

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

e quindi l'asserto.
iii) Stante la definizione di bigezione, iii) è un'applicazione immediata delle i) e ii) appena provate.

L'INVERSA DI UNA BIGEZIONE COMPOSTA

Proposizione: *Se $f : A \to B$ e $g : B \to C$ sono bigezioni, allora l'inversa di $g \circ f$ è data da:*

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

Dimostrazione: Intanto la questione ha senso perchè sappiamo che $g \circ f$ è bigettiva. Notiamo poi che la composizione $f^{-1} \circ g^{-1}$ è ben definita perchè $g^{-1} : C \to B$, mentre $f^{-1} : B \to C$, dunque l'insieme di arrivo di g^{-1} coincide con l'insieme di partenza di f^{-1} (la situazione è la stessa a quella relativa alle funzioni originarie). Dunque la funzione composta è rappresentata dal diagramma

$$C \xrightarrow{g^{-1}} B \xrightarrow{f^{-1}} A$$

Inoltre essa è una funzione da C in A, come previsto per $(g \circ f)^{-1}$. Sappiamo che per controllare che la funzione in questione è proprio l'inversa di $g \circ f$, basta controllare che, per ogni $c \in C$ si abbia:

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

perchè l'inversa in questione deve associare ad ogni $c \in C$ la propria preimmagine mediante $g \circ f$ nell'insieme A.

Per effettuare questa verifica, cominciamo applicando allo stesso modo la definizione di inversa sia per f che per g; abbiamo quindi:

$$f(f^{-1}(b)) = b, \qquad g(g^{-1}(c)) = c$$

per ogni $b \in B$ e per ogni $c \in C$.

Usando queste informazioni, otteniamo dunque:

$$(g \circ f)((f^{-1} \circ g^{-1})(c)) = (g \circ f)(f^{-1}(g^{-1}(c))) = g(f(f^{-1}(g^{-1}(c)))) = g(g^{-1}(c)) = c.$$

L'APPLICAZIONE IDENTICA

Def: Sia A un isneme. Si chiama applicazione identica di A o identità di A (o anche su A), l'applicazione

$$Id_A : A \to A$$

definita ponendo

$$\forall a \in \quad Id_A(a) = a.$$

Intuitivamente tale funzione opera sull'insieme A ma senza "alterarlo" in alcun modo. Lo stesso accade se la si compone con altre funzioni:

Proposizione: *Sia $f : A \to B$ un'applicazione. Allora risulta*

$$f \circ Id_A = f, \quad id_B \circ f = f.$$

Dimostrazione: Per ogni $a \in A$ abbiamo infatti

$$(f \circ id_A)(a) = f(Id_A(a)) = f(a)$$

e

$$(id_B \circ f)(a) = Id_B(f(a)) = f(a).$$

Si osservi che l'ultima uguaglianza è dovuta al fatto che $f(a)$ è sempre un elemento di B.

Utilizzando il concetto di funzione identica, l'inversa di una bigezione si può utilmente caratterizzare mediante il risultato seguente:

Prop: *Sia $f : A \to B$ una bigezione. L'inversa $f^{-1} : B \to A$ è l'unica applicazione da B in A che soddisfa la condizione seguente:*

$$f \circ f^{-1} = Id_B.$$

Dimostrazione: si ricordi che f^{-1} associa a ogni $b \in B$ la sua unica preimmagine in A, il che si tramuta in

$$f(f^{-1}(b)) = b$$

per ogni $b \in B$. Essa è quindi l'unica funzione da B in A per cui è vero questo per ogni $b \in B$. Ma tale proprietà si può reinterpretare come

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

per ogni $b \in B$ e questo significa che $f \circ f^{-1} : B \to B$ è la funzione identica Id_B.

Osservazione: Si noti che per una bigezione $f : A \to B$ vale anche:

$$f^{-1} \circ f = Id_A.$$

Ciò perchè anche f^{-1} è bigettiva e la sua inversa è f. Quindi basta applicare il risultato di prima con f^{-1} che svolge il ruolo di f.

INSIEMI FINITI E INFINITI

La discussione che segue mira a spiegare l'utilità del concetto di bigezione nell'ambito della trattazione di concetti fondazionali importanti: introdurremo una definizione rigorosa dei termini "infinito", "finito", "numerosità" di un insieme, e cosa significa che due insiemi hanno "lo stesso numero di elementi".

Si deve al grande matematico G. Cantor la formalizzazione e lo sviluppo sistematico e coerente dell'idea che tutti questi concetti si fondano sulla nozione di bigezione.

Def: Un insieme A si dice **finito** se $A = \emptyset$ oppure esiste una bigezione

$$f : A \to \{1, 2, \ldots, n\},$$

dove $n \geq \mathbb{N}$ è un intero naturale, $n \geq 1$.

Qui $\{1, 2, \ldots, n\}$ denota l'insieme di tutti i numerali naturali compresi tra 1 e n (se $n = 1$ si tratta dell'insieme $\{1\}$.)

Questa definizione poggia la sua motivazione sull'esperienza naturale del contare, con la quale tutti hanno confidenza sin dalla più tenera età. Assegnare una bigezione $f : A \to \{1, 2, \ldots, n\}$ significa in effetti associare un'etichetta diversa per ogni elemento dell'insieme, esaurendo tutti gli elementi di A e utilizzando tutti i numeri da 1 a n.

Con questo approccio, si considerano come modello di insieme finito gli insiemi del tipo $\{1, \ldots, n\} \subset \mathbb{N}$ e tutti gli altri insiemi finiti sono quelli che si ottengono come "copie" di tali modelli, cioè insiemi in corrispondenza biunivoca con uno di essi.

Def: Un insieme si dice **infinito** se non è finito.

INSIEMI EQIPOTENTI
INSIEMI NUMERABILI

Def: Due insiemi A e B si dicono **equipotenti** se esiste almeno una bigezione $f : A \to B$.

Si osservi che tale condizione prescinde dall'ordine in cui consideriamo gli insiemi, in virtù dell'esistenza dell'inversa di una bigezione.

Nota importante: Se A e B sono insiemi equipotenti e C è equipotente a B, allora anche A e C sono equipotenti.

Ciò è dovuto al fatto che la composizione di bigezioni è ancora una bigezione: se A e B sono equipotenti, esiste una bigezione $f : A \to B$; analogamente, se B e C lo sono, vi è almeno una bigezione $g : B \to C$. Allora $g \circ f : A \to C$ è una bigezione, il che mostra che A e C sono equiponenti.

Nota: Dunque un insieme finito è un insieme equipotente a qualche insieme del tipo $\{1, 2, \ldots, n\}$.

Il confronto tra insiemi mediante la nozione appena introdotta è un argomento importante e vasto che non discuteremo in dettaglio in questo corso. Nell'affrontare il problema di classificazione degli insiemi infiniti, la prima tipologia fondamentale si ottiene dal confronto con l'insieme $\mathbb{N}$, sul cui "terreno" avviene la più basilare esperienza del formarsi dell'idea stessa di infinito nella mente umana.
A questo proposito si introduce la seguente terminologia:

Def: Un insieme A si dice *numerabile* se è equipotente a $\mathbb{N}$.

Avvertenza: Il fatto stesso che $\mathbb{N}$ è infinito necessita di una dimostrazione, perchè si tratta di controllare se esso soddisfa la condizione richiesta (di non essere finito, ovvero di non essere equipotente a nessuno dei suoi sottoinsiemi $\{1, \ldots, n\}$, $n \geq 1$). Torneremo su questo punto nei prossimi paragrafi.

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

Dimostrazione: abbiamo già esibito un esempio di bigezione $f : \mathbb{Z} \to \mathbb{N}$.

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

Discuteremo la dimostrazione in un paragrafo successivo.

Il seguente risultato è di fondamentale importanza perchè mostra che vi è una tipologia di infinito diversa da quella di $\mathbb{N}$:

Teorema (Cantor): *L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.*

CARDINALITÀ DI UN INSIEME FINITO

Def: Sia A un insieme finito; se A è equipotente a $\{1, \ldots, n\}$, $n \geq 1$, l'intero n si chiama la **cardinalità** di A. Tale numero si denota con

$$|A|.$$

La cardinalità si chiama anche **il numero di elementi dell'insieme** finito A.

Nota: Nel caso dell'insieme vuoto $\emptyset$, che è finito per definizione, si pone $|\emptyset| := 0$.

Questa definizione è ragionevole, ma nasconde un problema: affinchè essa sia ben posta, occorre che la cardinalità sia univocamente determinata; a priori infatti, non è escluso che A possa essere equipotente sia a $\{1, \ldots, n\}$ che a $\{1, \ldots, m\}$ in corrispondenza di due interi diversi n e m. In tal caso non sarebbe per nulla chiaro qual è il numero di elementi di A!

La questione è risolta dal seguente risultato (intuitivamente e apparentemente ovvio):

Teorema: *Siano $n, m \in \mathbb{N} - \{0\}$ due numeri naturali non nulli, $n \neq m$. Allora gli insiemi $\{1, \ldots, n\}$ e $\{1, \ldots, m\}$ non sono equipotenti.*

Discuteremo questo teorema in un paragrafo successivo, in quanto risulta strettamente legato ad alcuni principi generali che sono alla base della struttura dell'insieme dei numeri naturali.

SUCCESSIONI E INSIEMI NUMERABILI

Def: Dato un insieme A, si chiama **successione di elementi di** A oppure **successione a valori in** A ogni applicazione

$$x : \mathbb{N} \to A.$$

Per ogni $n \in \mathbb{N}$, l'immagine $x(n)$ si denota più spesso con il simbolo

$$x_n.$$

Così, ad esempio data la successione

$$x : \mathbb{N} \to \mathbb{Q}$$
$$x(n) = \frac{n+1}{2},$$

allora $x_0 = x(0) = \frac{1}{2}$, $x_6 = \frac{7}{2}$, $x_9 = 5$.

Se A è un insieme numerabile, per definizione esiste almeno una bigezione $f : A \to \mathbb{N}$, che permette di enumerare gli elementi di A, ma anche un'applicazione bigettiva $x : \mathbb{N} \to A$, ovvero una successione bigettiva; essa permette quindi di "organizzare" gli elementi di A in una sequenza:

$$x_0,\ x_1,\ \cdots, x_n, x_{n+1}, \cdots$$

nella quale compaiono **tutti** gli elementi dell'insieme A, **senza ripetizioni** (ogni elemento figura una ed una sola volta come un certo x_n). Molto spesso per mostrare che un insieme è numerabile si cerca di esibire una tale sequenza.

Esempi: Considerato l'insieme P dei numeri naturali pari, la successione

$$x : \mathbb{N} \to P$$

$$x(n) := 2n$$

è bigettiva.
Infatti, x è ingettiva perchè se $x(n) = x(m)$, allora $2m = 2n$, e quindi $n = m$. Inoltre x è surgettiva perchè ogni numero pari p è del tipo $p = 2n = x(n)$, ovvero ammette sempre una preimmagine in $\mathbb{N}$ mediante x.

Ciò mostra che P è numerabile. Abbiamo costruito la successione:

$$0,\ 2,\ 4,\ 6,\ \cdots$$

dove

$$x_0 = 0,\ x_1 = 2,\ x_3 = 6, \cdots$$

In tale sequenza, tutti i numeri pari compaiono una ed una sola volta.

Allo stesso modo, l'insieme D dei numeri naturali dispari è numerabile e ciò si può verificare considerando la successione:

$$x : \mathbb{N} \to D$$

$$x(n) := 2n + 1.$$

Anche tale successione è bigettiva.

Es: Un altro esempio di sottoinsieme di $\mathbb{N}$ che è numerabile è $\mathbb{N}^* := \mathbb{N} - \{0\}$ (numeri naturali diversi da 0). La successione

$$x : \mathbb{N} \to \mathbb{N}^*$$

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

è infatti un'applicazione bigettiva.
Per controllarlo, si osservi che ogni $m \in \mathbb{N}^*$ ha una sola preimmagine $n \in \mathbb{N}$, in quanto l'equazione

$$x(n) = m$$

ovvero

$$n + 1 = m$$

ammette l'unica soluzione

$$n = m - 1$$

che è un numero intero non negativo perchè $m \geq 1$. Dunque $m - 1$ è l'unica preimmagine di m mediante x.

ULTERIORI ESEMPI SUL CONCETTO DI EQUIPOTENZA

Ricordiamo che due insiemi A e B si dicono **disgiunti** se $A \cap B = \emptyset$.

Esempio: Siano A e B insiemi disgiunti, equpotenti rispettivamente agli insiemi A' e B' e si supponga che anche A' e B' siano disgiunti. Allora si ha che:

$$A \cup B \text{ è quipotente a } A' \cup B'.$$

Per mostrarlo, supponiamo che $f : A \to A'$ e $g : B \to B'$ siano due bigezioni. A partire da esse, possiamo costruire una bigezione

$$h : A \cup B \to A' \cup B'$$

in questo modo:

$$h(x) := \begin{cases} f(x) & \text{se } x \in A \\ g(x) & \text{se } x \in B. \end{cases}$$

Attenzione: questa funzione **è** ben definita, perchè ogni oggetto x nell'unione $A \cup B$ può appartenere o soltanto ad A oppure soltanto a B; pertanto l'immagine $h(x)$ viene assegnata senza ambiguità, utilizzando o l'applicazione f oppure la g a seconda del caso.

h è ingettiva: se x e x' sono in $A \cup B$, con $x \neq x'$, allora si ha sempre $h(x) \neq h(x')$, perchè vi sono le seguenti possibilità:

x e x' entrambi in A: basta tener conto dell'ingettività di f;

x e x' entrambi in B: basta tener conto dell'ingettività di g;

$x \in A$ e $x' \in B$: abbiamo $h(x) = f(x)$ e $h(x') = g(x')$, ma tali oggetti $f(x)$ e $g(x')$ sono rispettivamente in A' e in B', che sono insiemi disgiunti, per cui certamente $f(x) \neq g(x')$. Dunque $h(x) \neq h(x')$.

Analogo discorso se $x \in B$ e $x' \in A$.

Surgettività: ogni $y \in A' \cup B'$ ha sempre una preimmagine, perchè se y appartiene ad A', allora esso possiede la sua preimmagine x in A mediante f, che soddisfa anche $h(x) = y$, mentre se appartiene a B', allora la sua preimmagine x mediante g svolge anche il ruolo di preimmagine di y mediante h.

Es: La bigezione $h : \mathbb{Z} \to \mathbb{N}$ che abbiamo discusso in precedenza:

$$\forall n \in \mathbb{Z} \quad h(n) = \begin{cases} 2n & \text{se } n \geq 0 \\ -2n - 1 & \text{se } n < 0. \end{cases}$$

risulta costruita in effetti con il criterio che abbiamo appena discusso, laddove si consideri $\mathbb{Z}$ come unione di $A = \{x \in \mathbb{Z} | x \geq 0\}$, $B = \{x \in \mathbb{Z} |\, x < 0\}$ e $\mathbb{N}$ come unione di $A' = P$ (numeri pari) e $B' = D$ (numeri dispari). Le due bigezioni che vengono "incollate" per costruire la nostra funzione h sono:

$$f : A \to A',\ f(x) := 2x,\ \ g : B \to B',\ g(x) := -2x - 1.$$

Esempio: L'unione $A \cup B$ di due insiemi numerabili disgiunti è numerabile.

Infatti, A è equipotente a $\mathbb{N}$, ma allora è anche equipotente a P, l'insieme dei numeri naturali pari, perchè sappiamo che anche P è equipotente a $\mathbb{N}$. Per lo stesso motivo, B è equipotente a D, l'inieme dei numeri naturali dispari.
Applicando il principio stabilito sopra, che è utilizzabile in quanto P e D sono disgiunti, consegue che $A \cup B$ è equipotente a $P \cup D = \mathbb{N}$. Quindi anche $A \cup B$ è numerabile.

Esempio: Se A è numerabile e x è un qualsiasi oggetto non appartenente ad A, allora anche $A \cup \{x\}$ è numerabile.

Per giustificare ciò, ragionando come sopra abbiamo che A risulta equipotente a $\mathbb{N}^* = \mathbb{N} - \{0\}$, perchè sappiamo che $\mathbb{N}^*$ è anch'esso numerabile. D'altra partè è chiaro che $\{x\}$ è equipotente a $\{0\}$ (l'unica funzione possibile $f : \{x\} \to \{0\}$ è quella definita ponendo $f(x) := 0$, che è bigettiva!).

Quindi usando ancora lo stesso principio sfruttato in precedenza, è lecito concludere che $A \cup \{x\}$ è equipotente a $\mathbb{N}^* \cup \{0\} = \mathbb{N}$, ovvero che $A \cup \{x\}$ è ancora numerabile.

Nota: In effetti, valgono risultati ben più forti: l'unione di due insiemi numerabili è sempre numerabile, anche se non sono disgiunti; questo si può estendere all'unione di un numero finito di insiemi numerabili, e addirittura all'unione di una successione:

$$A_1, \ldots, A_n, A_{n+1}, \ldots,$$

di insiemi numerabili. Ciò significa che si può dimostrare che l'unione di tutti gli insiemi in questione:

$$A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1} \cdots$$

che è l'insieme costituito da tutti e solo gli oggetti che stanno almeno in un A_n, risulta ancora numerabile. Non entreremo nel merito di questo tipo di risultati.

TOGLIERE UN ELEMENTO DA UN INSIEME FINITO

Abbiamo visto che togliendo ad $\mathbb{N}$ un oggetto oppure aggiungendo un elemento in più, non si altera la sua "numerosità", nel senso che l'insieme che si ottiene resta equipotente all'originale.

Ciò è falso per insiemi finiti, in accordo con la nostra quotidiana pratica del contare:

Esempio: Per ogni $n \in \mathbb{N}$, $n \geq 1$, risulta che:

$$\{1, 2, \ldots, n+1\} - \{y\} \text{ è equipotente a } \{1, 2, \ldots, n\},$$
$$\text{per ogni fissato numero } y \in \{1, 2, \ldots, n+1\}.$$

Una bigezione tra $\{1, 2, \ldots, n+1\} - \{y\}$ e $\{1, 2, \ldots, n\}$ si può agevolmente costruire come segue; definiamo

$$f : \{1, 2, \ldots, n+1\} - \{y\} \to \{1, 2, \ldots, n\}$$

ponendo

$$f(x) := \begin{cases} x & \text{se } 1 \leq x < j \\ x - 1 & \text{se } j < x \leq n+1. \end{cases} .$$

Ad esempio, se $n = 5$ e $y = 4$, allora abbiamo la bigezione

$$f : \{1, 2, 3, 5, 6\} \to \{1, 2, 3, 4, 5\}$$

$$1 \mapsto 1,\ 2 \mapsto 2, 3 \mapsto 3, 5 \mapsto 4, 6 \mapsto 5.$$

Come abbiamo detto in precedenza, risulta che gli insiemi $\{1, 2, \ldots, n+1\}$ e $\{1, 2, \ldots, n\}$ non sono equipotenti ($n \neq n+1$), dunque $\{1, 2 \ldots, n+1\}$ si comporta in modo ben diverso da $\mathbb{N}$, per quel che riguarda l'operazione di toglierne un oggetto.

Questo semplice esempio mostra in modo rigoroso che togliere un elemento da un insieme finito comporta diminuirne di un'unità la cardinalità.

NUMERABILITÀ DI $\mathbb{Q}$

Come applicazione di quanto visto finora, discutiamo la dimostrazione del fatto che $\mathbb{Q}$ è numerabile. Cominciamo con il caso più semplice dell'insieme:

$$A = \{q \in \mathbb{Q} |\, 0 < q < 1\}.$$

Si tratta di stabilire che è possibile costruire una successione

$$x_0, x_1, \ldots, x_n, \cdots$$

i cui elementi sono tutti gli elementi di A, senza ripetizioni.

Ricordiamo intanto che ogni numero razionale positivo ammette un'unica rappresentazione come frazione $q = \frac{m}{n}$ ridotta **ai minimi termini**; ciò significa che il numeratore m ed il denominore n sono interi naturali che non hanno divisori comuni (eccetto 1). Ad esempio, $\frac{3}{5}$ è una frazione ridotta ai minimi termini, mentre $\frac{4}{6}$ no; lo stesso numero però è uguale alla frazione $\frac{2}{3}$, che invece lo è.

Ciò premesso, notiamo che se $q = \frac{m}{n} < 1$, allora $m < n$. Ciò implica che le frazioni minori di 1, con denominatore fissato uguale a n sono soltanto le seguenti:

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}.$$

Di queste, quelle ridotte ai minimi termini sono al più $n-1$. Ad esempio, se $n = 5$ si tratta delle frazioni

$$\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5},$$

tutte ridotte ai minimi termini, mentre se consideriamo quelle con denominatore $n = 6$, abbiamo

$$\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}$$

di cui quelle ridotte ai minimi termini sono:

$$\frac{1}{6}, \frac{5}{6}.$$

Dunque possiamo scrivere tutti gli elementi di A come una successione senza ripetizioni, ordinando tutte le frazioni ridotte ai minimi termini rispetto al denominatore (scriviamo prima quelle con denominatore 2, poi quelle con denominatore 3, poi con denominatore 4, ecc); quelle con lo stesso denominatore vengono scritte in ordine crescente rispetto al numeratore:

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \frac{5}{6}, \frac{1}{7}, \frac{2}{7}, \frac{3}{7}, \frac{4}{7}, \frac{5}{7}, \frac{6}{7}, \cdots$$

Questa argomentazione mostra che A è numerabile.

Cerchiamo ora di migliore il risultato e provare che $\mathbb{Q}$ è numerabile.
L'insieme B dei numeri razionali maggiori di 1:

$$B = \{q \in \mathbb{Q} | \, q > 1\}$$

è equipotente all'insieme A già studiato: basta utilizzare l'osservazione che $q < 1$ se e solo se $\frac{1}{q} > 1$. Ciò permette di definire l'applicazione:

$$x \in A \mapsto \frac{1}{x} \in B$$

che è una bigezione. Pertanto anche B è numerabile, e tale è l'unione di A e B:

$$A \cup B = \{q \in \mathbb{Q} | \, q > 0, \, q \neq 1\}.$$

A tale insieme possiamo poi aggiungere 1, formando un altro insieme numerabile che è semplicemente:

$$\mathbb{Q}^+ := \{q \in \mathbb{Q} | \, q > 0\},$$

cioè l'insieme dei razionali positivi.
Siamo arrivati alla conclusione che $\mathbb{Q}^+$ è numerabile.

Infine, anche l'insieme dei numeri negativi $\mathbb{Q}^- = \{q \in \mathbb{Q} | \, q < 0\}$ è numerabile perchè equipotente a $\mathbb{Q}^+$. Infatti l'applicazione

$$x \in \mathbb{Q}^- \mapsto -x \in \mathbb{Q}^+$$

è bigettiva.

Conclusione: $\mathbb{Q}^* - \{0\} = \mathbb{Q}^- \cup \mathbb{Q}^+$ è numerabile e possiamo finalmente concludere che tale è $\mathbb{Q} = \mathbb{Q}^* \cup \{0\}$.

IL PRINCIPIO DEI CASSETTI

Torniamo alla questione relativa alla definizione della cardinalità di un insieme finito. Abbiamo già enunciato il risultato che garantisce che la cardinalità è univocamente determinata:

Teorema: *Siano* $n, m \in \mathbb{N} - \{0\}$ *due numeri naturali non nulli,* $n \neq m$*. Allora gli insiemi* $\{1, \ldots, n\}$ *e* $\{1, \ldots, m\}$ *non sono equipotenti.*

In realtà vale un risultato più forte, che è il cosiddetto **principio dei cassetti**:

se dobbiamo riporre delle camicie in una cassettiera, e ci sono più camicie che cassetti, almeno due camicie vanno a finire nello stesso cassetto.

In termini di numeri interi, questo principio si formula come segue. Conviene introdurre una notazione più comoda: per riferirci all' insieme $\{1, \ldots, n\}$, dove $n \in \mathbb{N}^*$, useremo il simbolo I_n. Quindi ad es. $I_1 = \{1\}$, $I_5 = \{1, 2, 3, 4, 5\}$.

Il principio dei cassetti è quindi il seguente:

Principio dei cassetti: *Se* $m, n \geq 1$ *sono due numeri naturali con* $m > n$*, non esiste alcuna applicazione ingettiva*

$$f : I_m \to I_n.$$

DISCUSSIONE SULLA DIMOSTRAZIONE DEL PRINCIPIO DEI CASSETTI

Ricordiamo cosa afferma il Principio dei Cassetti:

Principio dei Cassetti: *Se $m, n \geq 1$ sono due numeri naturali con $m > n$, non esiste alcuna applicazione ingettiva*

$$f : I_m \to I_n.$$

Questo risultato può apparire ovvio: per un'applicazione ingettiva $f : I_m \to I_n$ le immagini $f(1), \ldots, f(m)$ sarebbero esattamente m, pertanto più di n, ma in I_n non possono esservi più di n numeri.
Il problema in questa semplice argomentazione sta nell' ultima affermazione: implicitamente essa usa lo stesso principio dei cassetti!

Per capire quanto la questione sia sottile, risulta che il Principio dei Cassetti è equivalente a un altro Principio fondamentale che riguarda la struttura "intima" dell'insieme dei numeri naturali $\mathbb{N}$, che si chiama Principio del Minimo:

Principio del minimo (o del buon ordine): *Ogni sottoinsieme non vuoto A di $\mathbb{N}$ possiede un elemento mimimo a_o, cioè minore o uguale a tutti gli altri elementi di A:*

$$a_o \leq a \quad \forall a \in A.$$

Si osserva subito che tale a_o è univocamente determinato: dato un altro minimo $a'_o \in A$, dovrebbe aversi sia $a_o \leq a'_o$ che $a'_o \leq a_o$ e quindi $a_o = a'_o$.

Tale principio corrisponde all'idea intuitiva che ogni sottoinsieme di $\mathbb{N}$ ha un elemento "da cui inizia", così come l'intero $\mathbb{N}$ "inizia" da 0.
L'insieme più ampio dei numeri interi relativi non ha questa proprietà: ad esempio, dove inizierebbe il sottoinsieme $A = \{x \in \mathbb{Z} : x < 0\}$? Analogamente per l'insieme $\{x \in \mathbb{Q} | x > 0\}$ in $\mathbb{Q}$.

Tale principio è a sua volta è equivalente al cosiddetto Principio di Induzione:

Principio di induzione: *L'unico sottoinsieme di $\mathbb{N}$ che contiene 0 e che contiene, per ogni suo elemento n, anche il numero successivo $n + 1$, è $\mathbb{N}$ stesso.*

L'equivalenza tra tutti questi enunciati mostra che stabilire la validità del Principio dei Cassetti ha a che fare con il problema di chiarire il concetto stesso di "numero", cosa del tutto non banale e risolta dall'assiomatizzazione di Peano dell'insieme dei numeri naturali. In essa si assume proprio il Principio di Induzione come uno degli **assiomi** della teoria dei numeri. D'ora in poi assumeremo il principio di induzione, che fornisce un potente strumento dimostrativo per provare affermazioni in cui siano coinvolti i numeri naturali.

L'INDUZIONE COME TECNICA DIMOSTRATIVA

Il principio di induzione fornisce un metodo per dimostrare che una certa affermazione $P(n)$, formulata in termini di numeri naturali, e che può essere a priori vera o falsa assegnato un numero intero n, è **vera per tutti** i numeri naturali.

Vale infatti quanto segue:

Sia $P(n)$ un enunciato che ha senso per tutti i numeri naturali $n \in \mathbb{N}$. Si ammetta che sono soddisfatte le condizioni seguenti:

i) $P(0)$ è vera;
ii) Per ogni $n \geq 0$, se $P(n)$ è vero, anche $P(n+1)$ è vero.

Allora si può concludere che $P(n)$ è vero per tutti i numeri $n \in \mathbb{N}$.

La seconda condizione *ii)* si scrive in modo più formale come segue:

ii) $\forall n \in \mathbb{N} : \; P(n) \; \Rightarrow \; P(n+1)$.

La giustificazione di questa affermazione risiede in un'immediata applicazione del Principio di Induzione: basta fissare l'attenzione sull'insieme

$$A = \{n \in \mathbb{N} | \, P(n) \text{ è vero } \} = \{n \in \mathbb{N} | \; P(n)\}.$$

La condizione i) garantisce che $0 \in A$, mentre la ii) che, per ogni $n \in A$, anche il numero successivo $n+1$ appartiene ad A. Il principio di induzione garantisce che

$$A = \mathbb{N},$$

e ciò significa proprio che l'enunciato $P(n)$ è vero per ogni $n \in \mathbb{N}$.

Nella pratica quindi, per provare che $P(n)$ è vera per tutti gli interi naturali, si procede così:

1) Passo base: si verifica che la proprietà dimostrare è vera per $n = 0$;

2) Passo induttivo: si suppone che $P(n)$ sia vera per $n \geq 0$ e si prova, utilizzando tale ipotesi, che anche $P(n+1)$ è vera.

Esempio: Proviamo che per ogni $n \in \mathbb{N}$ si ha:

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

La proprietà in questione è

$$P(n) : \sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Procediamo per induzione.

Passo base: $P(0)$ è vera perchè sostituendo $n = 0$ ad ambo i membri si ottiene l'uguaglianza

$$0 = 0$$

che è vera!

Passo induttivo: Dato $n \geq 0$, supponiamo per ipotesi $P(n)$ e da ciò deduciamo come tesi $P(n+1)$.

IPOTESI: $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

TESI: $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$.

Per provare la tesi, partiamo dal primo membro dell'uguaglianza da provare:

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Il primo passaggio serve per poter sfruttare l'ipotesi induttiva, cosa che avviene nel passaggio successivo sostituendo alla quantità $\sum_{i=0}^{n} i$ il suo valore noto per ipotesi, ovvero $\frac{n(n+1)}{2}$.

Il metodo di dimostrazione per induzione si può applicare anche nella situazione più generale in cui siamo interessati a provare che un certo enunciato $P(n)$ è vero per tutti gli interi $n \geq n_0$ più grandi di un intero fissato n_0.

Sia $P(n)$ un enunciato che ha senso per tutti i numeri naturali maggiori o uguali ad un certo $n_o \in \mathbb{N}$. Se sono soddisfatte le condizioni seguenti:

i) $P(n_o)$ è vero;
ii) Per ogni $n \geq n_o$, se $P(n)$ è vero, anche $P(n+1)$ è vero,

allora $P(n)$ è vero per tutti gli interi $n \geq n_o$.

In questo caso, per giustificarlo, basta applicare il Principio di Induzione all'insieme:

$$A = \{0, \ldots, n_0 - 1\} \cup \{n \in \mathbb{N} |\, n \geq n_0 \text{ e } P(n) \text{ è vera } \}.$$

Esempio: Proviamo per induzione che per ogni $n \in \mathbb{N}$, $n \geq 5$ si ha:

$$n^2 \geq 11n - 30.$$

Abbiamo:

$$P(n) : n^2 \geq 11n - 30.$$

Passo base: $P(5)$ è vera perchè sostituendo $n = 5$ ad ambo i membri si ottiene

$$25 \geq 55 - 30$$

ovvero

$$25 \geq 25$$

che certamente è un'affermazione vera.

Passo induttivo: Dato $n \geq 5$, supponiamo per ipotesi vera $P(n)$ e da ciò deduciamo che $P(n+1)$ è vera.

IPOTESI: $n^2 \geq 11n - 30$.

TESI: $(n+1)^2 \geq 11(n+1) - 30$.

Possiamo riscrivere i due enunciati in modo più comodo come segue:

IPOTESI: $n^2 - 11n + 30 \geq 0$.
TESI: $(n+1)^2 - 11(n+1) + 30 \geq 0$.

Procediamo a provare la tesi partendo dal primo membro della disuguaglianza da provare:

$$(n+1)^2-11(n+1)+30 = n^2+2n+1-11(n+1)+30 = n^2-11n+30+2n+1-11 =$$

$$= n^2 - 11n + 30 + 2n - 10 \geq 0.$$

Dopo aver sviluppato $(n+1)^2$, nel passaggio successivo gli addendi sono stati riordinati in modo da far comparire prima la quantità $n^2 - 11n + 30$ su cui abbiamo informazioni grazie all'ipotesi induttiva.

L'ultima disuguaglianza è giustificata da due cose: in primo luogo l'ipotesi induttiva che garantisce che $n^2 - 11n + 30 \geq 0$, e poi il fatto che $2n - 10 \geq 0$, cosa vera perchè stiamo assumendo $n \geq 5$; pertanto la quantità $n^2 - 11n + 30 + 2n - 10$ è somma di due interi entrambi maggiori o uguali a zero e quindi è essa stessa maggiore o uguale a 0.

RIFORMULAZIONE DEL PRINCIPIO DEI CASSETTI

Nel seguito intendiamo fare la dimostrazione del Principio dei Cassetti, usando l'induzione. Ricordiamo che si tratta dell'affermazione : se $m > n$, allora non esistono applicazioni ingettive $f : I_m \to I_n$.

Per prima cosa riformuliamo il problema, e notiamo che basta provare quanto segue:

Per ogni $n \geq 1$, non esiste alcuna applicazione ingettiva

$$f : I_{n+1} \to I_n.$$

Infatti, assumiamo vera tale affermazione e consideriamo due interi con $m > n \geq 1$. Allora $n + 1 \leq m$, e quindi

$$I_{n+1} \subset I_m.$$

Se esistesse un'applicazione ingettiva

$$f : I_m \to I_n$$

allora esisterebbe anche un'applicazione ingettiva:

$$g : I_{n+1} \to I_n,$$

definita semplicemente da

$$g(x) := f(x)$$

per ogni $x \in I_{n+1}$. Ma questo è contro la nostra assunzione.

Si rifletta sul fatto che l'ingettività di g è garantita dall'ingettività di f: elementi distinti di I_{n+1} hanno sempre immagini distinte, perchè tale immagini si calcolano sempre mediante la funzione iniziale f, e la tale proprietà di avere immagini distinte vale per due qualsiasi elementi distinti del dominio I_m, e quindi a maggior ragione per elementi del dominio I_{n+1} di g incluso in esso.

La funzione g che abbiamo usato in questa argomentazione si dice ottenuta da f *restringendo il dominio* da I_m al suo sottoinsieme I_{n+1}.

Questa tecnica è molto utile, per cui prima di procedere oltre, nel prossimo paragrafo esaminiamo più in generale l'operazione di restrizione di una funzione.

RESTRIZIONE DI UN'APPLICAZIONE

Def: Siano $f : A \to B$ un'applicazione e $X \subset A$ un sottoinsieme dell'insieme di partenza. Si chiama **restrizione di f a X** l'applicazione denotata con $f : X \to B$ che associa ad ogni $x \in X$ la sua immagine $f(x)$ mediante f.

N. B. Il fatto di usare lo stesso simbolo f per denotare la restrizione non crea confusione, perchè il dominio della nuova funzione è diverso.
Si tratta della relazione $\{(x, f(x))|x \in X\}$ da X in B, che è un sottoinsieme della relazione originaria f.

È evidente che l'immagine di tale restrizione è $f(X)$.

Osservazione importante: *ogni restrizione di un'applicazione ingettiva è anch'essa ingettiva.*
Attenzione: non vale una proprietà analoga se sostiuisce "ingettiva" con "surgettiva"!

Def: Più in generale, siano $X \subset A$ e $Y \subset B$, due sottoinsiemi tali che

$$f(X) \subset Y.$$

Ciò significa che tutte le immagini $f(x)$ di elementi di X vanno in Y.
Allora f determina naturalmente un'applicazione

$$f : X \to Y, \quad x \mapsto f(x)$$

che si chiama *indotta da* f.

Vale ancora che ogni applicazione indotta da un'ingezione è essa stessa un'ingezione.

Es: : Sia $f : \mathbb{Z} \to \mathbb{Z}$ definita da $f(x) = x+1$. Se P denota l'insieme dei numeri interi pari e D l'insieme degli interi dispari, allora è ben definita l'applicazione indotta

$$f : P \to D,$$

perchè $f(P) \subset D$, in quanto per ogni pari x, l'immagine $x + 1$ è dispari.

Ossrvazione utile: *Sia $f : A \to B$ un'applicazione ingettiva e sia $x \in A$. Allora f induce sempre un'applicazione ingettiva*

$$f : A - \{x\} \to B - \{f(x)\}.$$

Infatti, l'immagine di qualsiasi $a \in A$, diverso da x, è sempre diversa da $f(x)$, per l'ingettività. In formule: $f(A - \{x\}) \subset B - \{f(x)\}$. Pertanto l'applicazione indotta è ben definita in accordo con il principio generale.

Come ulteriore esemplificazione della tecnica di costruire mediante restrizione ingezioni a partire da altre ingezioni, proviamo, usando il Principio dei Cassetti, che $\mathbb{N}$ è infinito:

Teorema: $\mathbb{N}$ *è infinito.*

Dimostrazione: supponiamo per assurdo che $\mathbb{N}$ sia finito; in tal caso esisterebbe una bigezione

$$f : \mathbb{N} \to I_n,$$

per qualche $n \in \mathbb{N} - \{0\}$. Consideriamo la seguente restrizione di f:

$$f : I_{n+1} \to I_n.$$

Tale funzione è ancora è ingettiva, ma questo è impossibile, perchè contraddice il Principio dei Cassetti.

Per completare il quadro resta ancora da provare il Principio dei Cassetti! Lo facciamo nel paragrafo seguente.

DIMOSTRAZIONE DEL PRINCIPIO DEI CASSETTI

In base alla discussione fatta in precedenza, dobbiamo provare in definitiva che:

$$\forall n \in \mathbb{N}\text{: } \textit{non esistono funzioni ingettive } f : I_{n+1} \to I_n.$$

Procederemo per induzione.

Passo base. Per $n = 0$ la proprietà da provare è che non esistono funzioni ingettive

$$f : I_2 \to I_1.$$

Ciò è vero perchè in realtà l'unica funzione

$$f : \{1, 2\} \to \{1\}$$

è quella costante, tale che:

$$f(1) = 2, \quad f(2) = 1.$$

Essa ovviamente non è ingettiva.

Passo induttivo. Assegnato un intero $n \geq 0$, mostriamo che, se l'affermazione è vera per n, allora è vera anche per $n + 1$. Dunque assumiamo come ipotesi che non esistano funzioni ingettive $f : I_{n+1} \to I_n$, e deduciamo che non esistono funzioni ingettive $f : I_{n+2} \to I_{n+1}$. Supponiamo per assurdo che vi sia almeno un'ingezione

$$f : I_{n+2} \to I_{n+1}.$$

Allora essa indurrebbe, un'altra ingezione:

$$f : I_{n+2} - \{n + 2\} \to I_{n+1} - \{f(n + 2)\}.$$

Ma $I_{n+2} - \{n + 2\} = I_{n+1}$, quindi avremmo un'ingezione

$$f : I_{n+1} \to I_{n+1} - \{y\}$$

dove abbiamo posto $y = f(n + 2)$.
Sappiamo però che l'insieme $I_{n+1} - \{y\}$ è equipotente a I_n. Fissata allora una bigezione

$$g : I_{n+1} - \{y\} \to I_n,$$

la funzione composta:

$$I_{n+1} \xrightarrow{f} I_{n+1} - \{y\} \xrightarrow{g} I_n$$

sarebbe una applicazione ingettiva $g \circ f : I_{n+1} \to I_n$, il che è contro l'ipotesi induttiva.

L'EQUIVALENZA TRA PRINCIPIO DEL MINIMO E PRINCIPIO DEI CASSETTI

Nei prossimi due paragrafi, inclusi per completezza e per stimolare l'interesse in questo tipo di questioni, non inclusi nel programma d'esame, discutiamo l'equivalenza tra il Principio dei Cassetti e il Principio del Minimo, dimostrando che ciascuno implica l'altro. Tale dimostrazione è diretta, non fa uso dell'induzione.

Teorema: *Il Principio del Minimo implica il Principio dei Cassetti.*

Assumendo il Principio dei cassetti, consideriamo l'insieme A di tutti e soli i numeri $n \geq 1$ per cui esiste un'applicazione ingettiva $f : I_{n+1} \to I_n$. Osserviamo che $1 \notin A$ perchè l'unica applicazione

$$f : \{1, 2\} \to \{1\}$$

non è ingettiva.

Vogliamo provare che in effetti $A = \emptyset$. Ragioniamo per assurdo, supponendo che $A \neq \emptyset$ e consideriamo il minimo n_o di A. Dunque $n_o > 1$. Fissiamo un'applicazione ingettiva

$$f : I_{n_o+1} \to I_{n_o}.$$

Posto $y = f(n_0 + 1)$, essa induce un'applicazione ingettiva

$$f : I_{n_o+1} - \{n_o + 1\} \to I_{n_o} - \{y\}.$$

Poichè $I_{n_o+1} - \{n_o + 1\} = I_{n_o}$ e l'insieme $I_{n_o} - \{y\}$ è equipotente a I_{n_o-1} ne consegue che esiste anche un'applicazione ingettiva

$$g : I_{n_o} \to I_{n_o-1}$$

il che significa che anche $n_o - 1$ appartiene ad A. Si tratta di una contraddizione, perchè n_o è il minimo di A. Questa contraddizione conclude la dimostrazione.

Si noti l'analogia di questa argomentazione con quella che abbiamo usato per dimostrare il Principio dei Cassetti usando l'induzione.

Teorema: *Il Principio dei Cassetti implica il Principio del Minimo.*

Bisogna provare che ogni $A \subset \mathbb{N}$ non vuoto è dotato di minimo; poichè ciò è banale se $A = \{0\}$, supporremo sempre che A contenga qualche numero positivo.
Mostriamo innanzitutto che è sufficiente provare ciò per ogni sottoinsieme A che è contenuto in qualche I_n.
Infatti, sia $n > 0$ in A; allora l'insieme $A' := A \cap I_n$ è non vuoto e contenuto in I_n; sia m il minimo di A'. Dunque $m \leq n$; per ogni $a \in A$ si deduce che $a \leq m$ se $a \leq n$, mentre se $a > n$ avremo

$$m \leq n < a.$$

Ciò prova che m è anche il minimo di A.

Ora, per provare che, dato ogni insieme $A \subset I_n$ non vuoto e non ridotto a $\{0\}$ è dotato di minimo, useremo il Principio dei Cassetti. Supponiamo per assurdo che A non ammetta minimo. Consideriamo l'applicazione

$$f : I_n \to I_n$$

definita come segue:

$$f(x) = \begin{cases} x & \text{se } x < a \text{ per ogni } a \in A \\ x - 1 & \text{altrimenti.} \end{cases}$$

Risulta che f è ingettiva: infatti, siano x e z due numeri tali che

$$f(x) = f(z).$$

Se abbiamo $f(x) = x$ e $f(z) = z$, segue direttamente $x = z$; analogamente se $f(x) = x - 1$, $f(z) = z - 1$ perchè si ottiene $x - 1 = z - 1$, da cui ancora $x = z$.
Resta il caso in cui $f(x) = x$ mentre $f(z) = z - 1$; in tal caso, per definizione, abbiamo che $x < a$ per ogni $a \in A$; d'altra parte $f(x) = f(z)$ implica che

$$x = z - 1$$

da cui

$$z = x + 1.$$

Stante l'informazione che abbiamo su x, da ciò si deduce che $z \leq a$ per ogni $a \in A$. Ma non può mai valere $z = a$ perchè altrimenti z sarebbe il minimo di A. Dunque z soddisfa anch'esso $z < a$ per ogni $a \in A$, e quindi $f(z) = z$, cioè $z - 1 = z$ e questo è assurdo.

Infine, notiamo che n non può appartenere all'immagine di f, perchè per ipotesi $A \subset I_n$. Dunque l'immagine $f(I_n)$ è contenuta in I_{n-1} ed f induce un'applicazione $f : I_n \to I_{n-1}$ ingettiva, contro il Principio dei Cassetti.

SAPER CONTARE: LA REGOLA DELLA SOMMA

Teorema: *Siano A e B insiemi finiti non vuoti e disgiunti. Allora $A \cup B$ è finito e si ha:*

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

Questo risultato è intuitivamente chiaro, basandoci sempre sull'esperienza naturale del contare. Per dimostrarlo in modo rigoroso, posto $|A| = n$ e $|B| = m$, abbiamo che A è equipotente a I_n, mentre B è equipotente a I_m.Vogliamo provare che $A \cup B$ è equipotente a I_{m+n}.

Osserviamo che $I_m = \{1, \ldots, m\}$ è anche equipotente a

$$\{n+1, n+2, \ldots, m+n\};$$

tale insieme è ottenuto aggiungendo n a ciascun numero di I_m; tra i due insiemi si può considerare quindi la bigezione

$$g : I_m \to \{n+1, n+2, \ldots, m+n\}$$

$$g(x) := x + n.$$

Dunque B è anche equipotente a questo insieme $\{n+1, n+2, \ldots, m+n\}$ e poichè esso è disgiunto da I_n, possiamo concludere, usando un principio ai noi già noto, che

$$A \cup B \text{ è equipotente a } I_n \cup \{n+1, n+2, \ldots, m+n\}.$$

Ma $I_n \cup \{n+1, n+2, \ldots, m+n\} = I_{m+n}$ e quindi la dimostrazione è completa.

Nota: Siano A un insieme finito non vuoto e B un sottoinsieme.
Allora la regola della somma implica che la cardinalità del *complementare*

$$C_A(B) := A - B$$

di B in A è data da $|A| - |B|$.

LE APPLICAZIONI INGETTIVE CONSERVANO LA CARDINALITÀ

Teorema: *Se $f : A \to B$ è un'applicazione ingettiva, allora A e l'immagine $f(A)$ sono insiemi equipotenti.*

Dimostrazione: basta considerare la funzione indotta

$$f : A \to f(A)$$

che è ancora ingettiva. Tale funzione è anche banalmente surgettiva per costruzione, perchè ogni elemento di $f(A)$ è del tipo $f(a)$ con $a \in A$ e quindi possiede una preimmagine mediante tale funzione. Dunque abbiamo costruito una bigezione tra A e $f(A)$.

Come conseguenza immediata abbiamo:

Corollario: *Se $f : A \to B$ è un'applicazione ingettiva, e A è finito, allora anche $f(A)$ è finito e*

$$|f(A)| = |A|.$$

UN ESERCIZIO: SOTTOINSIEMI DI INSIEMI FINITI

Come ulteriore esempio di dimostrazione per induzione, proviamo in modo rigoroso la seguente proprietà, sulla cui validità, a livello intuitivo, non dovremmo avere dubbi:

Se A è un insieme finito non vuoto di cardinalità n, allora ogni sottoinsieme proprio B ($B \subset A$ e $B \neq A$) è anch'esso finito e si ha $|B| < n$.

Ragioniamo per induzione sulla cardinalità n dell'insieme A in considerazione.

Passo base: $n = 1$. L'insieme in questione è equipotente a $I_1 = \{1\}$; segue da ciò che A è un insieme del tipo

$$A = \{x\}$$

per qualche oggetto x. Infatti, se consideriamo una bigezione $f : \{1\} \to A$, allora l'immagine di tale funzione è $\{f(1)\}$ (non vi sono altre immagini oltre $f(1)$!) e quindi $A = \{f(1)\}$ per la surgettività.
Ora, l'unica possibilità è che $B = \emptyset$, che è un insieme finito di cardinalità 0.

Passo induttivo: dato $n \geq 1$, supponiamo la proprietà vera per insiemi di cardinalità n e proviamo che è vera anche per insiemi di cardinalità $n + 1$.
Ammessa l'ipotesi induttiva, consideriamo quindi un arbitrario insieme A finito con $|A| = n + 1$ ed un suo sottoinsieme proprio B. Essendo $B \neq A$, vi è certamente almeno un elemento x di A che non appartiene a B. Allora risulta che:

$$B \subset A - \{x\}.$$

Ora, notiamo che $A - \{x\}$ è finito e $|A - \{x\}| = n$; ciò si può giustificare usando la tecnica che abbiamo incontrato nella dimostrazione del Principio dei Cassetti: assegnata una bigezione

$$f : A \to I_{n+1},$$

essa induce, come sappiamo, un'ingezione:

$$f : A - \{x\} \to I_{n+1} - \{f(x)\}.$$

In effetti, tale applicazione indotta è anch'essa surgettiva, per la surgettività dell' applicazione f di partenza (riflettere su questo punto). Quindi essa è bigettiva e $A - \{x\}$ risulta equipotente a $I_{n+1} - \{f(x)\}$.
D'altra parte, ci è noto che l'insieme $I_{n+1} - \{f(x)\}$ è equipotente a I_n e quindi in definitiva $A - \{x\}$ risulta equipotente a I_n.

Dunque all'insieme $A - \{x\}$ si può applicare l'ipotesi induttiva. Se $B = A - \{x\}$, allora B è finito e $|B| = |A - \{x\}| = n < n+1$ come volevasi. Se invece $B \neq A - \{x\}$, allora trattandosi di un sottoinsieme proprio di $A - \{x\}$, l'ipotesi induttiva garantisce ancora che B è finito con $|B| < |A - \{x\}| = n < n + 1$.

INSIEMI FINITI COSTRUITI MEDIANTE SEQUENZE

Nella pratica, siamo abituati a concepire un insieme finito (non vuoto) come un insieme della forma:

$$A = \{x_1, \ldots, x_n\}$$

dove $n \geq 1$ è un intero e

$$x_1, \ldots, x_n$$

è una sequenza di oggetti.
Notiamo che la sequenza potrebbe contenere ripetizioni, per cui riguardo la cardinalità, si può a priori dire che il nostro insieme risulta:

$$|A| \leq n,$$

ma non è detto che $|A| = n$ (dipende da quali oggetti sono effettivamente coinvolti).
Ad esempio, se

$$x_1 = 10,\ x_2 = 4,\ x_3 = 10,\ x_4 = \sqrt{2}$$

allora

$$A = \{10, 4, 10, \sqrt{2}\} = \{10, 4, \sqrt{2}\}$$

per cui $|A| = 3 < 4$.

Queste considerazioni sono fatte a livello intuitivo: se vogliamo convincerci che questo approccio è coerente con la definizione rigorosa che abbiamo dato sia di insiemi finito che di cardinalità, possiamo ragionare come segue.
Innanzitutto, assegnato l'insieme

$$A = \{x_1, \ldots, x_n\},$$

vi è certamente la funzione surgettiva:

$$x : I_n \to A$$

definita ponendo

$$x(i) := x_i.$$

per ogni $i = 1, \ldots, n$.
Ciò ancora non dice a norma di definizione che A è finito, ma possiamo giustificarlo subito come segue: a partire da questa x si può costruire una funzione ingettiva:

$$f : A \to I_n$$

ponendo

$$f(a) := \text{ più piccola preimmagine } i \text{ di } a \text{ mediante la funzione } x.$$

Tale funzione opera selezionando il primo indice con cui un elemento $a \in A$ compare nella sequenza

$$x_1, \ldots, x_n.$$

Essa è ben definita per il Principio del Minimo (applicato all'insieme delle preimmagini di ciascun y).

La funzione f così costruita è automaticamente ingettiva perchè, se a e a' sono elementi qualsiasi di A, tali che:

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

allora

$$x(f(a)) = x(f(a')),$$

ma $x(f(a)) = a$ per definizione di preimmagine, e analogamente per a'; quindi

$$a = a'.$$

A questo punto, applicando una proprietà delle funzioni ingettive studiata in precedenza, otteniamo che A è equipotente a $f(A)$; ma $f(A)$ è sottoinsieme dell'insieme finito I_n, per cui sappiamo che $f(A)$ è finito, e quindi tale è A. Inoltre

$$|A| = |f(A)| \leq |I_n|$$

e quindi abbiamo provato in modo rigoroso le nostre affermazioni: A è finito e

$$|A| \leq n.$$

Nota: Naturalmente ogni insieme finito A con cardinalità $n \geq 1$, si può sempre rappresentare nel modo descritto

$$A = \{x_1, \ldots, x_n\}$$

con tutti gli elementi x_i *diversi tra loro* (cioè in modo che la sequenza $x_1, \ldots, x_n$ non contiene ripetizioni).
Basta fissare una qualsiasi bigezione

$$x : I_n \to A$$

e considerare la sequenza delle immagini

$$x(1), \ldots, x(n).$$

Esse costituiscono l'intero insieme A (surgettività), e sono tutte distinte (ingettività).

CARDINALITÀ DELL'IMMAGINE DI UN'APPLICAZIONE

Abbiamo visto che le applicazioni ingettive conservano la cardinalità; per applicazioni qualsiasi vale questo risultato più debole, ma comunque significativo:

Teorema: *Sia A un insieme finito non vuoto. Allora per ogni applicazione*

$$f : A \to B$$

con dominio A, si ha che l'immagine $f(A)$ è un insieme finito e

$$|f(A)| \leq |A|.$$

Dimostrazione: Posto $n := |A|$, rappresentiamo l'insieme A come

$$A = \{x_1, \ldots, x_n\}$$

dove gli elementi della sequenza $x_1, \ldots, x_n$ sono tutti distinti. L'immagine $f(A)$ è per definizione data dall'insieme

$$f(A) = \{f(x_1), \ldots, f(x_n)\}.$$

In base alla discussione fatta nel paragrafo precedente, anche tale insieme è finito; non sappiamo se la sequenza $f(x_1), \ldots, f(x_n)$ contiene ripetizioni, ma in ogni caso possiamo affermare che

$$|f(A)| \leq n$$

ovvero

$$|f(A)| \leq |A|.$$

APPLICAZIONI TRA INSIEMI FINITI EQUIPOTENTI

Come applicazione del Teorema sulla cardinalità dell'immagine, otterremo il seguente risultato rilevante in cui si esamina una situazione particolare: applicazioni tra insiemi finiti equipotenti:

Teorema: *Sia $f : A \to B$ un'applicazione tra insiemi finiti, non vuoti, con la stessa cardinalità. Allora f è ingettiva se e solo se è surgettiva.*

Dimostrazione: Supponiamo che f sia ingettiva. Allora

$$|f(A)| = |A| = |B|$$

e quindi il sottoinsieme $f(A)$ di B non può essere proprio; in altri termini,

$$f(A) = B$$

dunque f è surgettiva.

Supponiamo ora che f sia surgettiva e proviamo che f è ingettiva; consideriamo due elementi x, x' in A tali che

$$f(x) = f(x').$$

Vogliamo dedurre che $x = x'$. Supponiamo per assurdo che $x \neq x'$. Osserviamo che la restrizione

$$f : A - \{x'\} \to B$$

sarebbe ancora surgettiva, perchè, stante la surgettività della funzione originaria f, ogni $b \in B$ ha una preimmagine $a \in A$; se $a \neq x'$, tale elemento appartiene a $A - \{x'\}$ ed è ancora una preimmagine di b mediante la restrizione. Se $a = x'$, abbiamo anche

$$f(x) = f(x') = b$$

e quindi x, che appartiene a $A - \{x'\}$, è preimmagine di b mediante la restrizione.

Quindi avremmo $B = f(A - \{x\})$ e in particolare:

$$|B| = |f(A - \{x'\})| \leq |A - \{x\}| = |A| - 1 = |B| - 1$$

e questo è assurdo. Dunque dev'essere $x = x'$ e resta provato che f è ingettiva.

Nota: Per applicazioni tra insiemi *infiniti* equipotenti, tale risultato non sussiste. Ad esempio

$$f : \mathbb{N} \to \mathbb{N}, \quad f(x) = x + 1$$

è ingettiva ma non surgettiva. L'applicazione

$$g : \mathbb{Z} \to \mathbb{N}, \quad g(x) = |x|$$

è surgettiva, ma non ingettiva.

PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Il risultato seguente generalizza il Principio della Somma ed è uno strumento molto importante nel calcolo combinatorio:

Teorema: *Siano A e B insiemi finiti. Allora $A \cup B$ è finito e*

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

Esempio: Si sa che tra 1000 persone ci sono 400 maschi, 200 bambini maschi e 300 tra bambini e bambine. Quante sono le donne adulte?

Usiamo la seguente schematizzazione:
P:= l'insieme delle persone coinvolte;
M:= maschi di P
D:= donne di P
B:= bambini e bambine in P.
A:= adulti in P.

Abbiamo

$$P = M \cup D = A \cup B.$$

Dati del problema: $|P| = 1000$, $|M| = 400$, $|B| = 300$, $|B \cap M| = 200$.

Obiettivo: calcolare $|D \cap A|$.
Usiamo il principio di inclusione-esclusione, applicato agli insiemi D e A:

$$|D \cap A| = |D| + |A| - |D \cup A|.$$

Dai dati, siccome A e B sono digiunti, ricaviamo subito che $|A| = 1000 - 300 = 700$, e analogamente $|D| = 1000 - 400 = 600$. Quindi resta solo da valutare $|D \cup A|$. L'ultimo dato permette di risalire indirettamente alla cardinalità di tale insieme, perchè:

$$C_P(D \cup A) = C_P(D) \cap C_P(A) = M \cap B$$

e quindi:

$$|C_P(D \cup A)| = 200$$

ovvero

$$|D \cup A| = 1000 - 200 = 800.$$

In definitiva:

$$|D \cap A| = 600 + 700 - 800 = 500.$$

LA REGOLA DELLA SOMMA NEL CASO DI PIÙ INSIEMI

La regola della somma può essere estesa in modo ovvio al caso di una sequenza di insiemi:

$$A_1, \ldots, A_n, \quad n \geq 2,$$

dando la seguente formula per calcolare la cardinalità dell'unione di tali insiemi (l'insieme degli oggetti che appartengono ad almeno uno degli insiemi A_i), sempre nell'ipotesi che gli A_i siano **a due a due disgiunti**:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

L'ipotesi è quindi che

$$A_i \cap A_j = \emptyset$$

per ogni coppia di indici $i \neq j$.

Il lettore può provare a fare la dimostrazione per induzione (su n). Il passo base $n = 2$ corrisponde al caso già noto.

DIMOSTRAZIONE DEL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Ricordiamo che si tratta di provare, dati due insiemi qualsiasi non vuoti A e B, che $A \cup B$ è finito e

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

Entrambe le affermazioni sono riconducibili al Principio della Somma, precisamente al caso di 3 insiemi a due a due disgiunti; infatti possiamo rappresentare $A \cup B$ nel modo seguente:

$$A \cup B = C_A(A \cap B) \cup (A \cap B) \cup C_B(A \cap B).$$

Dunque $A \cup B$ è finito e la sua cardinalità si ottiene come somma delle cardinalità dei 3 insiemi considerati:

$$|A \cup B| = |C_A(A \cap B)| + (A \cap B) + |C_B(A \cap B)|.$$

Ora, sappiamo che (è stato già osservato come conseguenza della regola della somma):

$$|C_A(A \cap B)| = |A| - |A \cap B|$$

e analogamente

$$|C_B(A \cap B)| = |B| - |A \cap B|.$$

Quindi in definitiva:

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

GENERALIZZAZIONE DEL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Nel caso di tre insiemi A, B, C sussiste il seguente risultato:

Teorema: *Se A, B, C sono insiemi finiti non vuoti, allora:*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Per dimostralo, basta utilizzare più volte il Principio di Inclusione-Esclusione e le seguenti leggi basilari (distributività dell'unione rispetto a all'intersezione e viceversa), valide per insiemi qualsiasi:

$$(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z), \;\; (X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z).$$

Procediamo quindi come segue:

$$\begin{aligned} |A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C| = \\ = |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| = \\ = |A| + |B| - |A \cap B| + |C| - \{|A \cap C| + |B \cap C| - |(A \cap B) \cap (B \cap C)|\} = \\ = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \end{aligned}$$

Nota: Nel caso generale, la formula per calcolare la cardinalità dell'unione di più insiemi $A_1, \ldots, A_n$ è più complicata, sebbene l'idea di fondo resti la stessa; alla somma

$$|A_1| + \cdots + |A_n|$$

va *sottratta* una quantitità che è a sua volta somma di più addendi; il generico di questi addendi è del tipo

$$(-1)^k \sum_I |A_{i_1} \cap \cdots \cap A_{i_k}|$$

dove $I = (i_1 \ldots, i_k)$ è un multi-indice di lunghezza k, e i k indici che lo costituiscono sono in ordine crescente:

$$1 \leq i_1 < \cdots < i_k \leq n.$$

Per ogni $k = 2, \ldots, n$ occorre considerare tutti i multi-indici possibili di lunghezza k. Si noti che in forza del fattore $(-1)^k$, gli addendi corrispondenti a multi-indici di lunghezza pari vanno sottratti, mentre quelli corrispondenti a multi-indici di lunghezza dispari vanno sommati alla quantità iniziale $|A_1| + \cdots + |A_n|$.
Ad esempio, nella formula che abbiamo studiato sopra, dove $n = 3$:

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

abbiamo tre addendi con multi-indici di lunghezza 2: ovvero $(1, 2)$, $(1, 3)$ e $(2, 3)$ e un solo multi-indice di lunghezza 3, ovvero $(1, 2, 3)$.

LA REGOLA DEL PRODOTTO

Il risultato seguente costituisce la seconda regola fondamentale del contare; anch'essa ci è familiare già dalla scuola primaria.

Teorema: *Siano A e B insiemi non vuoti. Allora $A \times B$ è finito e si ha:*

$$|A \times B| = |A| \cdot |B|.$$

Si tratta di contare quante sono le coppie ordinate (a, b) dove a può essere scelto in tutti modi possibili nell'insieme A e b in tutti i modi possibili nell'insieme B. Dunque un modo più espressivo per esprimere questa formula, sotto forma di regola pratica, è il seguente:

Se si può fare una scelta in m modi possibili, e per ciascuna di queste, vi sono n modi per farne un'altra, il numero totale di modi in cui è possibile fare entrambe le scelte è $m \cdot n$.

Anche questo principio si estende al caso di più insiemi. Il prodotto cartesiano

$$A_1 \times \cdots \times A_n$$

di n insiemi si può definire come l'insieme delle n-ple ordinate (terne se $n = 3$, quaterne se $n = 4$) di oggetti:

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

dove ogni a_i appartiene al corrispondente insieme A_i. Come nel caso delle coppie, vale il criterio di uguaglianza:

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \iff a_i = b_i \text{ per ogni } i = 1, \ldots, n.$$

Ad esempio, se $n = 3$

$$A \times B \times C = \{(a, b, c) | a \in A,\, b \in B,\, c \in C\}.$$

Tale insieme si può pensare come $(A \times B) \times C$, avendo identificato ogni coppia

$$((a, b), c)$$

dove $a \in A$, $b \in B$ e $c \in C$, con la terna:

$$(a, b, c).$$

Lo stesso insieme si può anche identificare con $A \times (B \times C)$ (in luogo di $(a, (b, c))$ scriviamo (a, b, c)).

La formula del prodotto si estende quindi in modo ovvio: dati gli insiemi $A_1, \ldots, A_n$, allora:

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Ad esempio, il numero di informazioni diverse rappresentabili mediante un byte è 2^8; infatti le possibili configurazioni sono ottenute scegliendo, per ogni bit, tra gli stati: 0 e 1. Dunque il numero totale di configurazioni possibili è

$$\underbrace{2 \cdots 2}_{8\,volte} = 2^8.$$

In termini più formali, un byte altri non è che un elemento del prodotto cartesiano:

$$\underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{\text{Prodotto di 8 insiemi identici}}$$

la cui cardinalità è $|\{0,1\}|^8$, ovvero 2^8.

DIMOSTRAZIONE DELLA REGOLA DEL PRODOTTO

Prima di procedere, conviene fare la seguente osservazione:

Per ogni insieme A e x oggetto qualsiasi fissato, i prodotti cartesiani $A \times \{x\}$ e $\{x\} \times A$ sono entrambi equipotenti ad A.

Esplicitamente abbiamo: $A \times \{x\} = \{(a, x) | \, a \in A\}$, $\{x\} \times A = \{(x, a) | \, a \in A\}$.
Infatti, possiamo considerare le seguenti applicazioni:

$$f : A \times \{x\} \to A, \; f(a, x) := a$$

$$g : \{x\} \times A \to A, \; g(x, a) := a.$$

Si noti che qui usiamo la notazione $f(a, x)$ in luogo di quella corretta $f((a, x))$ ma più pesante.
È evidente che entrambe sono bigezioni: ad esempio, riguardo f, ogni elemento $a \in A$ ha un'unica preimmagine, perchè se

$$f((a', x)) = a$$

allora

$$a' = a$$

e quindi tale preimmagine è la coppia (a, x).

Si tratta di provare che, dati due insiemi finiti non vuoti A e B con $|A| = n$ e $|B| = m$, allora $|A \times B| = mn$.
Procediamo per induzione sulla cardinalità n di A (potendo formulare l'enunciato come: per ogni insieme finito A, per ogni insieme finito B si ha $|A \times B| = mn$).

Passo base: $n = 1$. L'insieme A è del tipo $A = \{x\}$ e quindi, per quanto premesso, qualunque sia B:

$$|A \times B| = |\{x\} \times B| = |B| = m = 1 \cdot m.$$

Passo induttivo: dato $n \geq 0$, supponiamo l'enunciato vero per insiemi A di cardinalità n e proviamolo nel caso di insiemi di cardinalità $n + 1$.

Sia dunque $A = \{x_1, \ldots, x_n, x_{n+1}\}$ con $x_i \neq x_j$ per $i \neq j$, un insieme finito con $n+1$ elementi. Possiamo scrivere, per ogni altro insieme B:

$$A \times B = (\{x_1, \ldots, x_n\} \cup \{x_{n+1}\}) \times B = (I_n \times B) \cup (\{x_{n+1}\} \times B).$$

Gli insiemi $I_n \times B$ e $\{x_{n+1}\} \times B$ sono disgiunti perchè due coppie (x_i, b), $i \in I_n$ e (x_{n+1}, b') con $b, b' \in B$ sono sempre certamente diverse in quanto differiscono per la prima coordinata, avendosi $x_i \neq x_{n+1}$. Pertanto possiamo applicare la regola della somma:

$$|A \times B| = |I_n \times B| + |\{x_{n+1}\} \times B| = nm + m = (n + 1)m$$

dove la seconda uguaglianza è giustificata dall'ipotesi induttiva applicata a I_n e dal passo base già considerato.

CONTARE LE FUNZIONI

Siano A e B due insiemi.

Def: L'insieme di tutte le funzioni $f : B \to A$ si denoterà con il simbolo

$$A^B.$$

Un elemento generico dell'insieme A^B è quindi una tra tutte le possibili funzioni aventi come dominio B e insieme di arrivo A.

Esempio: un byte si può pensare come una funzione $f : \{1, \ldots, 8\} \to \{0, 1\}$ (per ogni bit di posto i, $f(i)$ è il valore corrispondente che può essere 0 oppure 1). Quindi l'insieme di tutti i byte è $\{0, 1\}^{\{1,\ldots,8\}} = \{0, 1\}^{I_8}$.

Questa notazione "esponenziale" è giustificata dall'importante risultato seguente, che conta il numero di tutte le funzioni possibili, fissati B e A.

Teorema: *Se A e B sono insiemi finiti non vuoti, allora anche A^B è finito e*

$$|A^B| = |A|^{|B|}.$$

Presentiamo due modi di ragionare per dimostrarlo entrambi utili, perchè corrispondono a due modi diversi di interpretare una funzione.

Poniamo $|A| = n$ e $|B| = k$, e rappresentiamo gli insiemi in questione come

$$A = \{a_1, \ldots, a_n\},\ B = \{x_1, \ldots, x_k\}$$

dove gli elementi a_i sono tutti diversi tra loro, e lo stesso per gli elementi x_i. Assegnare una funzione $f : B \to A$ equivale a scegliere, per ogni elemento x in B la sua immagine $f(x)$ in A. Si tratta quindi di effettuare tale scelta per ciascuno degli x_i. Ciascuna scelta può essere fatta sempre in n modi diversi (si tratta di selezionare un elemento di A tra gli n disponibili, senza vincoli); pertanto la regola del Prodotto ci insegna che il numero totale di modi per effettuare tutte le scelte è:

$$\underbrace{n \cdot n \cdots n}_{k \text{ volte}} = n^k.$$

Una dimostrazione più formale consiste nell'osservare che, assegnare una funzione $f : B \to A$ equivale ad assegnare la k-pla delle immagini:

$$(f(x_1), \ldots, f(x_k))$$

che è un elemento del prodotto cartesiano

$$\underbrace{A \times A \times \cdots \times A}_{k \text{ volte}} = A^k.$$

Viceversa, ogni k-pla $(y_1, \ldots, y_k)$ con gli elementi y_i tutti in A corrisponde in tal modo ad una sola funzione, quella definita da

$$f(x_i) := y_i, \qquad i = 1, \ldots, k.$$

In altri termini, vi è una corrispondenza biunivoca tra gli insiemi A^B e A^k, data da

$$f \in A^B \mapsto (f(x_1), \ldots, f(x_k)) \in A^k.$$

Ancora meglio: tali insiemi sono equipotenti. Dunque A^B è finito e, stante la regola del Prodotto:

$$|A^B| = |A^k| = |A|^k = n^k.$$

DISPOSIZIONI CON RIPETIZIONE

Def: Sia A un insieme finito con $n \geq 1$ elementi. Sia $k \geq 1$ un intero. Si chiama **disposizione (con ripetizioni) di classe k degli elementi di A**, ogni funzione

$$f : \{1, \ldots, k\} \to A$$

ovvero ogni funzione

$$f : I_k \to A.$$

In base al Teorema visto nel paragrafo precedente abbiamo che:
il numero totale delle disposizioni di classe k degli elementi di un insieme con n oggetti è:

$$n^k.$$

Questo numero ha un'interpretazione pratica: si tratta di contare il numero di modi in cui si possono selezionare k tra n oggetti assegnati, tendendo presente che *l'ordine in cui tali scelte sono effettuate è rilevante.*

Nel modello astratto $f : I_k \to A$ di una disposizione, $f(1)$ è la prima scelta, $f(2)$ la seconda, e così via, l'ultima scelta essendo $f(k)$.

In base a quanto osservato prima, in modo equivalente si tratta di contare tutte le possibili k-ple *ordinate*:

$$(a_1, \ldots, a_k)$$

dove gli a_i sono arbitrari elementi dell'insieme A.

Esempio: Il numero di tutte le possibili stringhe di 9 lettere dell'alfabeto anglosassone (26 caratteri) che si possono stampare è 26^9 (disposizioni di 26 caratteri di classe 9).

L'ordine in cui si susseguono i caratteri è rilevante e distingue le stringhe.

Se denotiano con $\mathcal{A}$ l'insieme di tutte le lettere dell'alfabeto, abbiamo contato tutte le funzioni:

$$f : \{1, \ldots, 9\} \to \mathcal{A},$$

ovvero il numero di tuttle le k-ple $(c_1, \ldots, c_9)$, con $c_i \in \mathcal{A}$, cioè il numero di elementi del prodotto

$$\underbrace{\mathcal{A} \times \cdots \times \mathcal{A}}_{9 \text{ volte}} = \mathcal{A}^9.$$

Esempio: Il numero possibile di targhe automobilistiche del formato

$$AB\ XYZ\ CD$$

con A, B, C, D lettere (alfabeto anglosassone), e X, Y, Z cifre decimali, è pari a:

$$26^2 \cdot 10^3 \cdot 26^2 = 26^4 \cdot 10^3.$$

Tale calcolo è giustificato dalla regola del prodotto; si tratta di tre scelte: stringa AB, stringa XYZ e stringa CD. La prima e la la terza sono entrambe disposizioni di 26 elementi di classe 2, la seconda è una disposizione di 10 elementi (le cifre $0, \ldots, 9$) di classe 3. In tutti i casi sono ammesse ripetizioni: ad esempio $EG\,909\,FF$ è una targa ammissibile. L'ordine in cui si presentano i vari oggetti è rilevante: ad esempio, la targa $FF\,909\,EG$ è diversa dalla precedente.

In modo più sintetico, il calcolo corrisponde a valutare la cardinalità del prodotto cartesiano:

$$\mathcal{A}^2 \times \mathcal{C}^3 \times \mathcal{A}^2,$$

dove $\mathcal{A}$ è l'alfrabeto anglosassone, mentre $\mathcal{C} = \{0, 1, \ldots, 9\}$.

DISPOSIZIONI SEMPLICI

Def: Sia A un insieme finito con $n \geq 1$ elementi. Sia $k \geq 1$ un intero. Si chiama **disposizione semplice (o senza ripetizioni) di classe k degli elementi di A**, ogni funzione **ingettiva**

$$f : \{1, \ldots, k\} \to A$$

ovvero ogni funzione ingettiva

$$f : I_k \to A.$$

Equivalentemente, una disposizione semplice di classe k degli elementi di A è una k-pla ordinata

$$(a_1, \ldots, a_k)$$

di elementi di A *tutti diversi tra loro.*

Per contare il numero di disposizioni semplici, possiamo utilizzare il risultato seguente:

Teorema: *Siano A e B insiemi finiti, con $|A| = n$ e $|B| = k$.*
Il numero $i(B, A)$ delle applicazioni ingettive da B in A è dato da:

$$i(B, A) = \begin{cases} 0 & \text{se } k > n \\ n(n-1)\cdots(n-k+1) & \text{se } k \leq n. \end{cases}$$

Il caso $k > n$ corrisponde al Principio dei Cassetti.
Se $k \neq n$, la dimostrazione procede come nel calcolo di $|A^B|$, con la differenza che non si può scegliere due volte lo stesso elemento di B. Posto quindi $B = \{x_1, \ldots, x_k\}$, l'immagine $f(x_1)$ può essere scelta in n modi, l'immagine di x_2 in $n-1$ modi, perchè $f(x_1)$ non è più a disposizione, $f(x_3)$ potrà scegliersi solo in $A - \{f(x_1), f(x_2)\}$ cioè in $n-2$ modi e così via. Per la Regola del Prodotto, il numero totale di modi in cui si possono fare tutte le k scelte è:

$$n(n-1)(n-2)\cdots(n-(k-1)) = n(n-1)\cdots(n-k+1).$$

Quindi, come caso particolare, quando $B = I_k$, abbiamo:

Il numero $D(n, k)$ di disposizioni semplici di n oggetti di classe k, con $1 \leq k \leq n$, è dato da:

$$D(n, k) = n(n-1)(n-2)\cdots(n-(k-1)) = n(n-1)\cdots(n-k+1).$$

PERMUTAZIONI

Def: Sia A un insieme, Si chiama **permutazione degli elementi di** A oppure **permutazione di** A ogni bigezione $f : A \to A$.

Una permutazione corrisponde, dal punto di vista pratico, a un riordinamento degli elementi dell'insieme, preservando il numero e gli elementi che lo costituiscono.

Es: Se $A = \{a, b, c\}$ con $|A| = 3$, allora vi sono 6 possibili permutazioni, che sono i sei modi diversi in cui possiamo elencare i tre oggetti diversi a, b, c:

$$A = \{a, b, c\} = \{a, c, b\} = \{b, a, c\} = \{b, c, a\} = \{c, a, b\} = \{c, b, a\}.$$

Ad esempio, la terza rappresentazione $\{b, a, c\}$ corrisponde alla bigezione:

$$f : \{a, b, c\} \to \{a, b, c\}$$

definita da:

$$f(a) = b,\ f(b) = a,\ f(c) = c.$$

Tale funzione descrive l'operazione di scambiare a e b e lasciare c come terzo elemento dell'elenco.

Tenendo presente che, se A è finito, le bigezioni da A in A sono tutte e sole le funzioni ingettive, possiamo calcolarne il numero semplicemente calcolando $i(A, A)$, che si ottiene dalla formula generale per $i(B, A)$, ponendo $k = n$. Si ottiene il numero:

$$n(n-1)(n-2)\cdots 1.$$

Tale quantità si chiama fattoriale di n. Più precisamente, per ogni $n \in \mathbb{N}$, chiamiano **fattoriale** di n l'intero, denotato con $n!$, così definito:

$$0! := 1,\ 1! := 1,\ n! := n(n-1)\cdots 1 \quad \text{se } n \geq 2.$$

Riassumendo, abbiamo provato:

Teorema: *Il numero di permutazioni di un insieme con n elementi è dato da n!.*

Nota importante: Il fattoriale può essere utilizzato convenientemente anche per scrivere il numero di disposizioni semplici; risulta infatti che:

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

COMBINAZIONI

Def: Sia A un insieme finito con $|A| = n$ e sia k un intero tale che $1 \leq k \leq n$. Si chiama **combinazione** di classe k degli elementi di A ogni sottoinsieme di A di cardinalità k.

Quindi una combinazione di n oggetti di classe k corrisponde in pratica a selezionare k di questi oggetti, raggruppandoli insieme, ignorando l'ordine con cui tali k scelte vengono effettuate.

Esempio: Se a una competizione partecipano 30 atleti, tutti i possibili *podi* (esiti della gara), ovvero il numero totale delle possibili assegnazioni delle tre medaglie (oro, argento, bronzo) è calcolato dal numero $D(20, 3)$: si tratta di *disposizioni semplici*: (A, B, C) dove A, B e C sono tre diversi atleti. Più precisamente, A è il primo classificato, B il secondo, C la medaglia di bronzo.

Invece, ogni possibile *terna di atleti premiati*, a prescindere dalla classifica, è semplicemente un insieme $\{A, B, C\}$ di tre atleti diversi, ovvero una *combinazione* di 30 oggetti di classe 3.
Notiamo che ognuno di questi gruppi di vincitori genera 6 podi diversi:

$$(A, B, C), (A, C, B), (B, A, C), (B, C, A), (C, A, B), (C, B, A),$$

gli unici in cui sono protagonisti gli atleti in questione. Il numero 6 è esattamente il numero di permutazioni dell'insieme considerato, ovvero della combinazione in esame.

Questa osservazione è del tutto generale: ogni combinazione $C \subset A$ dà luogo a $k!$ diverse disposizioni semplici formate dagli stessi k oggetti che costituiscono la combinazione stessa C. Si tratta semplicemente di disporre gli elementi di C (che è un insieme che non possiede un ordine intrinseco), in un certo ordine. Ma tutti gli ordinamenti possibili sono in numero pari alle permutazioni di C, cioè sono $k!$.

Naturalmente, viceversa, ogni disposizione $(a_1, , \ldots, a_k)$ semplice di classe k degli elementi di A è generata da una sola combinazione: $\{a_1, \ldots, a_k\}$.
Da queste considerazioni discende quindi che:

Toerema: *Il numero $C(n, k)$ di combinazioni di classe k di elementi di un insieme A con n oggetti è dato da:*

$$C(n, k) = \frac{D(n, k)}{k!} = \frac{n!}{k!(n-k)!}.$$

Def: La quantità

$$\frac{n!}{k!(n-k)!}$$

è un numero intero che ha senso per ogni coppia (n, k) di interi con $n \geq 0$ e $0 \leq k \leq n$; essa si denota con il simbolo

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

e prende il nome di **coefficiente binomiale** o **binomiale**.

Se $k = 0$ abbiamo sempre $\binom{n}{0} = 1$; possiamo pensare a questo caso particolare come ad un'assenza di scelte, ovvero a una combinazione di classe 0, che è data dall'insieme vuoto $\emptyset$ (esso è sottoinsieme di qualsiasi insieme).

Se $n = 0$ e quindi $k = 0$, si ottiene ancora $\binom{0}{0} = 1$: ciò corrisponde al fatto che l'insieme vuoto $\emptyset$ ha se stesso come unico sottoinsieme.

Un altro caso particolare è $n = k \geq 1$: otteniamo ancora $\binom{n}{n} = 1 = C(n, n)$, in accordo col fatto che l'unico sottoinsieme di cardinalità n di un insieme con n oggetti è l'intero insieme A.

L'INSIEME DELLE PARTI

Def: Dato un insieme A, l'insieme di tutti i suoi sottoinsiemi si denota con $\mathcal{P}(A)$ e si chiama **insieme delle parti** di A.
In simboli:

$$\mathcal{P}(A) := \{X | \, X \subset A\}.$$

Es: Per definizione, abbiamo sempre $A \in \mathcal{P}(A)$ e $\emptyset \in \mathcal{P}(A)$. Per ogni $a \in A$, si ha pure $\{a\} \in \mathcal{P}(A)$.

Es: Sia $A = \{0, 1\}$. Allora

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Nota: Se A è finito, le combinazioni di elementi di A (di qualsiasi classe, compresa la classe 0) sono esattamente gli elementi di $\mathcal{P}(A)$.

Def: Sia $X \subset A$ un sottoinsieme di A. Si chiama **funzione caratteristica** di X la funzione

$$c_X : A \to \{0, 1\}$$

definita come segue:

$$c_X(a) := \begin{cases} 1 & \text{se } a \in X \\ 0 & \text{se } a \notin X \end{cases}.$$

La funzione caratteristica di un sottoinsieme permette di ricostruire il sottoinsieme stesso come l'insieme di tutte le preimmagini di 1 mediante la funzione: in simboli

$$X = c_X^{-1}(1).$$

Infatti, stante la definizione della funzione caratteristica, X è esattamente l'insieme di tutti e soli gli elementi di A per i quali il valore assunto dalla funzione c_X è 1.
Pertanto, se è nota la funzione caratteristica, è noto l'insieme X.

Es: Se $A = \{0, 1\}$, la funzione caratteristica di $\{0\}$ è descritta da:

$$c_{\{0\}}(0) = 1, \; c_{\{0\}}(1) = 0$$

mentre per il sottoinsieme $\{1\}$ abbiamo:

$$c_{\{1\}}(0) = 0, \; c_{\{1\}}(1) = 1.$$

CARDINALITÀ DELL'INSIEME DELLE PARTI

Il risultato seguente permette mette in relazione il concetto di sottoinsieme con quello di funzione:

Teorema: *Sia A un insieme. L'insieme delle parti $\mathcal{P}(A)$ di A e l'insieme $\{0,1\}^A$ di tutte le funzioni $A \to \{0,1\}$ sono equipotenti. Più precisamente, la funzione*

$$c : \mathcal{P}(A) \to \{0,1\}^A$$

definita da

$$c(X) := c_X$$

è una bigezione tra questi due insiemi.

Dimostrazione.

Ingettività di c: siano X, Y sottoinsiemi di A tali che $c(X) = c(Y)$. Vogliamo dedurne che $X = Y$. Per definizione di c, abbiamo quindi che

$$c_X = c_Y.$$

Sappiamo che ogni sottoinsieme X è ricostruibile dalla corrispondente funzione caratteristica, in quanto coincide con l'insieme degli oggetti su cui la funzione in questione vale 1; in simboli:

$$X = c_X^{-1}(1).$$

Analogo discorso per Y e quindi si ricava, siccome le funzioni c_X e c_Y coincidono:

$$X = c_X^{-1}(1) = c_Y^{-1}(1) = Y$$

e quindi $X = Y$.

Surgettività di c: dobbiamo provare che ogni funzione $f : A \to \{0,1\}$ ha una preimmagine X mediante c, ovvero è ottenibile come funzione caratteristica di un opportuno sottoinsieme X; in simboli, si tratta di individuare un sottoinsieme di A tale che:

$$f = c_X.$$

A questo scopo, la scelta è obbligata: è sufficiente porre

$$X := \{a \in A | f(a) = 1\} = f^{-1}(1).$$

Con questa scelta di X, abbiamo in effetti che:

$$f(a) = \begin{cases} 1 & \text{se } a \in X \\ 0 & \text{se } a \notin X \end{cases}$$

e ciò mostra che f è esattamente la funzione caratteristica di X.

Come rilevante applicazione, abbiamo, nel caso di insiemi finiti:

Teorema: *Sia A un insieme finito di cardinalità n. Allora l'insieme delle parti $\mathcal{P}(A)$ è finito e si ha:*

$$\mathcal{P}(A) = 2^n.$$

Si tratta semplicemente di applicare il teorema sulla cardinalità dell'insieme delle funzioni tra insiemi finiti.

Nota: Questo risultato si può provare direttamente per induzione sulla cardinalità n di $|A|$, senza usare le funzioni caratteristiche.

Passo base: $n = 0$. Abbiamo $A = \emptyset$, ma $\mathcal{P}(\emptyset) = \{\emptyset\}$ e si ha effettivamente

$$|\mathcal{P}(\emptyset)| = 1 = 2^0.$$

Passo induttivo: Dato $n \geq 0$, supponiamo la tesi vera per insiemi di cardinalità n e proviamola per insiemi di cardinalità $n+1$. Dato A con $|A| = n+1$, sia $A' = A - \{x\}$ dove x è un fissato elemento di A. Ora, i sottoinsiemi di A si possono dividere in due categorie distinte: quelli non contenenti x e quelli contenenti x:

$$\mathcal{P}(A) = P_1 \cup P_2$$

dove

$$P_1 := \{X \subset A | \, x \notin X\}, \;\; P_2 := \{X \subset A | \, x \in X\}.$$

Chiaramente P_1 e P_2 sono disgiunti. Inoltre P_1 è esattamente l'insieme delle parti di A'; quindi per l'ipotesi induttiva, P_1 è finito con $|P_1| = 2^n$.
Quanto a P_2, ogni sottoinsieme X' di A che contiene x si può vedere come un insieme della forma:

$$X' = X \cup \{x\}$$

dove X non contiene x. Ciò significa che P_2 è equipotente a P_1; in altri termini, l'applicazione:

$$X \in P_1 \mapsto X \cup \{x\} \in P_2$$

è una bigezione tra P_1 e P_2.
Conclusione: per la regola della somma, anche $\mathcal{P}(A)$ è finito e

$$|\mathcal{P}(A)| = |P_1| + |P_2| = 2|P_1| = 2 \cdot 2^n = 2^{n+1}.$$

INTERPRETAZIONE DELLE COMBINAZIONI COME FUNZIONI

In precedenza, abbiamo definito le disposizioni (sia quelle con ripetizione che quelle semplici), usando il concetto di funzione (funzioni $I_k \to A$, ingettive nel secondo caso). Dalla discussione precedente sull'insieme delle parti, ricaviamo che un approccio simile è possibile anche per le combinazioni (senza ripetizioni). Cambia il tipo di funzione e la condizione richiesta:

Ogni combinazione di classe k degli elementi di un insieme finito A di cardinalità n è interpretabile come una funzione

$$f : A \to \{0, 1\}$$

soddisfacente la condizione aggiuntiva $|f^{-1}(1)| = k$.

Una tale funzione determina la combinazione $X = f^{-1}(1)$ costituita da tutti e soli gli elementi di A su cui la funzione assume il valore 1.
Viceversa, ogni combinazione X dà luogo a una tale funzione: la sua funzione caratteristica $f = c_X$.

Es: Un byte contentente 5 bits accesi (di valore 1), si può modellizzare come una funzione:

$$f : \{1, \ldots, 8\} \to \{0, 1\}$$

tale che $|f^{-1}(1)| = 5$. Dunque, altri non è che una combinazione di classe 5 dell'insieme $\{1, \ldots, 8\}$. Ad esempio, se il byte è 0 1 1 0 1 0 1 1, allora la funzione è:

$$f(1) = 0,\ f(2) = 1,\ f(3) = 1,\ f(4) = 0,\ f(5) = 1,\ f(6) = 0,\ f(7) = 1,\ f(8) = 1,$$

mentre la combinazione corrispondente è $\{2, 3, 5, 6, 8\}$.

Dunque il numero totale di bytes con 5 bits accesi è pari a $C(8, 5) = \binom{8}{5} = 56$.

ALCUNE PROPRIETÀ DEI COEFFICIENTI BINOMIALI

Nota: *Siano n e k numeri naturali, con $0 \leq k \leq n$. Allora*

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

La dimostrazione si può fare immediatamente usando la definizione $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, sostituendo $n-k$ al posto di k. È istruttivo però ragionare sul significato di $\binom{n}{k}$ come numero dei sottoinsiemi di cardinalità k di un assegnato insieme A con $|A| = n$. Infatti, ad ogni sottoinsieme C con $|C| = k$ corrisponde il suo complementare $C_A(C)$ che ha cardinalità $n-k$. Ora, la funzione

$$F : \mathcal{P}(A) \to \mathcal{P}(A)$$

$$F(C) := C_A(C)$$

che associa ad ogni sottoinsieme il proprio complementare, è bigettiva, in quanto ogni sottoinsieme X è il complementare di uno ed un solo sottoinsieme: il suo complementare $C_A(X)$! Dunque ogni X ha esattamente una preimmagine mediante F.

La bigezione F induce una bigezione tra l'insieme dei sottoinsiemi di A di cardinalità k e l'insieme di quelli di cardinalità $n-k$, che sono pertanto equipotenti. Dunque $\binom{n}{k} = \binom{n}{n-k}$.

Nota: Per ogni coppia di interi $n \geq 1$ e $1 < k \leq n$, si ha:

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

Anche questa identità si può spiegare ragionando sui sottoinsiemi di un insieme A con $|A| = n+1$, ad esempio $A = I_{n+1}$. Possiamo suddividere i sottoinsiemi di cardinalità k di I_{n+1} in due categorie disgiunte (si veda la dimostrazione per induzione dell'identità $|\mathcal{P}(A)| = 2^n$ discussa precedentemente): quelli non contenenti $n+1$ e quelli che contengono $n+1$.

I primi sono esattamente i sottoinsiemi di I_n di cardinalità k, e sono $\binom{n}{k}$, mentre i secondi sono del tipo $X \cup \{n+1\}$ con $X \subset I_n$ di cardinalità $k-1$, e questi sono $\binom{n}{k-1}$. A questo punto basta applicare la regola della somma che dà $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.

L'ultima proprietà fornisce un algoritmo per calcolare i coefficienti binomiali, che evita l'utilizzo diretto della formula che li definisce, evitando quindi di dover calcolare fattoriali: il cosiddetto Triangolo di Tartaglia (o di Pascal).

Per scrivere tutti i coefficienti binomiali $\binom{n}{k}$ fino ad un certo n, si può procedere costruendo una tabella step by step, con $n+1$ righe; ciascuna riga i-ma conterrà tutti i binomiali $\binom{i}{k}$, $0 \leq i \leq n,\ 0 \leq k \leq i$.

Le prime due righe sono ($i = 0, 1$):

1

1 1

Da questo punto in poi, basta applicare il seguente algoritmo: *i numeri di ogni riga si ottengono ponendo il primo uguale a 1; quindi si inserisce la sequenza che si ottiene effettuando le somme di coppie di numeri consecutivi della riga precedente; infine l'ultimo numero della riga è 1.*

Procedendo con tale metodo otteniamo, fino a $n = 5$:

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1.

COMBINAZIONI CON RIPETIZIONI

Si chiama **combinazione con ripetizioni** di classe k di n oggetti, il procedimento di compiere k scelte tra gli n oggetti, con eventuali ripetizioni, essendo irrilevante anche l'ordine con cui si effettuano tali scelte.

Es: Un vassoio di 10 pasticcini, scelti da un listino di 5 specialità diverse, è una combinazione di classe 10 di 5 oggetti.

Un modello alternativo di questo concetto è costituito da *stringhe di lunghezza k* costruite con caratteri scelti in un *alfabeto A con n caratteri*, con eventuali ripetizioni di caratteri, e considerate *a meno di una permutazione dei caratteri* stessi; ovvero due tali stringhe si considerano uguali se differiscono solo per una *permutazione dei loro caratteri.*

Tornando all'esempio del vassoio di paste, se le 5 tipologie sono *cannuolo, bignè, meringa, sfogliatella, tartufo*, contrassegnate con le lettere C, B, M, S, T, allora una possibile comanda per istruire il pasticciere a fare una confezione di 10 pasticcini è:

$$CCCBBMMSST$$

Tale confezione prevede 3 cannuoli, 2 bignè, ecc. La stringa rappresenta ancora una combinazione con ripetizioni di classe 10 di 5 oggetti. Naturalmente, il pasticciere è libero di posizionare nella confezione prima il tarfufo e poi gli altri tipi di paste: l'ordine delle scelte non è rilevante. Anche la stringa:

$$TCBBCMMCSS$$

rappresenta la stessa comanda.

Una definizione più rigorosa, basata come nei casi delle disposizioni (con ripetizione oppure semplici) e combinazioni semplici, sul concetto di funzione, si può dare facilmente se si osserva che l' informazione occorrente per ricostruire una combinazione di questo tipo è: *conoscere il numero di volte in cui lo stesso oggetto viene scelto, per ogni oggetto.*

Nel modello delle stringhe, non essendo importante la posizione dei caratteri, quello che occorre sapere è il numero di occorrenze in essa di ciascun carattere a disposizione. Esso è un numero naturale che varia tra 0 e k, dove k è la lunghezza delle stringa. La somma di tali occorrenze è ovviamente vincolata: dev'essere k.
Ad esempio, se $A = \{a, b, c, X, Y\}$, nella stringa

$$aXYa$$

il carattere a compare 2 volte, mentre b e c entrambi 0 volte, X e Y una sola volta. La sequenza di numeri $(2, 1, 1, 0, 0)$ identifica la stringa stessa, che si può anche interpretare ad esempio come $XaaY$, in base al criterio sull'uguaglianza tra stringhe.

Queste considerazioni portano alla seguente definizione rigorosa:

Def: Si chiama **combinazione con ripetizioni di classe** k degli elementi di un insieme $A = \{a_1, \ldots, a_n\}$ di cardinalità n, ogni funzione

$$f : A \to \{0, 1, \ldots, k\}$$

tale che

$$f(a_1) + f(a_2) + \cdots + f(a_n) = k.$$

Denoteremo il numero totale di combinazioni con ripetizione di classe k di n oggetti con il simbolo

$$c(n, k).$$

Tale numero fornisce, ad esempio, una soluzione al seguente tipo di problema rilevante:

Problema tipo: *Quante sono le n-ple di interi naturali* $(a_1, \ldots, a_n)$*,* $n \geq 1$*, la cui somma*

$$a_1 + \cdots + a_n$$

è un numero assegnato k*?*

Ad esempio, se $n = 3$ e $k = 5$, due terne che sodisfano la condizione richiesta sono

$$(5, 0, 0),\ (0, 3, 2),\ (1, 2, 2)$$

ma ce ne sono altre.
Se $k = 0$, allora qualunque sia n, vi è una sola possibilità: $(0, 0, \ldots, 0)$.

Assegnati n e k, risulta che *il numero totale delle n-ple in questione è proprio* $c(n, k)$*.*

Infatti, ogni n-pla che soddisfa il requisito richiesto si può schematizzare mediante la funzione $f : I_n \to \{0, \ldots, k\}$ tale che

$$f(i) := a_i$$

che è soggetta al vincolo:

$$a_1 + \cdots + a_n = k$$

ovvero

$$f(1) + \cdots + f(n) = k.$$

Quindi, in base alla definizione data sopra, si tratta di una combinazione con ripetizione di classe k degli elementi di $I_n = \{1, \ldots, n\}$. Dunque la risposta al problema è data dal numero totale di tali combinazioni, ovvero $c(n, k)$.

Nel paragrafo seguente diamo una semplice formula per calcolare $c(n, k)$.

CONTARE LE COMBINAZIONI CON RIPETIZIONI

Teorema: *Il numero $c(n,k)$ di combinazioni con ripetizioni di classe k di n oggetti è dato da*

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

Dobbiamo contare il numero di funzioni

$$f : I_n \to \{0,\dots,k\}$$

tali che

$$f(1) + \cdots + f(n) = k.$$

L'idea chiave della dimostrazione è il fatto che l'informazione racchiusa in una tale funzione si può compattare in un'unica stringa binaria, dove ogni valore $f(i)$ della funzione viene tradotto in una sequenza di $f(i)$ bits accesi (valore 1) consecutivi (eventualmente nessun bit se $f(i) = 0$); per distinguere tra loro questi n pacchetti di bits, viene utilizzato un bit 0, che funge da separatore. Quindi abbiamo $n-1$ separatori, mentre il numero totale di bits di valore 1 è pari a k.

Ad esempio, la stringa binaria

$$111011101111011$$

rappresenta la funzione

$$f : \{1,2,3,4\} \to \{0,\dots,12\}$$

definita da

$$f(1) = 3,\ f(2) = 3,\ f(3) = 4,\ f(4) = 2,$$

ovvero una combinazione con ripetizione di 4 oggetti, di classe 12. Mentre la stringa

$$001110011011$$

rappresenta la funzione

$$g : \{1,2,3,4,5,6\} \to \{0,\dots,7\}$$

tale che

$$g(1) = 0,\ g(2) = 0,\ g(3) = 3,\ g(4) = 0,\ g(5) = 2,\ g(6) = 2,$$

cioè una combinazione con ripetizioni di 6 oggetti, di classe 7.

Ciò premesso, fissati n e k, il numero da contare per valutare $c(n,k)$ è quello delle stringhe binarie di lunghezza $n-1+k$ con esattamente k bits pari a 1, ovvero il numero di tutte le funzioni:

$$f : I_{n+k-1} \to \{0,1\}$$

tali che $|f^{-1}(1)| = k$ che, come sappiamo, altri non è che il numero di combinazioni semplici $C(n+k-1,k)$, ovvero $\binom{n+k-1}{k}$.

Es: In quanti modi si possono distribuire 50 monete identiche in 5 salvadani? In quanti modi si può fare la stessa cosa se vogliamo che tutti i salvadani contengano almeno 6 monete?

Ciò che caratterizza una possibile distribuzione è la quantità di monete che conterrà ciascun salvadanaio, per cui detta s_i tale quantità relativa al salvadanio i-mo, si tratta di trovare il numero di 5-ple $(s_1, s_2, s_3, s_4, s_5)$ di numeri naturali tali che $s_1 + \cdots s_5 = 50$.
Un approccio equivalente, è modellizzare ogni possibile distribuzione di monete come una funzione:

$$f : \{1, 2, 3, 4, 5\} \to \{0, \ldots, 50\}$$

definita da $f(i) :=$ monete messe nel salvadanaio i-mo. Abbiamo il vincolo:

$$f(1) + f(2) + f(3) + f(4) + f(5) = 50.$$

Quindi la risposta alla prima domanda è data da $c(5, 50)$, che possiamo calcolare utilizzando il Teorema precedente:

$$c(5, 50) = \binom{55-1}{50} = \binom{54}{50} = \frac{54!}{50!4!} = \frac{54 \cdot 53 \cdot 52 \cdot 51}{4 \cdot 3 \cdot 2} = 316251.$$

Riguardo il secondo caso, possiamo ricondurci al primo mettendo prima 6 monete in ogni salvadanaio (totale 30 monete), e poi procedere con le monete rimaste; il quesito è quindi ricondotto al tipo precedente, e la risposta è fornita dal numero $c(20, 5)$.

Alternativamente, il problema consiste nel contare tutte le 5-ple $(s_1, \ldots, s_5)$ di numeri con $s_1 + \cdots + s_5 = 50$, soggette all'ulteriore vincolo $s_i \geq 6$ per ogni i. Se consideriamo in luogo di una tale 5-pla, la seguente:

$$(s_1 - 6, \ldots, s_5 - 6)$$

ottenuta sottraendo 6 ad ogni ingresso, per la quale risulta:

$$(s_1 - 6) + \cdots + (s_5 - 6) = s_1 + \cdots + s_5 - 5 \cdot 6 = 50 - 30 = 20,$$

il problema viene ricondotto a quello di trovare il numero di 5-ple di numeri naturali

$$(s'_1, \ldots, s'_5)$$

tali che

$$s'_1 + \cdots + s'_5 = 20.$$

A partire da una tale 5-pla, possiamo sempre ricostruire la distribuzione originale delle monete aggiungendo 6 a ciascuno dei numeri s'_i.
Quindi la risposta è sempre $c(20, 5)$.

PARTIZIONI DI UN INSIEME

Definizione: Sia A un insieme non vuoto. Si chiama **partizione** di A un sottoinsieme non vuoto $P \subset \mathcal{P}(A)$ dell'insieme $\mathcal{P}(A)$ delle parti di A, soddisfacente le seguenti condizioni:

1) Ogni $B \in P$ è non vuoto;

2) *ogni* elemento di A appartiene ad *uno ed uno solo* degli insiemi appartenenti a P.

Gli elementi di una partizione P sono detti *blocchi* della partizione.

Es: Sia $A = I_{10} = \{1, 2, \cdots, 9, 10\}$.

Considerati i sottoinsiemi $B_1 = \{1, 4, 7, 8\}, B_2 = \{2, 3, 5\}$, $B_3 = \{6, 9\}$ e $B_4 = \{10\}$ di A, allora

$$P = \{B_1, \ldots, B_4\}$$

è una partizione di A con 4 blocchi.

Es: Un esempio di partizione di $\mathbb{Z}$ è $P = \{B_1, B_2\}$, i cui due blocchi sono rispettivamente l'insieme degli interi pari e l'insieme degli interi dispari:

$$B_1 = \{2n | \, n \in \mathbb{Z}\}, \quad B_2 = \{2n + 1 | \, n \in \mathbb{Z}\}.$$

Es: Se A è un insieme non vuoto qualsiasi, allora si può costruire una partizione considerando come blocchi i "singleton", tutti i sottoinsiemi contenenti un solo oggetto:

$$P = \{\{a\} | \, a \in A\}.$$

Se A è infinito, tale partizione ha infiniti blocchi.

NUMERI DI STIRLING

Def: Il mumero di tutte le **partizioni** con esattamente k blocchi di un insieme avente n elementi si denota con

$$S(n,k)$$

e si chiama **numero di Stirling** (del secondo tipo) di indici n, k. Qui $n \geq 1$ e $k \geq 1$.

Osserviamo che, se $|A| = n$ e $k > n$ non esistono partizioni di A con k blocchi: dopo aver selezionato i blocchi a cui ciascuno degli elementi deve appartenere, avremo al massimo n blocchi distinti. (In modo più formale: abbiamo la funzione $a \in A \mapsto B_a \in P$ che associa ad ogni $a \in A$ l'unico blocco B_a a cui appartiene. Tale funzione è surgettiva, perchè ogni blocco è non vuoto, e quindi $n \geq k$).

Nota: Osserviamo che

$$S(n,1) = S(n,n) = 1.$$

Infatti, l'unica partizione con un solo blocco è $P = \{A\}$, mentre l'unica con n blocchi è quella fatta dai singleton: $P = \{\{a\} | \, a \in A\}$.

Teorema: *I numeri di Stirling verificano la relazione ricorsiva:*

$$S(n,k) = S(n-1,k-1) + k\, S(n-1,k),$$

dove $n \geq 2$, $2 \leq k \leq n-1$.

Per provarlo, consideriamo l'insieme modello $A = I_n$ e notiamo che le partizioni con k blocchi di I_n si possono dividere in due categorie disgiunte:

1^o tipo) $\{n\}$ è un blocco.

2^o tipo) $\{n\}$ non è un blocco.

Le partizioni di tipo 1 sono tante quante quelle di I_{n-1} con $k-1$ blocchi, perchè tutti i blocchi diversi da $\{n\}$ non possono contenere n e quindi sono sottoinsiemi di I_{n-1}.

Quelle di tipo 2) si ottengono mediante due scelte: una partizione di I_{n-1} con k blocchi e la scelta di un unico blocco tra questi, che deve contenere n. Vi sono k scelte di tale blocco, per cui per il principio del prodotto abbiamo in totale $k \cdot S(n-1,k)$ possibilità.
In conclusione, il principio della somma permette di concludere che $S(n,k)$ è dato da $S(n-1,k-1) + k\, S(n-1,k)$.

L'ultimo Teorema fornisce un algoritmo per calcolare i numeri di Stirling, mediante un algoritmo simile al Triangolo di Tartaglia.

Per scrivere tutti i numeri $S(n,k)$ fino ad un certo n, si può procedere costruendo una tabella step by step, con n righe; ciascuna riga i-ma conterrà tutti i numeri di Stirling $S(i,k)$, $1 \leq i \leq n,\ 1 \leq k \leq i$.

Le prime due righe sono ($i = 1, 2$):

1

1 1

Da questo punto in poi, basta applicare il seguente algoritmo: *i numeri di ogni riga si ottengono ponendo il primo uguale a 1; quindi si inserisce la sequenza che si ottiene utilizzando le coppie di numeri consecutivi della riga precedente, sommando ciascuno di tali numeri e il successivo moltiplicato per k, dove k è la posizione che gli compete nella riga di appartenenza; infine l'ultimo numero della riga è 1.*

Procedendo con tale metodo otteniamo, fino a $n = 6$:

1

1 1

1 3 1

1 7 6 1

1 15 25 10 1

1 31 90 65 15 1.

Ad esempio, il numero 90 è stato ottenuto effettuando l'operazione $15 + 3 \cdot 25$ (nella penultima riga, la posizione occupata dal 25 è la terza).

NUMERI DI BELL

Def: Il mumero di **tutte le partizioni** di un insieme avente $n \geq 1$ elementi si denota con

$$B(n)$$

e si chiama **numero di Bell** di indice n.

Vale l'ovvia relazione

$$B(n) = S(n,1) + S(n,2) + \cdots + S(n,n) = \sum_{k=1}^{n} S(n,k).$$

che permette di ricondurre il calcolo dei numeri di Bell al calcolo dei numeri di Stirling.

CONTARE LE FUNZIONI SURGETTIVE

Siano assegnati due insiemi finiti A e B, con $|A| = n \geq 1$ e $|B| = k \geq 1$. Osserviamo che se $k > n$, *non* esistono applicazioni *surgettive* $f : A \to B$.
Sappiamo infatti che per ogni funzione $f : A \to B$ vale sempre la relazione $|f(A)| \leq |A|$, per cui se f è surgettiva necessariamente $k \leq n$, poichè in tal caso $f(A) = B$.

Teorema. *Il numero delle applicazioni surgettive da un insieme A di cardinalità n in un insieme B di cardinalità k, con $1 \leq k \leq n$ è dato da*

$$S(n, k) \cdot k!$$

La dimostrazione è istruttiva perchè consiste nel tradurre l'informazione racchiusa in una funzione surgettiva in altro modo, utilizzando partizioni del suo dominio, ai cui blocchi sono assegnati opportuni "identificativi" provenienti dall'insieme di arrivo. Vediamo in cosa consiste questo cambio di linguaggio.

Per costruire una funzione surgettiva $f : A \to B$, si può procedere facendo due scelte:

Prima scelta: si fissa una partizione $\{B_1, \ldots, B_k\}$ di A con k blocchi.
Tale scelta serve a "preparare gli spazi" dove raggruppare gli elementi di A in base alle loro immagini mediante la funzione. L'idea è che elementi dello stesso blocco abbiano la stessa immagine.

Seconda scelta: si sceglie una k-pla ordinata di elementi $(b_1, \ldots, b_k)$ di elementi B tutti distinti; equivalentemente, si considera una *permutazione* degli elementi di B. Ciascun blocco B_i della partizione viene quindi etichettato con il simbolo b_i.

Fatte queste due scelte, si passa a definire la funzione $f : A \to B$ ponendo:

$$f(a) := b_i \quad \text{se } a \in B_i$$

per ogni $a \in A$.
La definizione è ben posta perchè ogni a appartiene ad uno ed un solo blocco.

Chiaramente, ogni $b \in B$ ha una preimmagine; più precisamente se $b = b_j$, esso ha come preimmagini esattamente gli oggetti di A che cadono nel blocco corrispondente B_j. Dunque la funzione $f : A \to B$ è surgettiva per costruzione.

Ci si rende subito conto che scelte diverse (della partizione e/o della permutazione) portano a costruire funzioni diverse.

Viceversa, ogni funzione surgettiva è ottenibile mediante il procedimento appena illustrato; infatti, se $f : A \to B$ è una funzione surgettiva assegnata, posto $B = \{y_1, \ldots, y_k\}$, allora possiamo costruire una una partizione di A ponendo

$$B_i := f^{-1}(y_i),$$

cioè il blocco i-mo è l'insieme di tutte le preimmagini di y_i. A tale partizione accoppiamo la permutazione $(y_1, \ldots, y_k)$.
Allora abbiamo che la funzione f da cui siamo partiti coincide esattamente con quella costruita con il procedimento descritto prima: infatti se $a \in B_i$, allora $a \in f^{-1}(y_i)$, e ciò significa proprio che $f(a) = y_i$.

In definitiva, contare le funzioni surgettive equivale a contare tutti i modi in cui possiamo effettuare le due scelte: partizione di A con k blocchi e permutazione degli elementi di B. Per il principio del prodotto, il numero di modi in cui si possono fare entrambe le scelte è $S(n, k) \cdot k!$.

PARTIZIONI E RELAZIONI

Stabiliremo ora che una partizione P di un insieme A determina canonicamente un modo per mettere in relazione elementi di A. Più precisamente, P determina una relazione $\mathcal{R}$ che gode di tre proprietà fondamentali, discusse qui di seguito. **Def:** Sia

P una partizione dell'insieme non vuoto A. Si chiama **relazione di equivalenza associata a** P (o determinata da P), la relazione $\mathcal{R}$ così definita:

$$a\mathcal{R}b \iff a \text{ e } b \text{ appartengono allo stesso blocco di } P.$$

Es: Consideriamo la partizione $P = \{\{1,3\},\{4\},\{7,9,10\},\{2,5\},\{6,7\},\{8\}\}$ di I_{10}. Allora abbiamo ad esempio che $1\mathcal{R}3$, $7\mathcal{R}10$, ma $5\not\mathcal{R}7$. Gli elementi 4 e 8 sono in relazione solo con se stessi.

La relazione $\mathcal{R}$ appena introdotta ha le seguenti proprietà rilevanti, valide per ogni a, b, c elementi di A:

1) $a\mathcal{R}a$ (riflessività).

2) Se $a\mathcal{R}b$, allora si ha anche $b\mathcal{R}a$ (simmetria).

3) Se $a\mathcal{R}b$ e $b\mathcal{R}c$, allora è vero anche che $a\mathcal{R}c$ (transitività).

1) e 2) sono evidenti; per quel che riguarda 3), se $a\mathcal{R}b$ e $b\mathcal{R}c$, allora a e b sono nello stesso blocco di P, e lo stesso vale per b e c; ma il blocco che contiene b è univocamente determinato, pertanto deve trattarsi dello stesso blocco per entrambe le coppie; in particolare a e c sono nello stesso blocco e quindi è vero che $a\mathcal{R}c$.

Nel prossimo paragrafo studiamo la classe delle relazioni che hanno tali proprietà (*relazioni di equivalenza*). Stabiliremo successivamente che in realtà la nozione di partizione e quella di relazione di equivalenza sono equivalenti.

RELAZIONI DI EQUIVALENZA

Def: Una relazione $\mathcal{R}$ su un insieme A si dice *relazione di equivalenza* se ha le seguenti proprietà:

- *riflessività:* per ogni $a \in A$ si ha $a \mathcal{R} a$;
- *simmetria:* per ogni $a, b \in A$, se $a \mathcal{R} b$ allora è vero anche $b \mathcal{R} a$;
- *transitività:* per ogni $a, b, c \in A$, se $a \mathcal{R} b$ e $b \mathcal{R} c$, allora si ha anche $a \mathcal{R} c$.

Il più basilare esempio di relazione di equivalenza è la relazione $=$ di uguaglianza.

Nel prossimo paragrafo discutiamo una famiglia di esempi fondamentali di relazioni di equivalenza su $\mathbb{Z}$, che saranno oggetto di studio sistematico nello sviluppo dell'aritmetica.

RELAZIONI DI CONGRUENZA IN $\mathbb{Z}$

Richiamiamo il seguente concetto basilare di aritmetica:

Definizione. Dati due interi a e b, si dice che b *divide* a e si scrive

$$b|a$$

se esiste un numero intero q tale che

$$a = bq.$$

Se $b|a$, si dice anche che a è *un multiplo* di b oppure che a è divisibile per b. Se b non divide a, si usa la notazione

$$b \not| a.$$

Ad esempio, abbiamo $3|48$, avendosi $48 = 3 \cdot 16$, ma anche $-3|48$ perchè $48 = (-3)(-16)$.
Si osservi anche che:

• 0 è l'unico intero divisibile per *ogni* altro intero;

• 1 e -1 sono gli unici interi che dividono *ogni* altro intero.

• 0 divide solo se stesso.

La relazione $|$ così definita su $\mathbb{Z}$ è riflessiva (è sempre vero che $a|a$), ed è transitiva. Infatti, se $a|b$ e $b|c$, allora $b = ah$ e $c = bk$ per opportuni interi h, k, e quindi $c = a(hk)$, per cui si ha $a|c$.
Non vale la proprietà di simmetria, perchè ad esempio, mentre è sempre vero che $1|a$, risulta $a|1$ solo se $a = \pm 1$.

Def: Fissato un intero $n > 0$, diciamo che due interi $a, b \in \mathbb{Z}$ sono *congrui modulo* n e scriviamo

$$a \equiv_n b$$

se

$$n|(a - b),$$

ovvero se $a - b$ è multiplo di n.

Abbiamo così una relazione $\equiv_n$ su $\mathbb{Z}$, detta **relazione di congruenza modulo** n.

Es: Abbiamo ad esempio $20 \equiv_3 2$, $7 \equiv_2 -7$.

Verifichiamo che, qualunque sia n, la relazione di congruenza $\equiv_n$ è una relazione di equivalenza su $\mathbb{Z}$.

Riflessività: per ogni $a \in \mathbb{Z}$ abbiamo $a \equiv_n a$ perchè $a - a = 0$.

Simmetria: se $a \equiv_n b$, allora $a - b = nh$, da cui $b - a = n(-h)$, e ciò prova che $b \equiv_n a$.

Transitività: supposto $a \equiv_n b$ e $b \equiv_n c$, allora si ha:

$$a - b = nh,\ b - c = nk$$

per opportuni $h, k \in \mathbb{Z}$. Sommando membro a membro ricaviamo

$$a - c = n(h + k)$$

e questo garantisce che $a \equiv_n c$.

CLASSI DI EQUIVALENZA

Sia assegnata una relazione di equivalenza su un insieme non vuoto A.

Definizione: Per ogni elemento $a \in A$, si dice *classe di equivalenza* di a rispetto ad $\mathcal{R}$ l'insieme, denotato con $[a]_{\mathcal{R}}$, di **tutti** gli elementi di A che sono in relazione con a:

$$[a]_{\mathcal{R}} := \{\, b \in A \mid a \,\mathcal{R}\, b \,\}.$$

Spesso si sottintende $\mathcal{R}$ e si scrive $[a]$ in luogo di $[a]_{\mathcal{R}}$.

Osservazione importante: Per la proprietà **riflessiva**, $[a]_{\mathcal{R}}$ contiene sempre l'elemento a stesso!

Fatto importante:

Per ogni $a, b \in A$: $a \,\mathcal{R}\, b$ se e solo se $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.

Per dimostrarlo, supponiamo dapprima che $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ e proviamo che $a \,\mathcal{R}\, b$.
Infatti, dal fatto che $a \in [a]_{\mathcal{R}}$ segue per ipotesi che $a \in [b]_{\mathcal{R}}$; pertanto $a \,\mathcal{R}\, b$.

Ora, supponiamo che $a \,\mathcal{R}\, b$ e proviamo che $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.
Infatti, gli insiemi $[a]_{\mathcal{R}}$ e $[b]_{\mathcal{R}}$ hanno gli stessi elementi, perchè per la proprietà transitiva abbiamo, qualunque sia c:

$$c \in [a]_{\mathcal{R}} \iff c \,\mathcal{R}\, a \iff c \,\mathcal{R}\, b \iff c \in [b]_{\mathcal{R}}.$$

Es: Consideriamo la relazione di congruenza modulo 2 su $\mathbb{Z}$. Abbiamo che ogni intero pari $2n$ è congruente a 0: $2n \equiv_2 0$, mentre ogni numero dispari $2n+1$ è congruente a 1: infatti $(2n+1) - 1 = 2n$.
La classe di un numero a si denota con $[a]_2$ (piuttosto che con $[a]_{\equiv_2}$).

Risulta quindi che $[0]_2$ e $[1]_2$ sono rispettivamente l'insieme dei numeri pari e l'insieme dei numeri dispari. Esse sono le uniche classi di equivalenza modulo 2.

CONFRONTO TRA PARTIZIONI E RELAZIONI DI EQUIVALENZA

Teorema: *Sia $\mathcal{R}$ una relazione di equivalenza sull'insieme non vuoto A. Allora l'insieme di tutte le classi di equivalenza:*

$$\{[a]_{\mathcal{R}} |\, a \in A\} \subset \mathcal{P}(A)$$

costituisce una partizione di A.
Tale insieme si chiama **quoziente di A modulo la relazione $\mathcal{R}$** *e si denota con il simbolo*

$$A/\mathcal{R}.$$

Infatti, ogni classe $[a]_{\mathcal{R}}$ è un insieme non vuoto, perchè contiene a. Mostriamo che $[a]_{\mathcal{R}}$ è l'unica classe di equivalenza a cui a appartiene: se $[b]_{\mathcal{R}}$ è una classe per cui $a \in [b]_{\mathcal{R}}$, allora $a\,\mathcal{R}\,b$, ma ciò garantisce per quanto visto sopra che $[b]_{\mathcal{R}} = [a]_{\mathcal{R}}$. Quindi ogni a appartiene ad una ed una sola classe di equivalenza.

Abbiamo ad esempio che l'insieme quoziente $\mathbb{Z}/\equiv_2$ è costituito da due soli elementi:

$$\mathbb{Z}/\equiv_2 = \{[0]_2, [1]_2\} = \{P, D\}$$

dove $P = \{2n |\, n \in \mathbb{Z}\} = [0]_2$ è l'insieme degli interi pari, mentre $D = \{2n+1 |\, n \in \mathbb{Z}\} = [1]_2$ è l'insieme degli interi dispari.

Teorema: *Dato un insieme non vuoto A, vi è una corrispondenza biunivoca tra partizioni di A e relazioni di equivalenza su A. Essa è data da*

$$P \mapsto \mathcal{R}_P$$

dove $\mathcal{R}_P$ denota la relazione di equivalenza associata a P.
L'inversa di questa bigezione è:

$$\mathcal{R} \mapsto A/\mathcal{R}.$$

Dimostrazione del Teorema. Proviamo che la funzione

$$P \mapsto \mathcal{R}_P$$

tra l'insieme delle partizioni di A e l'insieme delle relazioni di equivalenza è bigettiva, mostrando che ogni relazione di equivalenza $\mathcal{R}$ ha esattamente una preimmagine, data dalla partizione $A/\mathcal{R}$. Ricordiamo che, per definizione, i blocchi di $A/\mathcal{R}$ sono tutte le classi di equivalenza relative a $\mathcal{R}$.

Posto $P = A/\mathcal{R}$, si tratta quindi di verificare che

$$\mathcal{R} = \mathcal{R}_P.$$

Infatti, abbiamo $a \mathcal{R} b$ se e solo se $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$, ma ciò significa che a e b sono nello stesso blocco di $A/\mathcal{R}$ e quindi ciò equivalente a dire che $a \mathcal{R}_P b$.

Proviamo infine che la preimmagine di $\mathcal{R}$ è unica; supponiamo che Q sia un'altra partizione di A per la quale

$$\mathcal{R}_Q = \mathcal{R}.$$

Vogliamo provare che necessariamente $Q = A/\mathcal{R}$. Si tratta quindi di far vedere che ogni blocco $B \in Q$ è una classe di equivalenza rispetto a $\mathcal{R}$ e che, viceversa, ogni classe è un blocco di Q.

Dato un tale blocco B, fissiamo un suo elemento $a \in B$ (ricordiamo che $B \neq \emptyset$). Allora risulta:

$$B = [a]_{\mathcal{R}}$$

perchè per ogni b:

$$b \in B \iff b \mathcal{R}_Q a \iff b \mathcal{R} a \iff b \in [a]_{\mathcal{R}}.$$

Resta provato che ogni blocco è una classe di equivalenza. Viceversa, data una classe $[a]_{\mathcal{R}}$, detto B l'unico blocco di Q a cui a appartiene, quanto appena dimostrato dice che

$$B = [a]_{\mathcal{R}},$$

pertanto è anche vero che ogni classe di equivalenza è un blocco di Q.

DIVISIONE TRA INTERI

Proposizione: *Siano a e b due interi. Se $a|b$ e $b|a$, allora $b = \pm a$.*

Dimostrazione: Siano a e b tali che $a|b$ e $b|a$. Osserviamo che se $a = 0$, l'unica possibilità compatibile con l'ipotesi è che anche $b = 0$. Quindi in tal caso $a = b = 0$. Consideriamo quindi il caso in cui $a \neq 0$. Per ipotesi, esistono due interi q e q' tali che

$$b = qa \text{ e } a = q'b.$$

Da queste relazioni segue che

$$a = q'b = q'(qa) = (q'q)a.$$

Poiché $a \neq 0$ è necessariamente

$$q'q = 1$$

e quindi $q = q' = 1$ oppure $q = q' = -1$.

Nel primo caso concludiamo che $a = b$, mentre nel secondo caso otteniamo che $b = -a$.

Teorema (Divisione Euclidea) *Siano a e b elementi di $\mathbb{Z}$ con $b \neq 0$. Esistono e sono univocamente determinati due interi q ed r tali che*

$$a = qb + r \;\; e \;\; 0 \leq r < |b|.$$

Gli interi q ed r sono detti rispettivamente il **quoziente** *ed il* **resto** *della divisione di a per b.*

Ricordiamo che il *valore assoluto* $|a|$ di un numero intero a è il mumero intero *positivo* definito nel modo seguente:

$$|a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0. \end{cases}$$

DIMOSTRAZIONE DELL'ESISTENZA DEL QUOZIENTE E DEL RESTO

Esaminiamo prima il caso $a \geq 0, b > 0$*:*

• Se a è multiplo di b allora

$$a = qb \quad \text{con} \quad q \in \mathbb{N}.$$

Il quoziente è q ed il resto è 0.

• Se a *non* è multiplo di b allora sia q il più **grande** numero naturale tale che $qb < a$. Tale numero esiste grazie al Principio del Minimo: se si considera infatti

$$A := \{q' \in \mathbb{N} | \, q'b > a\},$$

, allora tale insieme è non vuoto (ad es. $2a \in A$); considerato il minimo q' di A, allora $q = q' - 1$ è il più grande numero tale che $qb < a$.

Abbiamo quindi, con questa scelta di q, che:

$$qb < a < (q+1)\, b \qquad (*)$$

Poniamo

$$r := a - qb.$$

Quindi

$$a = qb + r.$$

La prima delle disuguaglianze (*) dà

$$r > 0.$$

La seconda delle disuguaglianze (*) dà:

$$r < b.$$

DIMOSTRAZIONE DELL'ESISTENZA DEL QUOZIENTE E DEL RESTO

Caso generale:

Sappiamo che

$$|a| = q|b| + r \text{ con } 0 \leq r < |b|.$$

Se $a \geq 0$*:*

$$a = q|b| + r \text{ con } 0 \leq r < |b|.$$

che possiamo riscrivere

$$a = (\pm 1)qb + r.$$

Il quoziente che si ottiene è $\pm q$ a seconda del segno di b.
Il resto è sempre r.

Se $a < 0$:

$$-a = q|b| + r \text{ con } 0 \leq r < |b|.$$

da cui

$$a = (-q)\,|b| - r.$$

Aggiungendo e sottraendo $|b|$:

$$a = (-q)\,|b| - |b| + |b| - r.$$

Poniamo

$$r' := |b| - r$$

e otteniamo:

$$a = (-q - 1)\,|b| + r'.$$

Quindi in definitiva:

$$a = \mp(q+1)\,b + r' \quad \text{ con } 0 \leq r' < |b|.$$

Il quoziente è $\mp(q+1)$ a seconda del segno di b, mentre il resto ottenuto è $r' = |b| - r$.

UNICITÀ DEL QUOZIENTE E DEL RESTO

Supponiamo che si possa scrivere

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

e anche

$$a = q'b + r',\ 0 \leq r' < |b|$$

in corrispondenza di due coppie di interi (q, r) e (q', r'). Vogliamo provare che necessariamente

$$q = q',\ r = r'.$$

Possiamo supporre ad esempio $r' \geq r$. Sottraendo membro a membro le uguaglianze precedenti:

$$0 = (q - q')b + r - r'$$

ovvero

$$(q - q')b = r' - r. \qquad (*)$$

Prendendo i valori assoluti :

$$|q - q'||b| = |r' - r| = r' - r \leq r' < |b|.$$

Da qui segue:

$$|q - q'| < 1$$

e quindi, essendo $|q - q'|$ un numero naturale, necessariamente $q - q' = 0$, ovvero $q = q'$. Sostituendo nella (*) segue anche $r = r'$.

REGOLA PRATICA PER IL CALCOLO DEL RESTO

Siano $a, b \in \mathbb{Z}$ interi fissati con $b \neq 0$.

Dalla dimostrazione discussa sopra, ricaviamo la seguente regola pratica, che dice come ottenere il resto della divisione di a per b, in funzione del resto della divisione dei corrispondenti valori assoluti $|a|$ e $|b|$: quest'ultimo è quello che sappiamo calcolare col metodo elementare di divisione imparato a scuola.

Detto r il resto della divisione di $|a|$ per $|b|$, abbiamo che il resto della divisione di a per b è dato da:

- r, se $a \geq 0$.

- $|b| - r$, se $a < 0$.

MASSIMO COMUN DIVISORE

Definizione. Si dice *divisore comune* di due interi a e b ogni intero $c \in \mathbb{Z}$ tale che

$$c|a \text{ e } c|b.$$

Definizione. Siano a e b elementi di $\mathbb{Z}$. Si dice *massimo comun divisore* di a e b ogni intero d che soddisfi le condizioni seguenti:

i) d è divisore comune di a e b.

ii) Se d' è un divisore comune di a e b, allora $d'|d$.

In altri termini, un massimo comune divisore è ogni divisore comune di a e b che è *multiplo* di *tutti* gli altri divisori comuni.

Proposizione *Siano a e b interi. Allora se d è un MCD tra a e b, allora è anche un MCD tra $-a$ e b.*

Dimostrazione: Infatti, un qualunque intero c è divisore comune di a e b se e solo se è divisore comune di $-a$ e b. Poichè la definizione di massimo comum divisore dipende solo dall'insieme dei divisori comuni della coppia di numeri considerati, segue la tesi.

Conseguenza: *Nel determinare un MCD tra due interi, li si può sempre supporre* **entrambi positivi** *(a meno di sostituirli con i valori assoluti).*

Si pongono ora le seguenti questioni:
• dati $a, b \in \mathbb{Z}$, esiste un loro MCD?
• Quanti MCD tra a e b vi sono?

Risposta alla seconda domanda:

Teorema: *Siano a e b interi e sia d un loro massimo comune divisore. Allora oltre d vi è solo un altro massimo comune divisore tra a e b, che è $-d$.*

Dimostrazione: Sia d un MCD tra a e b. È immediato verificare che anche $-d$ è un massimo comune divisore. Si tratta di provare che non ve ne sono altri. Infatti, sia d' un altro MCD; applicando la proprietà ii) di d:

$$d'|d.$$

D'altra parte, applicando la stessa proprietà di d':

$$d|d'.$$

Concludiamo che $d' = \pm d$.

Conseguenza: per due qualunque elementi a e b di $\mathbb{Z}$, si può parlare in generale di "un massimo comun divisore" e non "del massimo comun divisore". Dicendo *il* " massimo comun divisore" di a e b si intenderà quello *positivo*.
Il massimo comun divisore **positivo** verrà denotato d'ora in poi con il simbolo:

$$MCD(a, b).$$

Teorema (Esistenza del massimo comun divisore) *Siano a e b numeri interi. Allora esiste il massimo comun divisore $MCD(a,b)$. un massimo comun divisore di a e b. Inoltre, posto $d = MCD(a,b)$ esistono due interi s e t tali che*

$$d = sa + tb. \tag{1}$$

Un'espressione del tipo (1) che esprime il Massimo Comun Divisore come combinazione lineare dei due interi coinvolti si chiama *identità di Bézout*.

Osservazione. Se $a = b = 0$ allora l'unico MCD è 0.

Per questo motivo, *tratteremo il caso in cui a e b non sono entrambi nulli*. In tal caso 0 non è mai MCD tra a e b. Possiamo limitarci poi al caso $a \geq 0$ e $b \geq 0$.

La dimostrazione consiste nell'*algoritmo di Euclide*, che fornisce un metodo efficiente per il calcolo di $MCD(a,b)$; esso è basato sui fatti seguenti:

A) Se $b = 0$, allora $MCD(a,0) = a$.

B) Se $b \neq 0$, si ha

$$MCD(a,b) = MCD(b,r)$$

dove

$$r = \textbf{resto} \text{ della divisione di } a \text{ per } b.$$

Questa uguaglianza va intesa: se esiste il $MCD(b,r)$ allora esso è anche il MCD tra a e b.

Queste osservazioni comportano che ci si può sempre ricondurre, dopo un numero finito di passi, al caso A), sostituendo, se occorre, la coppia (a,b) con la coppia (b,r), e quindi ripetendo questa sostituzione fino a che il secondo numero della coppia, che diventa sempre più piccolo, è zero.

Si eseguono cioè le seguenti divisioni successive:

$$\begin{array}{lll} & a = bq + r & 0 \leq r < b \\ \text{se } r \neq 0: & b = rq_1 + r_1 & 0 \leq r_1 < r \\ \text{se } r_1 \neq 0: & r = r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ \text{se } r_2 \neq 0: & r_1 = r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \\ & \vdots & \\ \text{se } r_{i+1} \neq 0 & r_i = r_{i+1} q_{i+2} + r_{i+2} & 0 \leq r_{i+2} < r_{i+1} \\ & \vdots & \end{array}$$

La successione **termina** quando si determina un **resto nullo**. Notiamo che:

• la successione delle divisioni deve terminare dopo un **numero finito** di passi.

• • L'ultimo resto **non nullo** è il $MCD(a, b)$.

Dimostrazione di •

Supponiamo per assurdo che tutte le divisioni abbiano un resto r_i non nullo; per costruzione tali resti formerebbero una successione di interi naturali, compresi tra 0 e b, tali che:

$$b > r > r_1 > r_2 > \cdots > r_i > r_{i+1} > \cdots$$

Ciò è impossibile, perchè, posto $r_0 := r$, avremmo una funzione ingettiva $i \mapsto r_i$ da $\mathbb{N}$ nell'insieme finito $\{x \in \mathbb{N} | 0 < x < b\}$.

La dimostrazione di •• è basata sull'uso ripetuto della proprietà fondamentale B) ed infine della A). Detto r_{i+1} il primo resto nullo abbiamo:

$$MCD(a, b) = MCD(b, r) = MCD(r, r_1) = MCD(r_1, r_2) = \cdots = MCD(r_i, r_{i+1}) = r_i.$$

Dimostrazione dell'identità di Bèzout.

Per costruzione r è combinazione lineare di a e b:

$$r = a - qb;$$

d'altra parte, r_1 è combinazione lineare di b e di r; segue che anche r_1 è combinazione lineare di a e b:

$$r_1 = b - rq_1 = b - (a - qb)q_1 = -q_1 a + (qq_1 + 1)b.$$

In generale, ciascun resto r_i, $i \geq 2$ è una combinazione lineare dei **due resti precedenti** r_{i-1} e r_{i-2}.

Questo comporta che ciascun resto è a sua volta combinazione lineare di a e b.

In particolare ciò vale per l'ultimo resto non nullo che è il nostro $MCD(a, b)$.

Per completare la giustificazione dell'algoritmo, resta da spiegare la proprietà B) di cui sopra:

$$MCD(a, b) = MCD(b, r)$$

dove r è il resto della divisione di a per b (assumendo $b \neq 0$).
Risulta che l'insieme $\mathcal{D}(a, b)$ dei divisori comuni di a e b coincide esattamente con l'insieme $\mathcal{D}(q, r)$ dei divisori comuni di b e r.

Infatti, se $d \in \mathcal{D}(a, b)$, allora $d|b$, ma d è anche divisore di r, perchè $r = a - qb$ è una combinazione lineare di a e di b. Quindi $d \in \mathcal{D}(b, r)$.
Analogamente, se $d \in \mathcal{D}(b, r)$, allora $d|b$, ma si ha pure $d|a$ perchè $a = qb + r$ è combinazione lineare di b e di r.

Pertanto, se esiste il $MCD(b, r)$, allora lo stesso numero soddisfa banalmente le condizioni richieste nella definizione per essere massimo comun divisore anche di a e b, perchè tali condizioni sono formulate esclusivamente coinvolgendo l'insieme dei divisori comuni dei due numeri coinvolti.

Esempio: Determiniamo il massimo comun divisore d tra 212 e 148 ed una identità di Bézout

$$d = s(212) + t(148), \quad s, t \in \mathbb{Z}.$$

Applicando l'algoritmo di Euclide, si ottiene la seguente sequenza di 4 divisioni:

$$\begin{array}{rcrcr} 212 & = & 1 \cdot 148 & + & 64 \\ 148 & = & 2 \cdot 64 & + & 20 \\ 64 & = & 3 \cdot 20 & + & 4 \\ 20 & = & 5 \cdot 4 & + & 0 \end{array}$$

Si ha quindi $d = 4$ (ultimo resto non nullo). Ricavando ora i resti:

$$64 = 212 - 148$$

$$20 = (148) - 2 \cdot 64 = (148) - 2 \cdot (212 - 148) = 3 \cdot (148) - 2 \cdot (212)$$

$$\begin{aligned} 4 &= 64 - 3 \cdot 20 = 212 - 148 - 3\,(3 \cdot 148 - 2 \cdot (212)) = \\ &= 7 \cdot 212 + (-10) \cdot 148. \end{aligned}$$

e quindi

$$4 = 7 \cdot (212) + (-10) \cdot 148.$$

che è l'identità voluta (con $s = 7$ e $t = -10$.)

NUMERI PRIMI TRA LORO

Def. Due numeri interi $a, b \in \mathbb{Z}$ si dicono **primi tra loro** se

$$MCD(a, b) = 1.$$

Vale la seguente caratterizzazione importante:

Prop: *Due numeri interi a, b sono primi tra loro se e solo se 1 è combinazione lineare di essi, ovvero se e solo se esistono due interi $s, t \in \mathbb{Z}$ tali che*

$$1 = sa + tb. \qquad (*)$$

Infatti, se $MCD(a, b) = 1$, allora l'identità di Bèzout dà direttamente (*). Viceversa, se vale (*) per opportuni interi s, t, allora ogni divisore comune d di a e b divide anche $sa + tb$, quindi $d|1$. Ciò significa che 1 soddisfa le condizioni richieste dalla definizione per essere massimo comune divisore di a e b.

Osservazione utile: *Siano a e b interi non entrambi nulli. Posto $d = MCD(a, b)$, allora gli interi*

$$\bar{a} := \frac{a}{d} \quad e \quad \bar{b} := \frac{b}{d}$$

sono primi tra loro.

Basta osservare che, dall'identità di Bèzout:

$$d = sa + tb$$

si ricava, dividendo ambo i membri per d:

$$1 = s\frac{a}{d} + t\frac{b}{d} = s\bar{a} + t\bar{b}.$$

EQUAZIONI DIOFANTEE

Si chiama **equazione diofantea lineare** un'equazione della forma

$$ax + by = c \tag{1}$$

dove a, b, c sono tutti numeri interi, $(a, b) \neq (0, 0)$, e le incognite x, y sono anch'esse numeri **interi**.

Def: Una soluzione di (1) è ogni coppia $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ di numeri interi tale che

$$ax_0 + by_0 = c.$$

Teorema: *L'equazione diofantea*

$$ax + by = c$$

ha almeno una soluzione se e solo se

$$MCD(a, b)|c.$$

In tal caso, vi sono infinite soluzioni.

Precisamente, posto $d = MCD(a, b)$*, se* (x_o, y_o) *è una soluzione qualsiasi, allora tutte le soluzioni sono*

$$(x_o + \frac{b}{d}t,\ y_o - \frac{a}{d}t)$$

al variare di $t \in \mathbb{Z}$.

METODO RISOLUTIVO PER LE EQUAZIONI DIOFANTEE LINEARI

Per risolvere l'equazione

$$ax + by = c \tag{1}$$

nell'ipotesi $MCD(a, b)|c$, si determina un'indentità di Bézout

$$d = sa + tb \tag{$*$}$$

per $d = MCD(a, b)$.

Stante l'ipotesi abbiamo

$$c = kd$$

per un opportuno $k \in \mathbb{Z}$ (quoziente della divisione di c per d).

Si moltiplicano allora ambo i membri di (*) per k:

$$c = (sk)a + (tk)b$$

e si ottiene la soluzione

$$(sk, tk).$$

Esempio: Risolvere l'equazione diofantea:

$$7x + 11y = 3$$

Determinare inoltre una soluzione (x, y) con $y < 0$.

Applicando l'algoritmo euclideo:

$$\begin{array}{rcl} 11 & = & 1 \cdot 7 \ +4 \\ 7 & = & 1 \cdot 4 \ + \ 3 \\ 4 & = & 1 \cdot 3 \ + \ 1 \\ 3 & = & 1 \cdot 3 \ +0 \end{array}$$

otteniamo $d = MCD(7, 11) = 1$ e quindi l'equazione ha soluzioni.

Ricaviamo l'identità di Bèzout:

$$\begin{array}{ll} 4 & = 11 - 7 \\ 3 & = 7 - 4 = 7 - (11 - 7) = (2)7 - 11 \\ 1 & = 4 - 3 = (11 - 7) - (2 \cdot 7 - 11) = 2 \cdot 11 - 3 \cdot 7 \end{array}$$

$$1 = 2 \cdot 11 - 3 \cdot 7$$

Dall'identità di Bèzout, moltiplicando per 3:

$$3 = -9(7) + 6(11)$$

per cui una soluzione è $(-9, 6)$. Tutte le soluzioni sono

$$(-9 + 11t, 6 - 7t)$$

al variare di $t \in \mathbb{Z}$. Per $t = 1$ (ad es.) otteniamo la soluzione $(2, -1)$ la cui seconda coordinata è negativa, come richiesto.

Ai fini di dimostrare il Teorema precedente sulle equazioni Diofantee, discutiamo la seguente proprietà dei numeri primi tra loro:

Proposizione: *Siano* $a, b, c \in \mathbb{Z}$ *e si supponga che*

$$a|bc.$$

Se a *e* b *sono primi tra loro, allora si ha necessariamente che*

$$a|c.$$

Dimostrazione: assunto che a e b siano primi tra loro, basta provare che c è combinazione lineare di a e di bc.

Infatti, utilizzando l'identità di Bèzout abbiamo che

$$1 = sa + tb$$

per opportuni $s, t \in \mathbb{Z}$; motiplicando per c ambo i membri:

$$c = s(ac) + t(bc) = (sc)a + t(bc).$$

Ciò premesso, consideriamo l'equazione diofantea:

$$ax + by = c$$

e poniamo $d := MCD(a, b)$. Se l'equazione ammette soluzione, allora c è combinazione lineare di a e b e quindi deve aversi $d|c$, in quanto d divide sia a che b.
Viceversa, supponiamo che $d|c$. Allora come abbiamo visto in precedenza, esponendo il metodo risolutivo, sfruttando l'identità di Bèzout si ricavache l'equazione ha almeno una soluzione.
Infine, fissata una soluzione (x_o, y_o), determiniamo tutte le altre; se (x, y) è una soluzione qualsiasi, allora deve aversi

$$a(x - x_o) + b(y - y_o) = 0$$

da cui

$$a(x - x_o) = b(y_o - y)$$

e quindi anche, dividendo ambo i membri per d:

$$\frac{a}{d}(x - x_o) = \frac{b}{d}(y_o - y). \qquad (*)$$

In particolare, segue che

$$\frac{a}{d} \mid \frac{b}{d}(y_o - y).$$

Siccome $\frac{a}{d}$ e $\frac{b}{d}$ sono primi tra loro, deduciamo (usando la Proposizione precedente) che

$$\frac{a}{d}|(y_o - y).$$

Dunque esiste $t \in \mathbb{Z}$ tale che

$$y_o - y = \frac{a}{d}t,$$

ovvero

$$y = y_o - \frac{a}{d}t.$$

Sostituendo infine tale relazione nella (*) si ricava subito che

$$x = x_o + \frac{b}{d}t.$$

PROPRIETÀ FONDAMENTALI DELLE CONGRUENZE

Sia n un fissato intero positivo.
Abbiamo già introdotto la relazione $\equiv_n$ di congruenza modulo n su $\mathbb{Z}$, che è una relazione di equivalenza. Ricordiamo che $a \equiv_n b$ per definizione significa che $a - b$ è un multiplo di n.

Se $a \equiv_n b$, si scriverà anche

$$a \equiv b \pmod{n}.$$

Risulta che alcune fondamentali proprietà aritmetiche valgono anche se al posto della usuale relazione di uguaglianza si considera la relazione $\equiv_n$. Infatti abbiamo:

Proposizione: *Per ogni $a, b, c, d \in \mathbb{Z}$, se si ha:*

$$a \equiv_n b, \quad c \equiv_n d,$$

allora risulta anche:

$$a + c \equiv_n b + d,$$
$$a \cdot c \equiv_n b \cdot d.$$

La dimostrazione è molto semplice; ad esempio, supposto $a \equiv_n b, \quad c \equiv_n d$, allora $a = b + hn$ e $c = d + kn$ per opportuni $h, k \in \mathbb{Z}$. Quindi

$$ac = (b + hn)(d + kn) = bd + (kb + dh)n + n^2$$

e quindi $ac - bd$ è anch'esso multiplo di n, e si è verificato che $a \cdot c \equiv_n b \cdot d$.

Conseguenza importante: In un'espressione della forma

$$a_1 x_1^{h_1} + a_2 x_2^{h_2} + \cdots + a_k x_k^{h_k} \equiv b \pmod{n}$$

dove $h_1, \ldots, h_k \in \mathbb{N}$, è lecito **sostituire** ciascuno dei numeri x_i, a_i oppure b con un numero **ad esso congruo** modulo n.

Esempio: Ogni intero è congruo **modulo 3** alla somma delle sue cifre.
Ad esempio:

$$1317 \equiv_3 (1 + 3 + 1 + 7).$$

Questa affermazione si può giustificare come applicazione del fatto che:

$$10 \equiv_3 1.$$

Infatti, considerato un intero a, e posto:

$$a = a_o + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k$$

cioè assumendo che a abbia $k+1$ cifre decimali, allora abbiamo:

$$a \equiv_3 a_o + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k.$$

Ora, in base a quanto stabilito, possiamo sostituire 1 al posto di 10, ricavando:

$$a \equiv_3 a_o + a_1 + a_2 + \cdots + a_k.$$

Questo fatto fornisce una dimostrazione del **criterio di divisibilità per** 3:
Un numero $a \in \mathbb{Z}$ è divisibile per 3 se e solo se lo è la somma delle sue cifre.

Infatti, notiamo che, in generale, qualsiasi sia $n > 0$, che

$$n|a \text{ se e solo se } a \equiv_n 0.$$

Quindi, essendo a e le somma s delle sue cifre congrui modulo 3, il primo è divisibile per 3 se e solo se lo è il secondo, in quanto $\equiv_3$ è una relazione di equivalenza!

In modo analogo si possono ricavare i noti criteri di divisibilità per 2 e per 5. Nel caso di 11, si può sfruttare il fatto che

$$10 \equiv_{11} -1.$$

Come sopra, sostituendo -1 al posto di 10 nella relazione

$$a \equiv_{11} a_o + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,$$

avremo stavolta che

$$a \equiv_{11} a_o - a_1 + a_2 - \cdots\cdots + (-1)^k a_k.$$

Dunque un numero a è divisibile per 11 se e solo se lo è la somma a segni alterni delle sue cifre (partendo dalle unità con segno +).

CLASSI RESTO

Teorema: *Ogni intero a è congruo modulo n ad uno ed un solo dei numeri*

$$0, 1, 2, \ldots, n-1.$$

Tale numero è il resto della divisione di a per n.

Infatti, consideriamo il quoziente ed il resto della divisione euclidea di a per n, di modo che

$$a = qb + r, \quad 0 \leq r < n.$$

Dunque $a - r = qb$ e ciò garantisce che $a \equiv_n r$. Se r' fosse un altro numero con verificante le condizioni:

$$a \equiv_n r', \quad 0 \leq r' \leq n-1$$

allora avremmo

$$a - r' = q'n$$

per un certo $q' \in \mathbb{Z}$, ma allora

$$a = q'n + r'.$$

Per l'unicità del quoziente e del resto, seguirebbe in particolare che $r' = r$.

Conseguenza: I numeri $0, 1, \ldots, n-1$ sono tutti sempre a due a due incongrui (cioè non congrui) modulo n.

Def: Fissato un intero positivo n, e $a \in \mathbb{Z}$, la classe di equivalenza di a rispetto alla relazione $\equiv_n$ di congruenza modulo n, si denoterà con

$$[a]_n.$$

Ricordiamo che tale classe è costituita, per definizione, da tutti e soli i numeri in relazione con a rispetto alla relazione $\equiv_n$; dunque si tratta dell'insieme:

$$[a]_n = \{a + kn|,\ k \in \mathbb{Z}\}.$$

Tale classe di equivalenza è detta una *classe resto modulo n*.

Def: L'insieme quoziente $\mathbb{Z}/_{\equiv_n}$ si denota con

$$\mathbb{Z}_n$$

e si chiama **insieme delle classi resto modulo** n.

Corollario: *Per ogni intero $n > 0$, l'insieme $\mathbb{Z}_n$ ha esattamente n elementi:*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}.$$

Infatti, basta ricordare che due numeri a, b sono congrui modulo n se e solo se

$$[a]_n = [b]_n,$$

e in base al Teorema precedente ogni numero a appartiene soltanto alla classe $[r]_n$ dove r è il resto della divisione di a per n. La classe resto $[r]_n$ è una sola delle classi $[0]_n, [1]_n, \cdots, [n-1]_n$.

LEGGE DI CANCELLAZIONE

Notiamo che la proprietà di *cancellazione* valida in $\mathbb{Z}$:

$$\text{se} \quad a \cdot c = b \cdot c \ \text{ e } \ c \neq 0, \ \text{allora } a = b$$

non ha un perfetto analogo se sostituiamo $\equiv_n$ al posto dell'uguaglianza. Ad esempio nella relazione

$$3 \cdot 2 \equiv 4 \cdot 2 \pmod 2$$

non è lecito "semplificare il 2" in quanto **non è vero** che

$$3 \equiv 4 \pmod 2.$$

Si può dimostrare però quanto segue:

Proposizione: *Siano $a, b, c \in \mathbb{Z}$. Se*

$$a \cdot c \equiv b \cdot c \ (mod\ n)$$

ed inoltre $MCD(c, n) = 1$, allora

$$a \equiv b \ (mod\ n).$$

Dimostrazione. Per ipotesi

$$n|(a - b) \cdot c.$$

Ma n e c sono primi tra loro, e quindi per una proprietà vista in precedenza, necessariamente $n|(a - b)$.□

Es. Dalla relazione

$$148 \equiv 4 \pmod 9$$

otteniamo, "dividendo per 2":

$$74 \equiv 2 \pmod 9.$$

Questo è corretto perchè $MCD(2,9) = 1$.

Nel caso in cui $MCD(c,n) \neq 1$ è possibile semplificare la congruenza

$$ac \equiv bc \pmod n$$

a patto di **cambiarne il modulo**, utilizzando il risultato seguente più generale:

Proposizione: *Sia $n > 0$ e siano $a, b, c \in \mathbb{Z}$ tali che*

$$ac \equiv bc \ (mod\ n).$$

Allora si ha

$$a \equiv b \ (mod\ \frac{n}{d})$$

dove $d = MCD(c,n)$.

Dimostrazione. Dalla congruenza

$$ac \equiv bc \pmod n$$

si deduce subito la seguente:

$$a\,\frac{c}{d} \equiv b\,\frac{c}{d} \pmod{\frac{n}{d}}.$$

Ricordiamo ora che $MCD(\frac{c}{d}, \frac{n}{d}) = 1$ per cui a questa congruenza si può applicare la legge di cancellazione provata in precedenza. Se ne deduce quindi

$$a \equiv b \pmod{\frac{n}{d}}.\square$$

Es: Dalla congruenza

$$30 \equiv 48 \pmod 9$$

se ne deduce l'altra

$$5 \equiv 8 \pmod{\mathbf{3}}.$$

Infatti possiamo riscrivere la prima come

$$6 \cdot 5 \equiv 6 \cdot 8 \pmod 9$$

e quindi semplificare il 6, cambiando però il modulo in $3 = \frac{9}{3}$, tenendo conto che $MCD(9,6) = 3$.

CAMBIAMENTO DI MODULO

Sia $p > 0$ un intero, e sia $n = qp$ un suo multiplo, dove $q > 0$.

La proprietà seguente stabilisce che legame c'è tra le classi $[a]_p$ e $[a]_n$ dove a è un intero qualsiasi.

Proposizione: *Per ogni $a \in \mathbb{Z}$ risulta che $[a]_p$ è l'unione di esattamente q classi resto modulo n, a due a due disgiunte:*

$$[a]_p = [a]_n \cup [a+p]_n \cup [a+2p]_n \cup \cdots \cup [a+(q-1)p]_n. \qquad (*)$$

Esempi: Abbiamo

$$[5]_3 = [5]_6 \cup [5+3]_6 = [5]_6 \cup [8]_6 = [5]_6 \cup [2]_6$$

mentre

$$[2]_7 = [2]_{21} \cup [2+7]_{21} \cup [2+14]_{21} = [2]_{21} \cup [9]_{21} \cup [16]_{21}.$$

Nel primo esempio $p = 3$, $n = 6$ e $q = 2$, mentre nel secondo $p = 7$, $n = 21$ e $q = 3$.

Dimostrazione: Ogni numero x che appartenga a una delle classi $[a+hp]_n$ che figura al secondo membro dell'uguaglianza (*), dove $0 \leq h \leq q-1$, è della forma:

$$a + hp + kn, \quad k \in \mathbb{Z}$$

e quindi

$$x = a + hp + kpq = a + (h + kq)p$$

per cui $x \in [a]_p$.
Viceversa, se $x \in [a]_p$, allora dev'essere

$$x = a + kp$$

con $k \in \mathbb{Z}$; dividendo k per q, denotando con h il quoziente e r il resto, otteniamo:

$$k = hq + r,$$

e quindi possiamo riscrivere x come:

$$x = a + (hq + r)p = a + rp + hn.$$

Deduciamo che $x \in [a + rp]_n$ e, quindi, essendo $0 \leq r \leq q-1$, si conclude che x appartiene all'unione delle classi al secondo membro di (*).

Infine, resta da provare che i numeri

$$a, a+p, \cdots, a+(q-1)p$$

sono a due a due incongrui modulo n. Infatti, se

$$a + iq \equiv a + jp \pmod{n}$$

con $0 \leq i, j \leq q-1$, allora segue:

$$ip \equiv jp \pmod{n}$$

da cui, applicando la legge di cancellazione:

$$i \equiv j \pmod{\frac{n}{p}}$$

ovvero

$$i \equiv j \pmod{q}$$

e quindi necessariamente $i = j$.

CONGRUENZE LINEARI

Def: Una **congruenza lineare** è un'equazione del tipo

$$ax \equiv b \pmod{n}$$

dove $x \in \mathbb{Z}$ è l'**incognita** e $a, b, n \in \mathbb{Z}$ sono interi assegnati.
Una **soluzione** di tale equazione è ogni intero $x_o \in \mathbb{Z}$ tale che $ax_o \equiv b \pmod{n}$.

Attenzione: una congruenza lineare può **non avere** soluzioni.

Es: Questa congruenza

$$15x \equiv 4 \pmod{3}$$

non ha soluzioni perchè $15 \equiv_3 0$.

Teorema: *La congruenza lineare:*

$$ax \equiv b \pmod{n}$$

ha soluzioni se e solo se $MCD(a, n) \mid b$.

In tal caso, posto $d := MCD(a, n)$*, l'insieme* S *di tutte le soluzioni è*

$$S = [x_o]_{\frac{n}{d}} = \{x_0 + k\frac{n}{d} \mid k \in \mathbb{Z}\}.$$

In particolare, si ha che S *è unione delle seguenti* d *classi resto disgiunte modulo* n*:*

$$S = [x_0]_n \cup [x_0 + \frac{n}{d}]_n \cup [x_0 + 2\frac{n}{d}]_n \cdots \cup [x_0 + (d-1)\frac{n}{d}]_n.$$

Quindi vi sono esattamente d *soluzioni nell'insieme* $\{0, 1, \ldots, n-1\}$*, ovviamente a due a due incongrue modulo* n*, e ogni altra soluzione è congrua ad una di queste modulo* n*.*

Si riassume ciò dicendo più brevemente che la congruenza, se è risolubile, *ammette esattamente* d *soluzioni modulo* n, dove $d = MCD(a, n)$.

METODO RISOLUTIVO E DIMOSTRAZIONE DEL TEOREMA

Determinare una soluzione x_o della congruenza lineare

$$ax \equiv b \pmod{n}$$

è **equivalente** a determinare una soluzione (x_o, y_o) dell'**equazione diofantea**:

$$ax - ny = b. \qquad (*)$$

Infatti,

$$ax \equiv b \pmod{n}$$

significa che esiste un intero y tale che

$$ax - b = yn$$

ovvero

$$ax - ny = b.$$

Ora, tale equazione ha soluzione se e solo se $MCD(a, n)|b$ e questo giustifica la prima affermazione del Teorema precedente.

L'ultima affermazione nell'enunciato segue dal fatto che la soluzione generale dell'equazione diofantea (*), come sappiamo, è:

$$(x_o - t\frac{n}{d}, y_o - t\frac{a}{d})$$

per cui le soluzioni della congruenza sono tutti e soli i numeri

$$x = x_o - t\frac{n}{d}, \quad t \in \mathbb{Z}$$

che costituiscono l'insieme $[x_o]_{\frac{n}{d}}$.

SISTEMI DI CONGRUENZE

Un **sistema di congruenze lineari** è un sistema di equazioni del tipo:

$$\begin{cases} a_1 x \equiv b_1 \ (\text{ mod } m_1) \\ a_2 x \equiv b_2 \ (\text{ mod } m_2) \\ \cdots\cdots \\ a_r x \equiv b_r \ (\text{ mod } m_r) \end{cases} \tag{1}$$

Una soluzione di tale sistema è ogni intero $x_o \in \mathbb{Z}$ che risulti soluzione di *tutte* le congruenze che lo costituiscono.

Il risultato fondamentale per la risoluzione di questo tipo di sistemi è il seguente:

Teorema cinese del resto: *Si consideri un sistema di congruenze del tipo*

$$\begin{cases} x \equiv b_1 \ (\ mod\ m_1) \\ x \equiv b_2 \ (\ mod\ m_2) \\ \cdots\cdots \\ x \equiv b_r \ (\ mod\ m_r) \end{cases} .$$

Se $MCD(m_i, m_j) = 1$ *per* $i \neq j$*, ovvero se i moduli* m_i *sono a due a due primi tra loro, allora il sistema ammette soluzioni e, se* x_o *è una soluzione, allora l'insieme* S *di tutte le soluzioni è*

$$S = [x_o]_m$$

dove $m = m_1 \cdot m_2 \cdots m_k$*.*

In sintesi, il sistema ammette una sola soluzione modulo $m_1 \cdot m_2 \cdots m_r$*.*

Questo risultato fornisce una condizione sufficiente, ma non necessaria, per la risolubilità di un sistema di congruenze. Di fatto, ogni sistema del tipo (*), nell'ipotesi che i moduli m_i, siano a due a due primi tra loro, è riconducibile ad un sistema del tipo considerato nell'enunciato del Teorema cinese del resto:

Corollario: *Si consideri un sistema*

$$\begin{cases} a_1 x \equiv b_1 \ (\ mod\ m_1) \\ a_2 x \equiv b_2 \ (\ mod\ m_2) \\ \cdots\cdots \\ a_r x \equiv b_r \ (\ mod\ m_r) \end{cases} \tag{2}$$

dove $MCD(m_i, m_j) = 1$ *per* $i \neq j$*. Allora, se ciascuna congruenza del sistema ammette soluzioni, il sistema ammette soluzioni.*

Infatti, in tali ipotesi, denotata con b'_i la soluzione dell'equazione i-ma modulo $\frac{m_i}{d_i}$, dove $d_i = MCD(a_i, m_i)$, allora il sistema è equivalente a

$$\begin{cases} x \equiv b'_1 \,(\bmod \frac{m_1}{d_1}) \\ x \equiv b'_2 \,(\bmod \frac{m_2}{d_2}) \\ \dots \\ x \equiv b'_r \,(\bmod \frac{m_r}{d_r}) \end{cases} \qquad (**).$$

Abbiamo ancora

$$MCD(\frac{m_i}{d_i}, \frac{m_j}{d_j}) = 1$$

per $i \neq j$, perchè per ipotesi:

$$1 = sm_i + tm_j,$$

per opportuni interi s, t e quindi vale anche:

$$1 = (sd_i)\,\frac{m_i}{d_i} + (td_j)\,\frac{m_j}{d_j},$$

e quindi anche i numeri $\frac{m_i}{d_i}$ e $\frac{m_j}{d_j}$ sono primi tra loro. Pertanto il Teorema cinese del resto è applicabile al sistema equivalente (**).

DIMOSTRAZIONE DEL TEOREMA CINESE DEL RESTO

Premettiamo la seguente osservazione:

Prop: *Siano $m, m_1, \ldots, m_k$ interi con $k \geq 1$. Se m è primo con ciascuno degli m_i, allora m è primo anche con il loro prodotto $m_1 \cdots m_k$.*
La dimostrazione è un esercizio (ragionare per induzione su k).

Consideriamo prima il caso di un sistema di due congruenze:

$$\begin{cases} x \equiv b_1 \ (\bmod\ m_1) \\ x \equiv b_2 \ (\bmod\ m_2) \end{cases}$$

dove $MCD(m_1, m_2) = 1$. Vogliamo provare che esso ha soluzioni, e che l'insieme di tutte le soluzioni è una singola classe del tipo $[x_o]_{m_1 m_2}$.

Gli interi x che soddisfano la prima congruenza sono tutti e soli i numeri della forma:

$$x = b_1 + km_1, \quad k \in \mathbb{Z}. \qquad (*)$$

Andando a sostituire nella seconda congruenza, abbiamo che x è soluzione di quest'ultima se e solo se

$$b_1 + km_1 \equiv b_2 \ (\bmod\ m_2)$$

ovvero se e solo se k è soluzione della congruenza seguente:

$$m_1 k \equiv b_2 - b_1 \ (\bmod\ m_2).$$

Questa congruenza è risolubile in forza dell'ipotesi $MCD(m_1, m_2) = 1$ e, fissata una sua soluzione soluzione k_o, sappiamo che tutte le altre sono gli interi:

$$k = k_o + tm_2, \quad t \in \mathbb{Z}.$$

Dunque, tenendo conto di (*), il sistema di partenza è risolubile, ammettendo come soluzioni tutti e soli gli interi x della forma:

$$x = b_1 + (k_o + tm_2)m_1 = b_1 + k_o m_1 + tm_1 m_2$$

al variare di $t \in \mathbb{Z}$. Tale insieme di numeri è la singola classe $[b_1 + k_o m_1]_{m_1 m_2}$ e quindi resta provata la nostra tesi.
Per provare il Teorema nel caso generale, ragioniamo per induzione sul numero r delle congruenze formanti il sistema. Il passo base corrisponde a $r = 2$, caso che abbiamo appena esaminato.

Dato $r \geq 2$, supponiamo ora che il Teorema sia vero per sistemi di congruenze con r equazioni, e proviamo che esso sussiste per sistemi con $r+1$ equazioni.
Consideriamo un tale sistema:

$$\begin{cases} x \equiv b_1 \ (\text{ mod } m_1) \\ x \equiv b_2 \ (\text{ mod } m_2) \\ \cdots\cdots \\ x \equiv b_r \ (\text{ mod } m_r) \\ x \equiv b_{r+1} \ (\text{ mod } m_{r+1}) \end{cases} \tag{1}$$

dove $MCD(m_i, m_j) = 1$ per $i \neq j$.

Fissiamo l'attenzione sul sistema formato dalle prime r congruenze: ad esso si può applicare l'ipotesi induttiva, perchè in particolare i moduli $m_1, \ldots, m_r$ sono a due due primi tra loro.
Quindi tale sistema ammette come insieme delle soluzioni una classe $[x_o]_n$, dove $n = m_1 \cdots m_r$. Sia x la generica soluzione, che è un numero del tipo:

$$x = x_o + k(m_1 \cdots m_r), \quad k \in \mathbb{Z}.$$

Tale numero soddisfa anche l'ultima congruenza del nostro sistema (1) se e solo se k soddisfa:

$$x_o + k(m_1 \cdots m_r) \equiv b_{r+1} \ (\text{mod } m_{r+1})$$

ovvero se e solo se k è soluzione della congruenza:

$$(m_1 \cdots m_r)k \equiv b_{r+1} - x_o \ (\text{mod } m_{r+1}).$$

In virtù dell'ipotesi sui moduli e della Proposizione enunciata sopra, m_{r+1} è primo con il prodotto $m_1 \cdots m_r$, e quindi anche questa congruenza è risolubile, con soluzione generale del tipo:

$$k = k_o + tm_{r+1}, \quad t \in \mathbb{Z}.$$

In conclusione, il sistema (1) ammette come soluzioni tutti e soli gli interi x della forma:

$$x = x_o + (k_o + tm_{r+1})m_1 \cdots m_r$$

cioè

$$x = x_o + k_o n + t\,(m_1 \cdots m_{r+1}),$$

che sono esattamente i numeri costituenti la classe $[x_o + k_o n]_m$, dove $m = m_1 \cdots m_{r+1}$.

STRUTTURE ALGEBRICHE

Sia X un qualsiasi insieme non vuoto.

Def. Si chiama **operazione interna** (o semplicemente **operazione**) su X ogni applicazione $* : X \times X \to X$.

Se $*$ è un'operazione su X, la coppia $(X, *)$ prende il nome di **struttura algebrica**.

Dati $a, b \in X$, piuttosto che scrivere

$$*((a, b))$$

si scrive

$$a * b.$$

Più in generale, si possono considerare strutture algebriche $(X, *_1, \ldots, *_k)$ dove $*_1, \ldots, *_k$ sono $k \geq 1$ operazioni su X.

Esempio: Sono operazioni interne la somma $+$ ed il prodotto $\cdot$ standard sugli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Quindi, ad esempio, sono strutture algebriche $(\mathbb{Z}, +)$, $(\mathbb{Z}, +, \cdot)$, ma anche $(\mathbb{Z}, +, \cdot)$ (struttura con due operazioni).

Esempio: Dato un insieme A, consideriamo l'insieme A^A di tutte le applicazioni da A in A. Allora l'operazione di composizione

$$*((f, g)) := f \circ g$$

è un'operazione su A^A.

Esempio: Dato un insieme A, abbiamo le operazioni su $\mathcal{P}(A)$ di intersezione e unione:

$$\cap : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A) \quad \text{e} \cup : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A).$$

LE OPERAZIONI DI SOMMA E PRODOTTO SU $\mathbb{Z}_N$

Fissato un intero positivo $n > 0$ è possibile definire in modo naturale due operazioni

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \ \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

dette ancora "somma" e "prodotto", ereditate dalle corrispondenti familiari operazioni su $\mathbb{Z}$, nel modo che ora descriviamo.

Def: Date due classi $[a]_n$ e $[b]_n$ si pone:

$$[a]_n + [b]_n := [a + b]_n.$$

$$[a]_n \cdot [b]_n := [a \cdot b]_n.$$

Attenzione: occorre controllare che queste operazioni sono **ben definite**!

In effetti, la definizione dipende solo dalle classi $[a]_n$ e $[b]_n$ e *non* dai numeri particolari a e b che le rappresentano. Più esplicitamente, se $[a]_n = [a']_n$ e $[b]_n = [b']_n$, allora si ha anche

$$[a + b]_n = [a' + b']_n$$

e

$$[a \cdot b]_n = [a' \cdot b']_n.$$

Ciò è garantito dalle proprietà basilari della relazione $\equiv_n$, già utilizzate in precedenza: da $a \equiv_n a'$ e $b \equiv_n b'$ segue, come sappiamo, che $a + b \equiv_n a' + b'$. Analogo discorso per l'operazione di prodotto.

Esempio: Posto $a = [5]_7$ e $b = [13]_7$, abbiamo

$$a + b = [5]_7 + [13]_7 = [18]_7 = [4]_7.$$

D'altra parte, poichè b si può anche scrivere $b = [6]_7$, la stessa operazione si può anche effettuare come segue:

$$a + b = [5]_7 + [6]_7 = [11]_7 = [4]_7.$$

Analogamente abbiamo anche $a = [-9]_7$ e ancora:

$$[-9]_7 + [13]_7 = [4]_7,$$

e anche:

$$[-9]_7 + [6]_7 = [-3]_7 = [4]_7.$$

Si ottiene sempre lo stesso risultato (stessa classe di $\mathbb{Z}_7$), che dipende solo da a e b, indipendentemente dal modo di fare la somma scegliendo 5 oppure -9 in a e 13 oppure 6 in b.

Definizione: Un'operazione $* : X \times X \to X$ si dice **associativa** se per ogni $x, y, z \in X$ risulta

$$x * (y * z) = (x * y) * z.$$

Es: Questa proprietà è soddisfatta per le strutture algebriche $(X, +)$ e $(X, \cdot)$, dove X è uno degli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Esempio: Le operazioni di somma e prodotto su $\mathbb{Z}_n$ sono entrambe associative. Infatti, ad esempio, abbiamo:

$$([a]_n + [b]_n) + [c]_n = ([a + b]_n) + [c]_n = [(a + b) + c]_n = [a + (b + c)]_n =$$

$$= [a]_n + [b + c]_n = [a]_n + ([b]_n + [c]_n),$$

come conseguenza dell'associatività della usuale somma tra interi.

Definizione: Si dice che una struttura algebrica $(X, *)$ è dotata di **elemento neutro** se esiste un elemento $u \in X$ tale che

$$\forall x \in X \quad u * x = x = x * u.$$

Teorema : *Se la struttura algebrica $(X, *)$ è dotata di elemento neutro, questo è unico.*

Dimostrazione: infatti, ammettendo che u ed u' siano entrambi elementi neutri, risulta

$$u' = u * u' = u.$$

La prima uguaglianza è giustificata dal fatto che u è elemento neutro, la seconda dal fatto che u' gode della stessa proprietà.

Esempio: In $(\mathcal{P}(A), \cap)$ l'elemento neutro è l'insieme A stesso.

In $(\mathcal{P}(A), \cup)$ l'elemento neutro è l'insieme vuoto $\emptyset$.

MONOIDI

Definizione: Si chiama **monoide** ogni struttura algebrica $(X, *)$ verificante le condizioni seguenti:

1) L'operazione $*$ è associativa.

2) $(X, *)$ è dotata di elemento neutro.

Esempi: $(X, +)$ è un monoide, essendo X è uno degli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. L'elemento neutro è 0.

$(X, \cdot)$ è un monoide, essendo X è uno degli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. L'elemento neutro è 1.

Sono monoidi anche le strutture algebriche $(\mathbb{Z}_n, +)$ e $(\mathbb{Z}_n, \cdot)$; infatti risulta:

- $[0]_n$ è l'elemento neutro di $(\mathbb{Z}_n, +)$
- $[1]_n$ è l'elemento neutro di $(\mathbb{Z}_n, \cdot)$.

Per verificarlo, basta effettuare i seguenti calcoli, basati sulla definizione della somma e del prodotto in $\mathbb{Z}_n$:

$$[x]_n + [0]_n = [x + 0]_n = [x]_n$$

$$[x]_n \cdot [1]_n = [x \cdot 1]_n = [x]_n$$

e ciò è sufficiente stante la commutatività di entrambe le operazioni.

ELEMENTI INVERTIBILI DI UN MONOIDE

Sia $(X, *)$ un monoide con elemento neutro u.

Def: Un elemento $x \in X$ si dice **invertibile** se esiste un altro elemento x' in X tale che

$$x * x' = u = x' * x.$$

Un tale elemento x' prende il nome di **inverso di** x.

Teorema: *Se x è un elemento invertibile di un monoide $(X, *)$, allora l'inverso di x è unico.*

Dimostrazione: supponiamo che x' e x'' siano entrambi inversi di x. Allora in particolare abbiamo

$$x * x' = u.$$

Applicando l'operazione $*$, "componendo" ambo i membri con x'' si ottiene:

$$x'' * (x * x') = x'' * u$$

ovvero

$$x'' * (x * x') = x''$$

che si può riscrivere, stante la proprietà associativa:

$$(x'' * x) * x' = x''.$$

D'altra parte, per definizione di inverso, sappiamo anche che $x'' * x = u$ e quindi l'ultima uguaglianza è

$$u * x' = x''$$

ovvero

$$x' = x''.$$

Oss: Si noti che l'elemento neutro u è sempre invertibile, con inverso u.

Esempio: In $(\mathbb{Z}, +)$ tutti gli elementi sono invertibili. Infatti l'inverso di $m \in \mathbb{Z}$ è $-m$:

$$m + (-m) = 0 = (-m) + m.$$

In $(\mathbb{Z}, \cdot)$ gli unici elementi invertibili sono +1 e -1 ed entrambi coincidono col proprio inverso. Infatti $xx' = 1$ è possibile sono se x e x' sono entrambi 1 o -1.

GRUPPI

Def: Si chiama **gruppo** ogni monoide i cui elementi sono sono **tutti invertibili.**

Sono gruppi:

- $(X, +)$ dove X è uno degli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

- $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$ dove $*$ indica l'insieme numerico in questione privato di 0.

  In relazione a questi esempi, si osservi che, denotato con X l'insieme numerico in questione, l'operazione di prodotto di X induce effettivamente un'operazione interna anche su X^*, ovvero una funzione:

  $$\cdot : X^* \times X^* \to X^*.$$

  Essa è ben definita, perchè se $a \neq 0$ e $b \neq 0$, la legge di annullamento del prodotto garantisce che $a \cdot b \neq 0$, ovvero il risultato dell'operazione è ancora un elemento *dello stesso insieme* X^*.

- $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \cdot)$ sono tutti monoidi che non sono gruppi.

Teorema: $(\mathbb{Z}_n, +)$ *è un gruppo.*

Infatti, sappiamo già che si tratta di un monoide. Se $[a]_n \in \mathbb{Z}_n$, allora $[a]_n$ è invertibile in quanto ammette come inverso $[-a]_n$; infatti:

$$[a]_n + [-a]_n = [a - a]_n = [0]_n = [-a]_n + [a]_n.$$

Esempio: L'inverso di $[8]_{10}$ in $(\mathbb{Z}_{10}, +)$ è $[-8]_{10} = [2]_{10}$. L'inverso di $[3]_6$ è $[-3]_6 = [3]_6$ (in effetti $[3]_6 + [3]_6 = [6]_6 = [0]_6$).

In generale, se $a > 0$, ricordiamo che

$$[-a]_n = [n - r]_n$$

dove r è il resto della divisione di a per n.

Notazione e convenzioni riguardanti i gruppi:

Dato un gruppo $(G, +)$ la cui operazione è denotata con notazione **additiva**, si usano di solito le seguenti **convenzioni**:

-L'elemento neutro si denota preferibilmente con 0.

-L'inverso di $a \in G$ si denota con $-a$ e si chiama **l'opposto di** a.

Dato un gruppo $(G, \cdot)$ la cui operazione è denotata con notazione **moltiplicativa**, si usano le seguenti convenzioni:

-L'elemento neutro si denota preferibilmente con 1 (talvolta è utilizzato anche il simbolo e).

-L'inverso di $a \in G$ si denota con a^{-1}.

Definizione: Un gruppo $(G, *)$ si dice **abeliano** se l'operazione $*$ gode della proprietà **commutativa**:

$$\forall a, b \in G \quad a * b = b * a.$$

Esempi: I gruppi $(X, +)$ dove $X = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono tutti abeliani.

I gruppi $(\mathbb{Q}^*, \cdot)$ e $(\mathbb{R}^*, \cdot)$ sono abeliani.

I gruppi $(\mathbb{Z}_n, +)$ sono tutti abeliani.

ELEMENTI INVERTIBILI DI $(\mathbb{Z}_N, \cdot)$

Ci poniamo ora il problema di stabilire se i monoidi $(\mathbb{Z}_n, \cdot)$ sono gruppi.
A tal fine daremo una caratterizzazione gli elementi invertibili.

Nel seguito supporremo sempre $n > 1$, perchè se $n = 1$, allora si ricade nel caso banale $\mathbb{Z}_1 = \{[0]_1\} = \{\mathbb{Z}\}$, in cui la struttura algebrica in questione ha un solo elemento, e l'unico elemento di tale insieme è elemento neutro sia rispetto alla somma che rispetto al prodotto (in particolare è invertibile).

Teorema: *Sia $n > 1$ un intero. Un elemento $[a]_n$ del monoide $(\mathbb{Z}_n, \cdot)$ è invertibile se e solo se*

$$MCD(a, n) = 1.$$

Corollario: *La classe $[0]_n$ non è mai invertibile in $(\mathbb{Z}_n, \cdot)$.*

Infatti, $MCD(0, n) = n > 1$.

Per dimostrare il teorema, abbiamo che $[a]_n$ è invertibile in $(\mathbb{Z}_n, \cdot)$ se e solo se esiste $[x]_n$ tale che

$$[a]_n \cdot [x]_n = [1]_n = [x]_n \cdot [a]_n$$

e, siccome l'operazione $\cdot$ è commutativa, ciò equivale a

$$[a]_n \cdot [x]_n = [1]_n,$$

che si riscrive, per definizione di $\cdot$:

$$[ax]_n = [1]_n$$

ovvero:

$$ax \equiv 1 \pmod{n}.$$

Ora, tale congruenza ha soluzioni se e solo se $MCD(a, n)|1$, cioè se e solo se $MCD(a, n) = 1$.

Conclusione: i monoidi $(\mathbb{Z}_n, \cdot)$ non sono gruppi; possiamo però determinare in essi un gruppo in modo naturale, considerandone l'insieme di tutti gli elementi invertibili. La situazione migliore sarà quella in cui, a parte $[0]_n$, tutte le classi risultino invertibili. Prima di caratterizzare questa circostanza, discutiamo in generale la nozione di gruppo degli elementi invertibili di un monoide qualsiasi.

IL GRUPPO DEGLI ELEMENTI INVERTIBILI DI UN MONOIDE

.

Def: Sia $(G, \cdot)$ un monoide. L'insieme di **tutti gli elementi invertibili** di G si denoterà con il simbolo

$$U(G).$$

Detto 1_G l'elemento neutro di G, abbiamo che $1_G \in U(G)$.

Proposizione: *1) Se a, b sono elementi invertibili di $(G, \cdot)$, allora tale è $a \cdot b$ e il suo inverso è $b^{-1} \cdot a^{-1}$.*

2) L'insieme $U(G)$ è un gruppo rispetto all'operazione ristretta:

$$\cdot : U(G) \times U(G) \to U(G).$$

Il gruppo $(U(G), \cdot)$ si chiamerà **il gruppo degli elementi invertibili del monoide** $(G, \cdot)$.

Dimostrazione: 1) Basta fare la seguente verifica:

$$(a \cdot b) \cdot (b^{-1}a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = (a \cdot 1_G) \cdot a^{-1} = a \cdot a^{-1} = 1_G$$

e analogamente

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = (b^{-1} \cdot 1_G) \cdot b = 1_G.$$

2) L'operazione ristretta è ben definita perchè il punto 1) ci assicura che il risultato dell'operazione $a \cdot b$, effettuata con a, b entrambi in $U(G)$, è ancora un elemento dello stesso insieme $U(G)$.
Inoltre, avendosi $1_G \in U(G)$, è chiaro che 1_G è ancora elemento neutro per tale operazione ristretta, e che la proprietà associativa si conserva. Quindi $(U(G), \cdot)$ è un monoide. Infine, osserviamo che se $a \in U(G)$, anche l'inverso a^{-1} di a in G è un elemento invertibile: infatti ammette a come inverso! Quindi $a^{-1} \in U(G)$ e poichè continuano a valere le uguaglianze

$$a \cdot a^{-1} = 1_G = a^{-1} \cdot a$$

rispetto all'operazione ristretta su $U(G)$, abbiamo che ogni $a \in U(G)$ è invertibile. Pertanto $(U(G), \cdot)$ è un gruppo, stante la definizione.

LA FUNZIONE DI EULERO E I NUMERI PRIMI

Continuiamo lo studio dei monoidi $(\mathbb{Z}_n, \cdot)$. Sappiamo che una classe $[a]_n$, che possiamo supporre rappresentata da un numero tale che $1 \leq a < n$, è invertibile se e solo se a è primo con il modulo n. Dunque la cardinalità del gruppo $U(\mathbb{Z}_n)$ degli elementi invertibili di $\mathbb{Z}_n$ è data da:

$$|U(\mathbb{Z}_n)| = |\{a \in \mathbb{N} | \, 1 \leq a < n \text{ e } MCD(a, n) = 1\}|.$$

Si introduce a questo proposito la funzione seguente:

Def: Si chiama **funzione di Eulero** la funzione

$$\varphi : \mathbb{N}^* \to \mathbb{N}$$

così definita:

$$\varphi(1) = 1$$

e, per $n \geq 2$:

$\varphi(n) :=$ numero degli interi k positivi, strettamente minori di n e **primi con** n.

Esempio: $\varphi(6) = 2$ in quanto nell'insieme $\{1, \ldots, 5\}$, gli unici numeri che sono primi con 6 sono 1 e 5.

Quindi, per definizione, per ogni $n > 1$ abbiamo:

$$|U(\mathbb{Z}_n)| = \varphi(n).$$

Richiamiamo ora la seguente definizione fondamentale:

Definizione Un numero $p \in \mathbb{Z}$ con $p \neq 0$, $p \neq \pm 1$, si dice **primo** se i suoi unici divisori sono $1, -1, p$ e $-p$.

È chiaro che per ogni numero primo $p \in \mathbb{N}$ si ha: $\varphi(p) = p - 1$, perchè tutti i numeri interi positivi a con $a < p$ non possono avere divisori comuni con p, a parte 1 e -1.

Dato l'intero $n > 1$, denotiamo con $\mathbb{Z}_n^*$ l'insieme $\mathbb{Z}_n - \{[0]_n\} = \{[1]_n, \ldots, [n-1]_n\}$.

In base alla definizione di numero primo e alle considerazione fatte sopra, possiamo concludere:

Teorema: *Il gruppo $U(\mathbb{Z}_n)$ concide con $\mathbb{Z}_n^*$ se e solo se n è un numero primo.*

ANELLI

Def: Si chiama **anello** ogni struttura algebrica $(A, +, \cdot)$ consistente di un insieme A e di due operazioni su A verificanti le seguenti condizioni:

a) $(A, +)$ è un **gruppo abeliano**.

b) $(A, \cdot)$ è un **monoide**.

c) Valgono le proprietà **distributive** del prodotto rispetto alla somma: per ogni $a, b, c \in A$

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

Se $(A, +, \cdot)$ è un anello, l'elemento neutro del gruppo $(A, +)$ si denota con 0 e si chiama *zero dell'anello A*. L'elemento neutro del monoide $(A, \cdot)$ si denota con 1 e si chiama *unità dell'anello A*.

Def: Un anello $(A, +, \cdot)$ si dice **commutativo** se l'operazione $\cdot$ è commutativa.

Esempi:
- Sono anelli gli insiemi numerici $(X, +, \cdot)$ dove $X = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $+$, $\cdot$ sono le usuali operazioni di somma e prodotto.

- Per ogni $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo.

Per verificarlo, resta solo da controllare che sia valida la condizione c) della definizione; poichè l'operazione $\cdot$ è commutativa, si tratta di fare una sola verifica:

$([a]_n+[b]_n)\cdot[c]_n = [a+b]_n\cdot[c]_n = [(a+b)c]_n = [ac+bc]_n = [ac]_n+[bc]_n = [a]_n\cdot[c]_n+[b]_n\cdot[c]_n.$

LEGGE DI CANCELLAZIONE IN UN GRUPPO

Sia $(G, \cdot)$ un gruppo. Vale la seguente proprietà basilare, che permette di effettuare semplificazioni:

Teorema: *Siano a, b, c elementi di G. Allora se*

$$a \cdot c = b \cdot c$$

oppure

$$c \cdot a = c \cdot b,$$

allora $a = b$.

La dimostrazione consiste in una semplice applicazione del fatto che c ammette l'inverso c^{-1}: denotato con 1 l'elemento neutro di G, assumendo ad esempio che

$$a \cdot c = b \cdot c,$$

allora moltiplicando ambo i membri per c^{-1} segue:

$$(a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1}$$

da cui

$$a \cdot (c \cdot c^{-1}) = b \cdot (c \cdot c^{-1})$$

ovvero

$$a \cdot 1 = b \cdot 1$$

e quindi in definitiva

$$a = b.$$

Esempio: Come applicazione, abbiamo la seguente proprietà: se $a \in G$ è tale che:

$$a \cdot a = a,$$

allora $a = 1$.
Infatti l'uguaglianza precedente si può interpretare come

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

e quindi, semplificando:

$$a = 1.$$

Nota: In un gruppo $(G, +)$ la cui operazione è denotata additivamente, la legge di cancellazione assume la forma:

$$a + c = b + c \Rightarrow a = b.$$

Dunque, ad esempio: se

$$a + a = a$$

allora si deduce che necessariamente $a = 0$.

ELEMENTI INVERTIBILI DI UN ANELLO

Sia $(A, +, \cdot)$ un anello. Ricordiamo che 0 denota l'elemento neutro rispetto alla somma $+$. Il seguente fatto ne stabilisce il comportamento rispetto al prodotto:

Proposizione: *Per ogni $a \in A$ si ha:*

$$a \cdot 0 = 0 = 0 \cdot a.$$

Dimostrazione: in base alla proprietà distributiva:

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

Siccome $(A, +)$ è un gruppo, da ciò possiamo dedurre

$$a \cdot 0 = 0.$$

In modo del tutto analogo si verifica che $0 \cdot a = 0$.

Osservazione: Se in anello accade che $0 = 1$, allora si ha che A ha un solo elemento:

$$A = \{0\}.$$

Infatti per ogni $x \in A$ si ottiene $x = x \cdot 1 = x \cdot 0 = 0$.
In tal caso si parla di *anello banale* e tale caso sarà di norma scartato nelle nostre considerazioni.

Def: Un elemento a di un anello $(A, +, \cdot)$ si dice **invertibile** se è invertibile rispetto al prodotto, cioè se è un elemento invertibile del monoide $(A, \cdot)$.

Se a è invertibile, l'inverso si denoterà sempre con a^{-1}. Tale oggetto non va confuso con l'opposto $-a$. Riassumendo, se a è invertibile abbiamo:

$$a \cdot a^{-1} = 1 = a^{-1} \cdot a,$$

mentre è sempre vero che:

$$a + (-a) = 0 = (-a) + a.$$

Esempio: Nell'anello $\mathbb{Z}$ gli unici elementi invertibili sono 1 e -1.
Negli anelli $\mathbb{Q}$ e $\mathbb{R}$ sono invertibili **tutti** gli elementi **diversi da zero**.

Proposizione: *In un anello non banale, lo 0 non è mai invertibile.*
Ciò è immediata conseguenza del risultato precedente, perchè se 0 fosse invertibile, esisterebbe $x \in A$ tale che

$$0 \cdot x = 1$$

da cui

$$0 = 1.$$

CORPI E CAMPI

Dato un anello $(A, +, \cdot)$, possiamo considerare l'insieme dei suoi elementi invertibili, che costituisce il gruppo $U(A)$ degli elementi invertibili del monoide soggiagente $(A, \cdot)$.

Def: Si chiama **corpo** ogni anello $(A, +, \cdot)$ nel quale **tutti** gli elementi diversi da zero sono invertibili. In altri termini, dire che A è un corpo significa che

$$U(A) = A^*$$

dove $A^* = \{\, a \in A \mid a \neq 0 \,\}$.

Un corpo **commutativo** si chiama **campo**.

Esempi: Sono campi $\mathbb{Q}$ ed $\mathbb{R}$ e $\mathbb{C}$.

Attenzione: $\mathbb{Z}$ non è un campo!

Dall'analisi fatta in precedenza sugli elementi invertibili di $\mathbb{Z}_n$ segue:

Teorema: *L'anello $\mathbb{Z}_n$ è un campo se e solo se n è un numero primo.*

Dimostrazione: infatti, inanzitutto l'anelllo $\mathbb{Z}_n$ è commutativo; abbiamo che $\mathbb{Z}_n$ è un campo se e solo se è un corpo, ovvero se e solo se $U(\mathbb{Z}_n) = \mathbb{Z}_n^*$, ma sappiamo che ciò accade se e solo se n è primo.

IL TEOREMA FONDAMENTALE DELL'ARITMETICA

Teorema (fondamentale dell'aritmetica) *Sia $a \in \mathbb{Z}$ un numero intero con $a \neq 0$, $a \neq \pm 1$. Allora a è primo oppure può essere scritto come il prodotto di un numero finito di numeri primi (non necessariamente distinti):*

$$a = p_1 \cdot p_2 \cdots p_s, \quad s \geq 1$$

dove i $p_i \in \mathbb{Z}$ sono tutti numeri primi.
Tale fattorizzazione è essenzialmente unica nel senso che, se

$$a = p_1 \cdot p_2 \cdots p_s \quad e \quad a = q_1 \cdot q_2 \cdots q_t$$

dove i numeri p_i $(1 \leq i \leq s)$ e q_j $(1 \leq j \leq t)$ sono primi, allora $s = t$ ed a meno di riordinare i fattori si ha

$$p_1 = \pm q_1,\ p_2 = \pm q_2, \ldots,\ p_s = \pm q_s.$$

Corollario: *Ogni $a \in \mathbb{Z}$, $a \neq 0$, $a \neq \pm 1$ si scrive in modo unico (a parte il riordino dei fattori) nella forma:*

$$a = (p_1)^{m_1} \cdot (p_2)^{m_2} \cdots (p_s)^{m_s}$$

dove i p_i sono primi **distinti tra loro** *e gli m_i sono interi positivi.*

Il Teorema non è costruttivo: determinare esplicitamente la fattorizzazione di un numero come prodotto di primi è un'operazione laboriosa. Non si conoscono algoritmi davvero efficienti per effettuarla.

Ci limiteremo a dimostrare l'esistenza della fattorizzazione; ovviamente basta considerare il caso in cui $a \in \mathbb{N}$ e quindi $a \geq 2$.

Si ragionerà per induzione. Conviene però utilizzare la seguente riformulazione del Principio di Induzione:

Teorema (II^a forma del Principio di Induzione): *Sia $P(n)$ un enunciato che ha senso per tutti i numeri naturali maggiori o uguali ad un certo $n_o \in \mathbb{N}$. Supponiamo soddisfatte le condizioni seguenti:*

i) $P(n_o)$ è vero;
ii) Per ogni $n \geq n_o$, se $P(k)$ è vero per tutti i numeri $k \in \{n_o, n_o + 1, ..., n\}$, allora anche $P(n+1)$ è vero.

Allora $P(n)$ è vero per tutti i numeri interi $n \geq n_o$.

Sia dunque n un intero con $n \geq 2$.

Passo base: $n = 2$; si tratta di un numero primo e non c'è nulla da provare.

Passo induttivo: Dato $n \geq 2$, supponiamo che la proprietà di di fattorizzazione sia vera per ogni numero k con $2 \leq k \leq n$ e proviamola anche per $n + 1$.
Se $n + 1$ è primo, non c'è nulla da provare; altrimenti $n + 1$ ammette divisori non banali, per cui si può scrivere come prodotto:

$$n + 1 = ab$$

dove a e b sono entrambi maggiori o uguali a 2 e minori strettamente di $n + 1$. Pertanto a tali numeri si può applicare l'ipotesi induttiva, che garantisce che essi si possono scrivere nella forma:

$$a = p_1 \cdots p_s, \quad b = q_1 \cdots q_t,$$

con i p_i e i q_j tutti numeri primi; quindi:

$$n + 1 = p_1 \cdots p_s \cdot q_1 \cdots q_t$$

e quindi la tesi è provata per $n + 1$.

N. B: La seconda forma del Principio di Induzione si dimostra facilmente usando la prima. Infatti, assumendo le condizioni 1) e 2), posto

$$Q(n) := \text{“}P(k) \text{ è vera per ogni } k \text{ tale che } n_o \leq k \leq n\text{”},$$

basta provare che $Q(n)$ è vera per ogni $n \geq n_o$. Ma ciò si può fare per induzione (prima forma):

Passo base: $Q(n_0)$ vèra, perchè in base a 1) $P(n_o)$ lo è.

Passo induttivo: dato $n \geq n_o$, supponiamo che $Q(n)$ sia vera e deduciamo $Q(n+1)$. Per ipotesi dunque sappiamo che $P(k)$ è vera per ogni k tale che $n_o \leq k \leq n$. Ma allora, per la 2), anche $P(n + 1)$ è vera. Dunque tale è $Q(n + 1)$.

PROPRIETÀ DELLA FUNZIONE DI EULERO

Nota la scomposizione di un intero $n \in \mathbb{N}^*$ in fattori primi (positivi), il calcolo di $\varphi(n)$ è agevolato dalle seguenti proprietà rilevanti della funzione φ:

Teorema:
1) Se $p \in \mathbb{N}$ è un primo, allora $\varphi(p^k) = p^k - p^{k-1}$.

2) Se $a, b \in \mathbb{N}^*$ sono numeri primi tra loro, allora $\varphi(ab) = \varphi(a)\varphi(b)$.

Come conseguenza abbiamo che, se si scompone un numero $n \in \mathbb{N}^*$ come prodotto di potenze di primi distinti:

$$n = p_1^{k_1} \cdots p_s^{k^s},$$

allora siamo in grado di calcolare agevolmente $\varphi(n)$, avendosi, in base alla 2) del Teorema:

$$n = \varphi(p_1^{k_1}) \cdots \varphi(p_s^{k^s}),$$

in quanto i numeri $p_i^{k_i}$ sono a due a due primi tra loro. Dunque siamo ricondotti al caso 1) del Teorema:

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_s^{k_s} - p_s^{k_s-1}).$$

Esempio: Calcoliamo $\varphi(18) = \varphi(3^2) \cdot \varphi(2) = (9-3) \cdot 1 = 6$.

IL TEOREMA DI FERMAT-EULERO

Sia $(G, \cdot)$ un gruppo e sia $a \in G$.

Per ogni $m \in \mathbb{N}^*$ si definiscono le potenze a^m in modo naturale, ponendo:

$$a^m := \underbrace{a \cdot a \cdots a}_{m \text{ volte}}$$

mentre per $m = 0$, si pone

$$a^0 = 1.$$

Le potenze con esponente negativo si introducono come segue: se $m \in \mathbb{Z}$ con $m < 0$ allora, per definizione si pone:

$$a^m := (a^{-1})^{-m}.$$

Ad esempio, $a^{-4} = a^{-1}a^{-1}a^{-1}a^{-1}$.

Concentriamo ora la nostra attenzione sul gruppo $U(\mathbb{Z}_n)$ degli elementi invertibili di $\mathbb{Z}_n$, $n > 1$.
Il risultato seguente è molto importante:

Teorema (Fermat-Eulero): *Siano $n \in \mathbb{N}$, $n > 1$ ed a un intero primo con n. Allora*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

Il risultato mostra che, nel gruppo $U(\mathbb{Z}_n)$ elevando qualsiasi elemento $[a]_n$ a $\varphi(n)$ si ottiene l'unità $[1]_n$:

$$[a]_n^{\varphi(n)} = [1]_n.$$

Come caso particolare si ottiene il cosiddetto *piccolo Teorema di Fermat*:

Teorema: *Sia $p > 0$ un numero primo e a un intero non divisibile per p. Allora si ha:*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Infatti in questo caso a è primo con p e $\varphi(p) = p - 1$.

CALCOLO DI POTENZE MODULO N

Le usuali proprietà delle potenze valgono in un gruppo astratto qualsiasi:

Teorema: *Siano $(G,\cdot)$ un gruppo, $a \in G$ ed n, m numeri interi. Allora*

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

$$(a^m)^n = a^{m \cdot n}.$$

La dimostrazione si può fare per induzione. Come applicazione del Teorema di Fermat-Eulero, fissato un intero $n > 1$, mettiamo in evidenza la seguente proprietà, che è molto utile ai fini di calcolare le potenze a^k di un numero modulo n:

Prop: *Se $h \equiv k \pmod{\varphi(n)}$, allora per ogni $a \in \mathbb{Z}$ con $MCD(a,n) = 1$ si ha:*

$$a^h \equiv a^k \pmod{n}.$$

Nel caso generale, in cui h o k possono essere numeri negativi, il risultato va letto in termini di potenze di $[a]_n$ calcolate nel gruppo $U(\mathbb{Z}_n)$, a cui $[a]_n$ appartiene. Esso dice che:

$$[a]_n^h = [a]_n^k.$$

In altri termini, per calcolare $[a]_n^h$, è lecito sostituire l'esponente h con qualsiasi altro intero congruo ad esso modulo $\varphi(n)$.

Per dimostrarlo, supponiamo che $h \equiv k \pmod{\varphi(n)}$; segue per definizione che

$$h = k + t\varphi(n)$$

per qualche $t \in \mathbb{Z}$. Allora, usando le proprietà delle potenze nel gruppo $U(\mathbb{Z}_n)$:

$$[a]_n^h = [a]_n^{(k+t\varphi(n))} = [a]_n^k \cdot [a]_n^{t\varphi(n)} = [a]_n^k \cdot \left([a]_n^{\varphi(n)}\right)^t = [a]_n^k \cdot [1]_n^t = [a]_n^k$$

dove appiamo applicato il Teorema di Fermat-Eulero nella forma $[a]_n^{\varphi(n)} = [1]_n$.

Nota: Se h e k sono interi positivi, si può anche evitare l'uso delle classi di equivalenza, e delle proprietà delle potenze in un gruppo, utilizzando solo le proprietà aritmetiche della congruenza modulo n: supponendo ad esempio $h > k$ e quindi $t > 0$:

$$a^h = a^{k+t\varphi(n)} = a^k \cdot (a^{\varphi(n)})^t \equiv_n a^k \cdot 1^t \equiv_n a^k.$$

Esempi: Abbiamo $14^{64} \equiv 1 \pmod 3$ perchè $\varphi(3) = 2$ e l'esponente 64 soddisfa $64 \equiv_2 0$.
2) Calcoliamo $(-453)^{32}$ modulo 11. Riguardo la base risulta $453 \equiv_{11} (3-5+4) \equiv_{11} 2$ e quindi $-453 \equiv_{11} 9$; inoltre, essendo 11 numero primo, $\varphi(11) = 10$ e si ha $32 \equiv_{10} 2$; pertanto:

$$-453^{32} \equiv_{11} 9^2 \equiv_{11} 81 \equiv_{11} -7 \equiv_{11} 4.$$

SUL METODO CRITTOGRAFICO RSA

Il Teorema di Fermat-Eulero ha un'importante applicazione nel campo della crittografia. Qui descriviamo il prinicipio matematico alla base del sistema crittografico RSA, rimandando a testi specializzati per maggiori informazioni relative all'effettiva implementazione.

Si intende mandare messaggi ad un utente U, che saranno in forma cifrata. L'utente dovrà essere in grado di decodificare il messaggio, essendo però l'unico in grado di farlo. Il metodo RSA per farlo consiste nel seguente schema:

- U pubblica una coppia di numeri naturali
$$(n, s)$$
di cui $n = pq$ è prodotto di due numeri primi grandi (con molte cifre decimali) e s è un intero a sua scelta tale che
$$1 < s < \varphi(n).$$
Ricordiamo che $\varphi(n) = (p-1)(q-1)$.
La coppia (n, s) è visibile a tutti gli utenti (chiave pubblica).

- Ogni altro utente manda messaggi a U, sotto forma di numeri interi a soddisfacenti le seguenti limitazioni:
$$1 < a < n,\ MCD(a, n) = 1.$$
Ciascun intero a viene trasmesso in forma criptata, sostituendolo con l'unico intero b tale che
$$a^s \equiv_n b, \quad 1 \leq b < n.$$

- Per decodificare i messaggi ricevuti, U calcola preliminarmente l'inverso t di s di modulo $\varphi(n)$ (più precisamente calcola l'inverso di $[s]_{\varphi(n)}$), ovvero risolve la congruenza
$$st \equiv 1 \pmod{\varphi(n)}.$$
Quindi per decodificare il messaggio ricevuto b, calcola b^t. Tale informazione è sufficiente per ricavare il numero originario a, perchè:
$$b^t \equiv_n (a^s)^t \equiv_n a^{st} \equiv_n a^1 \equiv_n a.$$
L'operazione effettuata prende il nome di *logaritmo discreto* di b.

- La sicurezza del metodo sta nel fatto che l'utente U **non divulga i numeri p e q, ma solo il numero grande n.**
Pertanto la chiave t utilizzata per decriptare è segreta: infatti per calcolare t occorre $\varphi(n)$, ma il calcolo della funzione di Eulero senza conoscere la fattorizzazione di n è impossibile. D'altra parte scomporre il numero n per risalire a p e q è un'operazione che può richiedere anche molti anni, con i mezzi attuali.

TEOREMA DI FERMAT ASTRATTO

Come abbiamo visto, il Teorema di Fermat-Eulero si interpreta come una proprietà riguardante il calcolo delle potenze di un elemento invertibile del gruppo $U(\mathbb{Z}_n)$. In realtà tale proprietà è del tutto generale, ed è in tale forma che ne forniremo una dimostrazione:

Teorema di Fermat astratto: *Sia $(G, \cdot)$ un gruppo finito. Allora per ogni elemento a di G si ha*

$$a^{|G|} = 1.$$

Nel caso in cui $G = U(\mathbb{Z}_n)$ si ritrova esattamente il risultato di Fermat-Eulero, in quanto sappiamo che $\varphi(n)$ è proprio la cardinalità di $U(\mathbb{Z}_n)$.

Uno strumento basilare per la dimostrazione è il seguente.
Def: Sia $(G, \dot{})$ un gruppo e $a \in G$ un suo elemento. L'applicazione

$$L_a : G \to G,$$

definita da

$$L_a(x) := a \cdot x$$

si chiama **traslazione a sinistra** relativa all'elemento a.

Fatto importante: Ogni traslazione $L_a : G \to G$ è una bigezione.

Infatti, L_a è ingettiva perchè, se $x, y \in G$ sono tali che:

$$L_a(x) = L_a(y),$$

allora

$$a \cdot x = a \cdot y$$

e quindi basta applicare la legge di cancellazione per concludere che

$$x = y.$$

Surgettività: dato $y \in G$, una preimmagine $x \in G$ è un elemento tale che

$$L_a(x) = y$$

ovvero

$$a \cdot x = y.$$

Tale equazione si può risolvere in G facendo uso degli assiomi di gruppo: moltiplicando ambo i membri per a^{-1} si ottiene subito

$$x = a^{-1} \cdot y.$$

Tale elemento è effettivamente una preimmagine di y; verifica:

$$L_a(a^{-1}y) = a \cdot (a^{-1} \cdot y) = (a \cdot a^{-1}) \cdot y = 1 \cdot y = y.$$

DIMOSTRAZIONE DEL TEOREMA DI FERMAT NEL CASO ABELIANO

Trattiamo prima il caso di un gruppo abeliano $(G, \cdot)$. Posto $n = |G|$, supponiamo

$$G = \{x_1, \ldots, x_n\}$$

dove $x_i \neq x_j$.
Fissato $a \in G$ vogliamo provare che

$$a^n = 1.$$

A tal scopo notiamo che, essendo la traslazione $L_a : G \to G$ una bigezione, gli elementi

$$a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n$$

sono esattamente gli stessi elementi $x_1, \ldots, x_n$ di G, permutati tra loro. Pertanto, siccome l'operazione del gruppo è commutativa, vale l'uguaglianza:

$$x_1 \cdots x_2 \cdots x_n = (a \cdot x_1) \cdot (a \cdot x_2) \cdots (a \cdot x_n).$$

in quanto il risultato dell'operazione al primo membro non dipende dall'ordine dei fattori coinvolti.
D'altra parte, ancora per le proprietà associativa e commutativa, possiamo riordinare gli elementi al secondo membro, in modo da far comparire prima le varie istanze di a, che sono n, ottenendo:

$$x_1 \cdots x_2 \cdots x_n = \underbrace{(a \cdots a)}_{n \text{ volte}} \cdot x_1 \cdots x_2 \cdots x_n$$

ovvero

$$x_1 \cdots x_2 \cdots x_n = a^n \cdot x_1 \cdots x_2 \cdots x_n.$$

A questo punto basta utilizzare la legge di cancellazione per concludere che

$$1 = a^n.$$

Da notare che in questo caso rientra il Teorema di Fermat-Eulero, perchè esso riguarda il gruppo $U(\mathbb{Z}_n)$, che è abeliano.

Prima di trattare il caso generale, è conveniente procedere con la teoria dei gruppi, sviluppando il concetto di sottogruppo.

SOTTOGRUPPI

Def: Sia $(G, \cdot)$ un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice un **sottogruppo** se:

1) Per ogni $a, b \in H$ si ha che $a \cdot b \in H$;

2) Per ogni $a \in H$ risulta $a^{-1} \in H$.

Fatto importante: Se H è un sottogruppo, allora l'elemento neutro 1 di G appartiene necessariamente a H.

Infatti, fissato un elemento $a \in H$ (cosa possibile perchè per definizione $H \neq \emptyset$), allora stante la proprietà 2) di cui sopra, $a^{-1} \in H$; applicando la 1) segue $1 = a \cdot a^{-1} \in H$.

Il termine "sottogruppo" è giustificato dal fatto seguente:

Prop: *Ogni sottogruppo H di un gruppo $(G, \cdot)$ è esso stesso un gruppo, rispetto all'operazione ristretta*

$$\cdot : H \times H \to H.$$

Infatti, l'operazione ristretta ha senso per la proprietà 1), che garantisce che il prodotto di elementi di H è sempre un elemento di H. È chiaro che tale operazione resta associativa. Per quanto già osservato, sappiamo che $1 \in H$ e naturalmente tale elemento è ancora elemento neutro. Infine, grazie alla 2), ogni $a \in H$ è invertibile: l'inverso è sempre a^{-1}.

Esempi:

- L'insieme dei numeri interi pari è un sottogruppo di $(\mathbb{Z}, +)$.

  Più in generale, se $m \in \mathbb{Z}$, l'insieme $H = \{km | \, k \in \mathbb{Z}\}$ dei multipli di m è un sottogruppo.

- L'insieme $H = \{x \in \mathbb{Q} | x > 0\}$ è sottogruppo di $(\mathbb{Q}^*, \dot{})$, perchè il prodotto di numeri razionali positivi è positivo, e l'inverso di un numero positivo ha lo stesso segno.

  Invece $H' = \{x \in \mathbb{Q} | \, x < 0\}$ non lo è, perchè la proprietà 1) non è soddisfatta.

- $H = \{[0]_6, [2]_6, [4]_6\}$ è sottogruppo di $(\mathbb{Z}_6, +)$. Infatti abbiamo $[2]_6 + [4]_6 = [0]_6 \in H$, e quindi la 1) è certamente soddisfatta (non occorre controllare le somme di $[0]_6$ con gli altri elementi). Per quel che riguarda 2) abbiamo:

$$-[2]_6 = [4]_6 \in H, \; -[4]_6 = [2]_6 \in H.$$

IL SOTTOGRUPPO GENERATO DA UN ELEMENTO

Siano $(G, \cdot)$ un gruppo e $a \in G$.

Si pone

$$< a >:= \{ a^m \mid m \in \mathbb{Z} \}$$

Cioè $< a >$ è l'insieme di tutte le potenze di a.

Proposizione: *$< a >$ è un sottogruppo di G, ed è sempre un gruppo abeliano.*

Def: Il sottogruppo $< a >$ si chiama **sottogruppo generato da** a.

Nota: Se $a = 1$ allora $< a >= \{1\}$.
$< a >$ contiene sempre gli elementi 1 ed a.

La dimostrazione è un' immediata applicazione delle proprietà delle potenze: infatti date due potenze a^h e a^k, allora

$$(a^h) \cdot (a^k) = a^{h+k}$$

è ancora elemento di $< a >$. Inoltre l'inverso di una potenza di a è anch'esso una potenza:

$$(a^n)^{-1} = a^{-n}.$$

Infine, risulta

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

per cui $(< a >, \cdot)$ è un gruppo abeliano.

Esempi: -In $(\mathbb{Z}, +)$ abbiamo

$$< 2 >= \{\text{numeri pari }\}.$$

-In $(\mathbb{Q}^*, \cdot)$:

$$< -1 >= \{1, -1\}, \ < \frac{1}{3} >=< 3 >= \{ 3^k \mid k \in \mathbb{Z} \}.$$

- In $(\mathbb{Z}_5^*, \cdot)$ risulta $< [2]_5 >= \{[1]_5, [2]_5, [4]_5, [3]_5\} = \mathbb{Z}_5^*$.
Infatti, le classi $[1]_5, [2]_5, [4]_5, [3]_5$ si ottengono, in quest'ordine, calcolando le potenze di $[2]_5$ con esponenti 0,1,2,3. Poichè $[2]_5^4 = [16]_5 = [1]_5$, le successive potenze a esponente positivo si ripetono e sono tutte uguali a queste.
Si osservi che essendo $[2]_5^{-1} = [3]_5$, non occorre di fatto calcolare le potenze a esponente negativo.

IL TEOREMA DI LAGRANGE E SUA APPLICAZIONE AL TEOREMA DI FERMAT

Sia $(G, \cdot)$ un gruppo **finito** e sia $n := |G|$. la cardinalità, che spesso si si chiama anche l'**ordine** del gruppo.

L'ordine di un gruppo e l'ordine dei suoi sottogruppi sono correlati secondo il seguente risultato importante:

Teorema (Lagrange): *Se H è un sottogruppo del gruppo finito G, allora l'ordine di H divide l'ordine di G.*

Come applicazione, possiamo dimostrare il Teorema di Fermat astratto nel caso di un gruppo qualsiasi.

Dato un gruppo $(G, \cdot)$, fissato $a \in G$, abbiamo che $a \in < a >$, ed il sottogruppo $< a >$ è un gruppo abeliano. Quindi, per il caso già esaminato, sappiamo che:

$$a^{|<a>|} = 1.$$

D'altra parte, per il teorema di Lagrange:

$$|G| = k\,|< a >|$$

per un certo intero positivo k, per cui:

$$a^{|G|} = a^{k|<a>|} = \left(a^{|<a>|}\right)^k = 1^k = 1.$$

Osservazione utile: Una conseguenza del Teorema di Fermat è che l'inverso di ogni elemento a di un gruppo finito è una sua potenza: precisamente

$$a^{-1} = a^{|G|-1}.$$

Infatti $a^{|G|-1} \cdot a = a^{|G|} = 1 = a \cdot a^{|G|-1}$.

Ad esempio, in $U(\mathbb{Z}_n)$, l'inverso di $[a]_n$ si può ricavare calcolando $a^{\varphi(n)-1}$ modulo n.

Altra conseguenza: affinchè un sottoinsieme H non vuoto di un gruppo *finito* sia un sottogruppo, basta che soddisfi la prima condizione della definizione: ovvero basta controllare che per ogni $a, b \in H$, $a \cdot b \in H$. Tale condizione si abbrevia dicendo che H è *chiuso* per l'operazione del gruppo.

Infatti, se ciò è vero, allora per ogni $a \in H$ si ha automaticamente che $a^{-1} \in H$, essendo a^{-1} prodotto di elementi di H, in quanto potenza di a.

Attenzione: questa scorciatoia non si applica nel caso di gruppi infiniti!

LATERALI DI UN SOTTOGRUPPO

Def: Sia H un sottogruppo del gruppo $(G, \cdot)$. Si chiama **laterale** (sinistro) di H ogni sottoinsieme di G del tipo

$$aH = \{a \cdot h | \, h \in H\},$$

dove $a \in G$ è un fissato elemento di G.

Il laterale in questione è quindi ottenuto moltiplicando per a tutti gli elementi del sottogruppo. Le seguenti proprietà dei laterali sono utili:

- Se $a \in H$, allora $aH = H$.

  Infatti, ogni prodotto $a \cdot h$ con $h \in H$ coinvolgendo due elementi di H, deve appartiene a H per la prima proprietà dei sottogruppi. Quindi vale l'inclusione $aH \subset H$. Viceversa, se $h \in H$, allora possiamo scrivere h come

  $$h = a \cdot (a^{-1} \cdot h)$$

  e quindi $h \in aH$ perchè per la seconda proprietà dei sottogruppi, $a^{-1} \in H$, pertanto anche $a^{-1} \cdot h$ appartiene al sottogruppo.

- Se $a \notin H$, allora $1 \notin aH$. In particolare, aH non è un sottogruppo e quindi $aH \neq H$.

  Infatti, se fosse $1 = ah$ con $h \in H$, seguirebbe $a = h^{-1} \in H$.

- Ogni laterale aH è un insieme equipotente a H.

  Infatti, la restrizione della traslazione $L_a : H \to aH$ è una bigezione tra i due insiemi.

  Proposizione: *I laterali di un sottogruppo costituiscono una partizione del gruppo.*

  Si tratta di mostrare che ogni $a \in G$ appartiene ad uno ed un solo laterale. Esso è aH; infatti, intanto abbiamo $a = a \cdot 1$, per cui certamente $a \in aH$. Mostriamo che aH è l'unico laterale a cui a appartiene. Supponiamo che si abba anche $a \in bH$ per un certo $b \in G$, e proviamo che

  $$aH = bH.$$

  Infatti, siccome $a \in bH$, allora si ha:

  $$a = b \cdot h$$

  per un certo $h \in H$. Segue che

  $$aH = (b \cdot h)H = b(hH) = bH$$

  perchè $hH = H$.

DIMOSTRAZIONE DEL TEOREMA DI LAGRANGE

Dato un gruppo finito $(G, \cdot)$, con $|G| = n$, sia H un suo sottogruppo. Dobbiamo provare che $|G|$ è un multiplo di $|H|$. Utilizzeremo a tal fine la partizione costituita dai laterali di H: siano

$$a_1H, \ldots, a_kH$$

i laterali distinti.

Chiaramente, per definizione di partizione, tali insiemi sono a due a due disgiunti e la loro unione coincide con l'intero gruppo G:

$$G = a_1H \cup \cdots \cup a_kH.$$

Ma allora (principio della somma):

$$|G| = |a_1H| + \cdots + |a_kH| = k|H|$$

perchè, come sappiamo, ciascun laterale è equipotente al sottogruppo H.

Esempio: Come illustrazione della dimostrazione e del concetto di laterale, consideriamo in $\mathbb{Z}_{15}$ il sottogruppo

$$H = \{[0]_{15}, [5]_{15}, [10]_{15}\}.$$

Il laterale $[2]_{15} + H$ (qui la notazione è additiva) si ottiene sommando $[2]_{15}$ a tutti gli elementi di H:

$$[2]_{15} + H = \{[2]_{15}, [7]_{15}, [12]_{15}\}.$$

Analogamente:

$$[3]_{15} + H = \{[3]_{15}, [8]_{15}, [13]_{15}\}.$$

$$[4]_{15} + H = \{[4]_{15}, [9]_{15}, [14]_{15}\}.$$

$$[6]_{15} + H = \{[6]_{15}, [11]_{15}, [1]_{15}\}.$$

Non vi sono altri laterali diversi da questi e da H. Essi costituiscono la partizione di $\mathbb{Z}_{15}$ descritta nella dimostrazione; in tal caso vi sono quindi 5 blocchi, tutti di cardinalità 3, pari all'ordine del sottogruppo H considerato, in accordo col fatto che l'ordine di $\mathbb{Z}_{15}$ è $15 = 3 \cdot 5$.

GRUPPI CICLICI

Def: Un gruppo $(G, \cdot)$ si dice **ciclico** se esiste un elemento $a \in G$ tale che

$$G =< a > .$$

In tal caso, a si dice un **generatore** di G.

Nota importante: In un gruppo G la cui operazione è denotata con $+$, la potenza di un elemento

$$a^n$$

prende il nome più opportunamente di **multiplo secondo** n di a e si denota con

$$na.$$

Quindi, cambiando opportunamente la simbologia (senza modificare la sostanza del concetto), se $m \in \mathbb{N}$, $m > 0$:

$$ma = \underbrace{a + a \cdots + a}_{m \text{ volte}}$$

mentre per $m = 0$

$$0a = 0.$$

Se $m \in \mathbb{Z}$ con $m < 0$ allora, per definizione:

$$ma = (-m)\,(-a).$$

Dunque, in tal caso scriviamo $< a >= \{m\, a |\, m \in \mathbb{Z}\}$.

In definitiva, un gruppo ciclico G è un gruppo costituito da tutte e sole le potenze/multipli (a seconda della notazione) di un suo certo elemento a.

Due Esempi fondamentali:

- $(\mathbb{Z}, +)$ è ciclico. Infatti $\mathbb{Z} =< 1 >$ avendosi che ogni intero n si può scrivere

$$n = n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ volte}}.$$

- $(\mathbb{Z}_n, +)$ è ciclico. Un generatore è $[1]_n$. Infatti, se a è un intero positivo:

$$[a]_n = \underbrace{[1 + 1 + \cdots + 1]_n}_{a \text{ volte}} = \underbrace{[1]_n + \cdots + [1]_n}_{a \text{ volte}} = a[1]_n.$$

• In un gruppo qualsiasi G, il sottogruppo $< a >$ generato da qualsiasi elemento è un gruppo ciclico.

PERIODO DI UN ELEMENTO

Def: Siano $(G, \cdot)$ un gruppo e $a \in G$. Diremo che a ha **periodo (o ordine) finito** se il sottogruppo $< a >$ è finito. In tale caso, si chiama **ordine o periodo di** a l'ordine (cardinalità) del gruppo $< a >$, che si denota con $o(a)$.

Se $< a >$ è infinito (questo può accadere solo se G lo è), si dice che a ha **periodo infinito**. Si scrive anche $o(a) = \infty$.

Oss: Ovviamente, tutti gli elementi di un gruppo finito hanno ordine finito ($< a >$ è un sottoinsieme di G).

Es: In $(\mathbb{Q}^*, \cdot)$ abbiamo $o(-1) = 2$, perchè $< -1 >= \{1, -1\}$, mentre $o(3) = \infty$, perchè $< 3 >= \{3^k | \, k \in \mathbb{Z}\}$ e tale insieme è infinito (è equipotente a $\mathbb{Z}$).
In $(\mathbb{Z}, +)$ abbiamo $o(0) = 1$ in quanto $< 0 >= \{0\}$, mentre ogni numero $m \neq 0$ ha ordine infinito, in quanto $< m >= \{km|, k \in \mathbb{Z}\}$.
In generale, l'ordine dell'elemento neutro 1 di un gruppo $(G, \cdot)$ è sempre 1, avendosi $< 1 >= \{1\}$.
La circostanza che il periodo sia finito è caratterizzata dal risultato seguente, che chiarisce anche il significato dell'ordine in questo caso:

Teorema: *Siano $(G, \cdot)$ un gruppo e $a \in G$ un suo elemento. Allora a ha periodo finito se e solo se esiste $k \in \mathbb{N}$, $k > 0$, tale che*

$$x^k = 1.$$

In tal caso, $o(a)$ è il più piccolo numero $n \in \mathbb{N}^*$ tale che $a^n = 1$ e si ha che:

$$< a >= \{1, a, a^2, \ldots, a^{n-1}\}.$$

Infine, se a ha periodo finito n, le potenze di a si ripetono secondo il seguente schema:

$$a^s = a^t \iff s \equiv_n t.$$

La caratterizzazione dell'altra possibilità è invece la seguente:
Teorema: *Un elemento $a \in G$ di un gruppo $(G, \cdot)$ ha ordine infinito se e solo se tutte le potenze a^k di a al variare di $k \in \mathbb{Z}$ sono distinte tra loro.*

Questo segue direttamente dal primo Teorema, in base all'osservazione seguente:
affermare che esiste $k \in \mathbb{N}^*$ per cui $a^k = 1$ equivale a dire che esistono due potenze coincidenti $a^m = a^n$ di a con esponenti diversi $m \neq n$.
Infatti, da $a^k = 1$ con $k > 0$ segue $a^k = a^0$. Viceversa, se $a^m = a^n$ con $m > n$, allora moltiplicando per a^{-n} si ottiene

$$a^m \cdot a^{-n} = 1$$

ovvero

$$a^{m-n} = 1.$$

Esempio: Se $o(a) = 5$ allora $a^{-3} = a^2$, $a^{18} = a^3$.

Esempio: Calcoliamo $o([4]_6)$ in $\mathbb{Z}_6$ tenendo presente la prima affermazione del primo Teorema; si tratta di calcolare i multipli di $[4]_6$, fermandosi al primo multiplo $m[4]_6$ con $m > 0$, uguale a $[0]_6$. Risulta:

$$0[4]_6 = 0,\ 1[4]_6 = [4]_6,\ 2[4]_6 = [8]_6 = [2]_6,\ 3[4]_6 = [12]_6 = [0]_6.$$

Dunque $o([4]_6) = 3$. Il sottogruppo generato da tale elemento ha quindi 3 elementi, che sono tutti i multipli che abbiamo calcolato:

$$< [4]_6 >= \{[0]_4, [4]_6, [2]_6\}.$$

Nota: Si noti he, per il Teorema di Lagrange, nel caso di un gruppo finito G, l'ordine di qualsiasi elemento dev'essere *un divisore* dell'ordine $|G|$ del gruppo stesso.

Proposizione: *Sia G un gruppo qualsiasi e a un elemento di periodo $o(a) = n$. Allora il periodo di una sua potenza a^k è*

$$o(a^k) = \frac{n}{MCD(n,k)}.$$

Come applicazione, abbiamo una formula diretta per calcolare il periodo di tutti gli elementi di $\mathbb{Z}_n$:

Corollario: *Il periodo di $[a]_n$ in $(\mathbb{Z}_n, +)$ è dato da $\frac{n}{MCD(a,n)}$.*

Infatti, sappiamo che $[1]_n$ è un generatore di $\mathbb{Z}_n$, cioè $< [1]_n >= \mathbb{Z}_n$, per cui $o([1]_n) = n$. Ogni altra classe $[a]_n$ può vedersi come multiplo $a[1]_n$, e quindi si può applicare il risultato precedente.

Corollario: *Se G è un gruppo ciclico finito di ordine n, con generatore a, allora tutti e soli i generatori sono le potenze a^k tali che $MCD(k,n) = 1$.*

Infatti, tutti gli elementi di G sono del tipo a^k; abbiamo che $< a^k >= G$ se e solo se $| < a^k > | = n$ ovvero $o(a^k) = n$, il che accade se e solo se $\frac{n}{MCD(k,n)} = n$ o equivalentemente $MCD(k,n) = 1$.

Conseguenza: *I generatori di $(\mathbb{Z}_n, +)$ sono tutte e sole le classi $[a]_n$ tali che $MCD(a,n) = 1$, cioè gli elementi invertibili di $(\mathbb{Z}_n, \cdot)$.*

Dunque il numero dei generatori di $\mathbb{Z}_n$ è dato da $\varphi(n)$. Più in generale, ciò vale se G è un gruppo finito di ordine n.

SOTTOGRUPPI DI GRUPPI CICLICI

Il seguente teorema permette facilmente di determinare tutti i sottogruppi di un gruppo ciclico.

Teorema: *Sia $(G, \cdot)$ un gruppo ciclico. Allora:*
1) Tutti i sottogruppi di G sono ciclici.

2) Se G è finito, allora per ogni divisore positivo k di $n = |G|$ vi è uno ed un solo sottogruppo di G di ordine k.

Esempio: $\mathbb{Z}_5$ ha solo due sottogruppi: $\{[0]_5\}$ e $\mathbb{Z}_5$. Più in generale, $\mathbb{Z}_p$ con $p > 0$ numero primo possiede soltanto i sottogruppi cosiddetti banali $\{[0]_p\}$ e $\mathbb{Z}_p$.

Riassumendo, abbiamo i seguenti metodi che possiamo applicare per risolvere dei problemi standard in un gruppo ciclico finito G, con $|G| = n$, di cui sia noto un generatore a:

a) DETERMINARE TUTTI I GENERATORI: Sono gli elementi a^k dove $k > 0$ è primo con n

b) DETERMINARE TUTTI I SOTTOGRUPPI: Per ogni divisore k di n, vi è il sottogruppo $K =< a^q >$ dove $q = \frac{n}{k}$.

c) DETERMINARE TUTTI GLI ELEMENTI DI PERIODO ASSEGNATO k: Detto K il sottogruppo con $|K| = k$, basta determinarne tutti i generatori, riconducendosi al problema di tipo a).

Esempio: Determiniamo tutti i sottogruppi di $\mathbb{Z}_{12}$ e gli elementi di periodo 6.

Abbiamo $12 = 3 \cdot 4$, per cui, a parte i sottogruppi banali $\{[0]_{12}\}$ e $\mathbb{Z}_{12}$, vi sono esattamente quattro sottogruppi, K_1, K_2 e K_3, K_4 di ordini rispettivamente 2, 3, 4 e 6. Il primo è

$$K_1 =< [6]_{12} >= \{[0]_{12}, [6]_{12}\}$$

che si ottiene scegliendo come generatore $[6]_{12}$, in quanto $\frac{12}{2} = 6$; il secondo è

$$K_2 =< [4]_{12} >= \{[0]_{12}, [4]_{12}, [8]_{12}\}$$

il cui generatore è individuato tenendo conto che $\frac{12}{3} = 4$,, il terzo è

$$K_3 =< [3]_{12} >= \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\},$$

ottenuto in corrispondenza di $\frac{12}{4} = 3$, ed infine abbiamo

$$K_4 =< [2]_{12} >= \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\},$$

il cui generatore è ottenuto da $\frac{12}{6} = 2$.

Gli elementi di periodo 6 sono necessariamente i generatori di K_4, che si ottengono scegliendo i seguenti multipli del generatore $[2]_{12}$:

$$[2]_{12},\ 5[2]_{12} = [10]_{12}.$$

TEOREMA DELL'ELEMENTO PRIMITIVO

Il seguente risultato è notevole:

Teorema: *Sia* $(\mathbb{K}, +, \cdot)$ *un campo finito. Allora il gruppo* $(\mathbb{K}^*, \cdot)$ *è ciclico.*

In particolare:

Corollario: *Per ogni primo* $p > 0$*, il gruppo* $(\mathbb{Z}_p^*, \cdot)$ *è un gruppo ciclico.*

Def: Se $\mathbb{K}$ è un campo finito, ogni **generatore** di $(\mathbb{K}^*, \cdot)$ si chiama un **elemento primitivo** del campo.

Attenzione: Un risultato del genere non vale per il gruppo $U(\mathbb{Z}_n)$ degli elementi invertibili dell'anello $\mathbb{Z}_n$, che in diversi casi risulta **non** essere ciclico.

Esempio: Un elemento primitivo di $\mathbb{Z}_{11}$ è $[2]_{11}$. Infatti, $[2]_{11}$ ha periodo 10 perchè entrambe le potenze

$$[2]_{11}^2 = [4]_{11}, \ [2]_{11}^5 = [6]_{11}$$

sono diverse da $[1]_{11}$. Siccome il periodo di un elemento di $\mathbb{Z}_{11}^*$, dovendo dividere 10, può essere solo 1,2,5 o 10 possiamo concludere che $o([2]_{11}) = 10$.

Nota: Attualmente **non** si conosce alcuna formula per calcolare direttamente un elemento primitivo in $\mathbb{Z}_p$, occorre procedere per tentativi.

È stato dimostrato che [2] è primitivo nei campi $\mathbb{Z}_p$ dove

$$p = 4q + 1, \quad q \text{ primo} .$$

OMOMORFISMI

Definizione: Siano $(G, \cdot)$ e $(H, *)$ due monoidi, con elementi neutri rispettivamente 1_G e 1_H.
Un'applicazione $f : G \to H$ si dice un **omomorfismo** se
1) Per ogni $x, y \in G$ si ha: $f(x \cdot y) = f(x) * f(y)$,
2) $f(1_G) = 1_H$.

Un omomorfismo bigettivo si dice un **isomorfismo.** Due monoidi si dicono **isomorfi** se esiste almeno un isomorfismo tra essi.

Nota: Si verifica facilmente che, se $f : G \to H$ è un isomorfismo, tale è la funzione inversa $f^{-1} : H \to G$.

Nota: Due monoidi isomorfi rappresentano due "forme" o "rappresentazioni" dello stesso oggetto matematico.

Esempio: L'applicazione $f : (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$ definita da

$$f(n) = 2^n$$

è un omomorfismo di monoidi. Non è un isomorfismo perchè non è surgettiva. Abbiamo infatti:

$$f(n + m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m)$$

e inoltre $f(0) = 2^0 = 1$.

Esempio: La funzione $f : (\mathbb{Q}, +) \to (\mathbb{Q}, +)$ definita da

$$f(x) = \frac{5}{3}\, x$$

è un isomorfismo di monoidi (si dice anche che è un automorfismo del monoide $(\mathbb{Q}, +)$).
Infatti,

$$f(x + y) = \frac{5}{3}\,(x + y) = \frac{5}{3}\, x + \frac{5}{3}\, y = f(x) + f(y)$$

e inoltre $f(0) = 0$. Inoltre, f è bigettiva.

OMOMORFISMI TRA GRUPPI

Nel caso dei gruppi, gli omomorfismi sono caratterizzati dalla prima delle due proprietà 1) e 2) di cui sopra:

Prop: *Siano* $(G, \cdot)$ *e* $(H, *)$ *due gruppi. Affinchè un'applicazione* $f : G \to H$ *sia un omomorfismo è sufficiente che*

$$f(x \cdot y) = f(x) * f(y)$$

per ogni $x, y \in G$.
Infatti, in tal caso abbiamo

$$f(1_G) = f(1_G \cdot 1_G) = f(1_G) * f(1_G)$$

da cui, applicando la legge di cancellazione nel gruppo $(H, *)$ segue

$$1_H = f(1_G).$$

In particolare, un isomorfismo tra due gruppi è semplicemente una bigezione $f : G \to H$ che soddisfa

$$f(x \cdot y) = f(x) * f(y)$$

per ogni $x, y \in G$.

Esempio: I gruppi $(\mathbb{Z}_3^*, \cdot)$ e $(\mathbb{Z}_2, +)$ sono isomorfi: un isomorfismo è dato dalla funzione

$$f : \mathbb{Z}_2 \to \mathbb{Z}_3^*$$
$$\underline{0} \mapsto 1, \ \underline{1} \mapsto \underline{2}.$$

Infatti possiamo verificare direttamente che:

$$f(\underline{0} + \underline{0}) = f(\underline{0}) = \underline{1} = f(\underline{0}) \cdot f(\underline{0})$$
$$f(\underline{0} + \underline{1}) = f(\underline{1}) = \underline{2} = f(\underline{0}) \cdot f(\underline{1})$$
$$f(\underline{1} + \underline{1}) = f(\underline{0}) = \underline{1} = f(\underline{1}) \cdot f(\underline{1}).$$

Nota: Ogni omomorfismo tra gruppi $f : G \to H$ "preserva gli inversi" nel senso che per ogni $x \in G$ si ha $f(x^{-1}) = f(x)^{-1}$. Lo dimostreremo in seguito. Dunque f preserva le potenze:

$$f(x^k) = f(x)^k$$

per ogni $k \in \mathbb{Z}$. Questa osservazione fa prevedere che gruppi ciclici con la stessa cardinalità siano isomorfi, in quanto costituiti dalle potenze di un fissato generatore: l'idea è far corrispondere un generatore del primo gruppo ad un generatore dell'altro. Ciò viene discusso nel prossimo paragrafo.

LA CLASSIFICAZIONE DEI GRUPPI CICLICI

Il risultato seguente è importante, in quanto stabilisce che vi sono essenzialmente solo due tipologie di gruppi ciclici: $\mathbb{Z}$ e $\mathbb{Z}_n$. Ogni altro è una "copia" di uno di tali modelli.

Teorema: *1) Ogni gruppo ciclico infinito è isomorfo a* $\mathbb{Z}$.
Più precisamente, se $(G, \cdot)$ *è ciclico infinito, con generatore* a, *allora l'applicazione*

$$f : \mathbb{Z} \to G$$

definita ponendo

$$f(n) := a^n$$

è un isomorfismo.

2) Ogni gruppo ciclico finito è isomorfo a $\mathbb{Z}_n$ *dove* n *è l'ordine del gruppo.*
Più precisamente, se $(G, \cdot)$ *è ciclico con generatore* a, *e* $n = |G|$, *allora l'applicazione*

$$f : \mathbb{Z}_n \to G$$

tale che

$$f([k]_n) := a^k$$

è ben definita ed è un isomorfismo.

Esempio: Consideriamo il gruppo $H = \{2n | n \in \mathbb{Z}\}$ costituito dai numeri interi pari. Esso è un sottogruppo di $(\mathbb{Z}, +)$ ed è ciclico perchè $H =< 2 >$.
Allora H, essendo infinito, è isomorfo a $\mathbb{Z}$. Tenendo conto del punto 1) del Teorema, possiamo esplicitare un isomorfismo

$$f : \mathbb{Z} \to H$$

ponendo

$$f(n) = n2 = 2n.$$

Esempio: Il gruppo $U(\mathbb{Z}_9)$ degli elementi invertibili dell'anello $\mathbb{Z}_9$ è ciclico. Infatti, ricordando che gli elementi invertibili sono le classi $[a]_9$ con $MCD(a, 9) = 1$, abbiamo

$$U(\mathbb{Z}_9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}.$$

L'ordine del gruppo è 6 $(= \varphi(9))$. Risulta che $a = [2]_9$ è un generatore, perchè

$$a^3 = [8]_9 \neq [1]_9.$$

Ciò basta per dedurre che $o(a) = 9$, in quanto a priori l'ordine di ogni elemento deve dividere 9, ovvero è sempre è uno dei numeri 1, 3 oppure 9.
Conclusione: il gruppo in questione è isomorfo a $\mathbb{Z}_6$. Un isomorfismo $f : \mathbb{Z}_6 \to U(\mathbb{Z}_9)$ si può costruire tenendo conto della parte 2) del Teorema precedente:

$$f([0]_6) = [2]_9^0 = [1]_9,\ f([1]_6) = [2]_9^1 = [2]_9,\ f([2]_6) = [2]_9^2 = [4]_9,\ f([3]_6) = [2]_9^3 = [8]_9,$$
$$f([4]_6) = [2]_9^4 = [7]_9, f([5]_6) = [2]_9^5 = [5]_9.$$

PRODOTTO DIRETTO DI MONOIDI E DI GRUPPI

Siano $(G, \cdot)$ e $(H, *)$ due monoidi.

Il prodotto cartesiano $G \times H$ può essere munito in modo naturale di una struttura di monoide, la cui operazione è la seguente:

$$(a, x) \cdot (b, y) := (a \cdot b, x * y) \quad \forall a, b \in G \ \forall x, y \in H.$$

Questo monoide si chiama il **prodotto diretto** di G e H.

- L'associatività dell'operazione è conseguenza del fatto che $\cdot$ e $*$ sono associative.
- L'elemento neutro è $(1_G, 1_H)$, dove 1_G e 1_H sono gli elementi neutri dei due monoidi,.
- Se G e H sono entrambi, gruppi, tale è $G \times H$. Per verificarlo, basta osservare: L'inverso di $(a, x) \in G \times H$ è (a^{-1}, x^{-1}).

Se G e H sono due gruppi abeliani, si usa anche la notazione $G \oplus H$ per il loro prodotto diretto.

Esempio: Risulta che il prodotto diretto $\mathbb{Z}_2 \times \mathbb{Z}_3$ è isomorfo a $\mathbb{Z}_6$, sia a livello di gruppi, che a livello di monoidi (ricordiamo che ogni $(\mathbb{Z}_n, +)$ è un gruppo, mentre $(\mathbb{Z}_n, \cdot)$ è solo un monoide). Un isomorfismo standard (che va bene in entrambi i casi) si può definire come segue:

$$f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$$

tale che

$$f([a]_6) := ([a]_2, [a]_3).$$

Questa funzione è ben definita: il valore che assume in $[a]_6$ non dipende dalla scelta di a come rappresentante della classe stessa; infatti, se $a \equiv_6 b$, allora a maggior ragione, è anche $a \equiv_2 b$ e $a \equiv_3 b$, perchè 6 è multiplo sia di 2 che di 3. Se consideriamo ora le operazioni di somma, risulta effettivamente:

$$f([x]_6 + [y]_6) = f([x + y]_6) = ([x + y]_2, [x + y]_3) = ([x]_2 + [y]_2, [x]_3 + [y]_3) =$$
$$= ([x]_2, [x]_3) + ([y]_2, [y]_3) = f([x]_6) + f([y]_6).$$

Dunque f è un omomorfismo tra gruppi. Per il prodotto la verifica è esattamente analoga, e inoltre abbiamo per definizione $f([1]_6) = ([1]_2, [1]_3)$ e quindi f è anche un omomorfismo tra monoidi.
Esplicitando la funzione, possiamo controllare che si tratta di una bigezione:

$$f([0]_6) = ([0]_2, [0]_3),\ f([1]_6) = ([1]_2, [1]_3),\ f([2]_6) = ([0]_2, [2]_3),$$
$$f([3]_6) = ([1]_2, [0]_3),\ f([4]_6) = ([0]_2, [1]_3),\ f([5]_6) = ([1]_2, [2]_3).$$

Dunque f è un isomorfismo.

ANELLI PRODOTTO E ISOMORFISMI

Le nozioni che abbiamo sviluppato nella categoria dei gruppi si estendono in modo naturale alla categoria degli anelli.

Siano $(A, +, \cdot)$ e $(B, +, \cdot)$ due anelli.
Allora coesistono sia il gruppo prodotto $(A \times B, +)$, che è un gruppo abeliano, che il monoide prodotto $(A \times B, \cdot)$.
Risulta che $(A \times B, +, \cdot)$ è a sua volta un anello, che chiameremo ancora **anello prodotto di** A e B.

Occorre verificare che valgono le proprietà distributive. Ad esempio, dati (a, b), (a', b') e (a'', b'') allora si ha:

$$((a,b)+(a',b'))\cdot(a'',b'') = (a+a', b+b')\cdot(a'',b'') = ((a+a')\cdot a'', (b+b')\cdot b'') =$$

$$= (a\cdot a''+a'\cdot a'', b\cdot b''+b'\cdot b'') = (a\cdot a'', b\cdot b'')+(a'\cdot a'', b'\cdot b'') = (a,b)\cdot(a'',b'')+(a',b')\cdot(a'',b'').$$

Osservazione: Riguardo gli elementi invertibili di tale anello $A \times B$, si dimostra facilmente che:

$$U(A \times B) = U(A) \times U(B).$$

Def: Un **omomorfismo** tra gli anelli A e B è un'applicazione $f : A \to B$ che è contemporaneamente un omomorfismo tra i gruppi $(A, +)$ e $(B, +)$ e tra i monoidi $(A, \cdot)$ e $(B, \cdot)$.

Dunque si tratta di una funzione che soddisfa le seguenti condizioni:

$$\forall x, y \in A \quad f(x + y) = f(x) + f(y).$$
$$\forall x, y \in A \quad f(x \cdot y) = f(x) \cdot f(y).$$
$$f(1_A) = 1_B.$$

Un **isomorfismo** tra A e B è un omomorfismo bigettivo.
Discutiamo un esempio significativo, che generalizza quanto esaminato in precedenza in un caso particolare:

Teorema: *Siano m_1 e m_2 due interi positivi primi tra loro. Allora la funzione*

$$f : \mathbb{Z}_{m_1 m_2} \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$$

definita ponendo

$$f([x]_{m_1 m_2}) := ([x]_{m_1}, [x]_{m_2})$$

è un isomorfismo tra gli anelli $\mathbb{Z}_{m_1 m_2}$ e $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.

Questo isomorfismo può rivelarsi utile per effettuare calcoli in $\mathbb{Z}_{m_1 m_2}$ (ad es. calcoli di potenze modulo $m_1 m_2$) in modo più conveniente, svolgendo le operazioni separatamente in $\mathbb{Z}_{m_1}$ e in $\mathbb{Z}_{m_2}$, reintepretando poi il risultato in $\mathbb{Z}_{m_1 m_2}$ mediante la funzione inversa f^{-1}.

Dimostrazione: L'applicazione f è un omomorfismo; ad esempio, considerando le operazioni di somma nei due anelli abbiamo:

$$f([x]_{m_1m_2} + [y]_{m_1m_2}) = f([x+y]_{m_1m_2}) = ([x+y]_{m_1}, [x+y]_{m_2}) =$$

$$= ([x]_{m_1} + [y]_{m_1}, [x]_{m_2} + [y]_{m_2}) = ([x]_{m_1}, [x]_{m_2}) + ([y]_{m_1}, [y]_{m_2}) =$$

$$= f([x]_{m_1m_2}) + f([y]_{m_1m_2}).$$

Discorso analogo si può fare rispetto al prodotto.
La bigettività di f è una conseguenza del Teorema Cinese del resto. Infatti, si fissi un elemento $([b_1]_{m_1}, [b_2]_{m_2})$ di $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$; una sua preimmagine è ogni classe $[x]_{m_1m_2}$ tale che

$$f([x]_{m_1m_2}) = ([b_1]_{m_1}, [b_2]_{m_2}),$$

cioè tale che

$$([x]_{m_1}, [x]_{m_2}) = ([b_1]_{m_1}, [b_2]_{m_2}),$$

o equivalentemente tale che:

$$[x]_{m_1} = [b_1]_{m_1} \text{ e } [x]_{m_2} = [b_2]_{m_2}.$$

Pertanto il problema di determinare le preimmagini consiste nel risolvere il sistema di congruenze:

$$\begin{cases} x \equiv b_1 \,(\bmod m_1) \\ x \equiv b_2 \,(\bmod m_2) \end{cases}.$$

Poichè per ipotesi $MCD(m_1, m_2) = 1$, il teorema cinese del resto è applicabile, e sappiamo che il sistema è risolubile, anzi l'insieme delle soluzioni del sistema è una singola classe $[x_o]_{m_1m_2}$. Pertanto tale classe è l'unica preimmagine di $([b_1]_{m_1}, [b_2]_{m_2})$. Ciò mostra che la funzione è bigettiva.

ANCORA SULLA FUNZIONE DI EULERO

Come applicazione, utilizziamo l'isomorfismo di anelli discusso sopra per dimostrare l'importante proprietà moltiplicativa della funzione di Eulero. Ricordiamo che, se a e b sono interi positivi primi tra loro, abbiamo affermato che:

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Sappiamo che:

$$\varphi(ab) = |U(\mathbb{Z}_{ab})|,\ \varphi(a) = |U(\mathbb{Z}_a)|,\ \varphi(b) = |U(\mathbb{Z}_b)|.$$

Ora, notiamo che in generale, dati due anelli A e B, ogni isomorfismo

$$f : A \to B$$

induce un isomorfismo

$$f : U(A) \to U(B).$$

tra i corrispondenti gruppi degli elementi invertibili. Quindi abbiamo che

$$f : U(\mathbb{Z}_{ab}) \to U(\mathbb{Z}_a \times \mathbb{Z}_b)$$

è un isomorfismo di gruppi. D'altra parte, il gruppo degli elementi invertibili dell'anello prodotto $\mathbb{Z}_a \times \mathbb{Z}_b$ è dato da:

$$U(\mathbb{Z}_a \times \mathbb{Z}_b) = U(\mathbb{Z}_a) \times U(\mathbb{Z}_b).$$

Quindi in definitiva abbiamo che f induce un isomorfismo

$$f : U(\mathbb{Z}_{ab}) \to U(\mathbb{Z}_a) \times U(\mathbb{Z}_b).$$

In particolare, tali gruppi sono equipotenti, e quindi :

$$|U(\mathbb{Z}_{ab})| = |U(\mathbb{Z}_a) \times U(\mathbb{Z}_b)| = |U(\mathbb{Z}_a)||U(\mathbb{Z}_b)|,$$

e pertanto resta provato che:

$$\varphi(ab) = \varphi(a)\varphi(b).$$

ULTERIORI PROPRIETÀ DEGLI OMOMORFISMI

Prop: *Sia $f : G \to H$ un omomorfismo tra i gruppi $(G, \cdot)$ e $(H, \cdot)$.*
Allora:

1) Per ogni $x \in G$ si ha $f(x^{-1}) = f(x)^{-1}$.
2) Per ogni $x \in G$ e $k \in \mathbb{Z}$ si ha: $f(x^k) = f(x)^k$.
3) Se $x \in G$ è un elemento di periodo finito, allora anche $f(x)$ ha periodo finito.

Dimostrazione: 1) Fissato x in G abbiamo:

$$x \cdot x^{-1} = 1_G = x^{-1} \cdot x;$$

applicando f ad ambo i membri si ricava

$$f(x \cdot x^{-1}) = f(1_G) = f(x^{-1} \cdot x);$$

tenendo conto che f è un omomorfismo queste uguaglianze si riscrivono, usando il prodotto in H:

$$f(x) \cdot f(x^{-1}) = f(1_G) = f(x^{-1}) \cdot f(x).$$

D'altra parte sappiamo che $f(1_G) = 1_H$, quindi

$$f(x) \cdot f(x^{-1}) = 1_H = f(x^{-1}) \cdot f(x).$$

Per l'unicità dell'inverso di $f(x)$ in H segue che $f(x^{-1})$ dev'essere l'inverso $f(x)^{-1}$ di $f(x)$.

2) È conseguenza immediata di 1). Riguardo 3), se x ha periodo finito, allora $x^k = 1$ per qualche intero $k > 0$, e quindi $f(x)^k = 1_H$; ciò implica che anche $f(x)$ ha periodo finito.

COSTRUZIONE DI OMOMORFISMI

Abbiamo visto che i gruppi ciclici sono completamente classificati, esibendo degli isomorfismi standard $\mathbb{Z} \to G$, ovvero $\mathbb{Z}_n \to G$ a seconda che si tratti di un gruppo infinito o finito:

$$k \mapsto a^k, \ [k]_n \mapsto a^k$$

dove a è un fissato generatore del gruppo. L'idea fondamentale è che tali isomorfismi sono determinati dall' immagine del generatore 1 ovvero $[1]_n$: in entrambi i casi la funzione assume in tale generatore il valore a.
Estendiamo ora la trattazione, mostrando come sia possibile costruire, seguendo lo stesso principio, tutti gli omomorfismi

$$G \to H$$

tra un gruppo ciclico G e un gruppo qualsiasi H. Osserviamo che tra due gruppi qualsiasi G e H vi è sempre almeno un omomorfismo: la funzione costante $x \mapsto 1_H$.
Trattiamo prima il caso in cui G è infinito.

Teorema: *Sia $G =< a >$ in gruppo ciclico infinito e $(H, \cdot)$ un gruppo qualsiasi. Ogni omomorfismo*

$$f : G \to H$$

è completamente determinato dal valore $f(a)$ che assume nel generatore a di G. Posto $y = f(a)$ si ha:

$$f(a^k) = y^k. \tag{1}$$

Viceversa, assegnato un qualunque elemento y di H, esiste uno ed un solo omomorfismo $f : G \to H$ tale che

$$f(a) = y,$$

che è definito da (1).

Dunque gli omomorfismi $G \to H$, con G ciclico infinito, sono in corrispondenza biunivoca con gli elementi di H.
La (1) è conseguenza immediata $f(a) = y$ in base alla proprietà di f di trasformare potenze di a in potenze di y, che abbiamo discusso. Poichè ogni elemento di G è della forma a^k, la (1) determina completamente la funzione. Viceversa, assegnato y in H, la definizione (1) è ben posta, perchè ogni ogni elemento di G è della forma a^k, per un solo $k \in \mathbb{Z}$ (le potenze di a sono tutte diverse, perchè a ha periodo finito). Tale funzione è un omomorfismo per le proprietà delle potenze:

$$f(a^k \cdot a^s) = a^{k+s} = y^{k+s} = y^k \cdot y^s = f(a^k) \cdot f(a^s).$$

Nota importante: Dato l'omomorfismo $f : G =< a > \to H$ e posto $y = f(a)$, valgono i seguenti criteri:

$$f \text{ è } \textit{surgettivo} \iff H \text{ è ciclico con generatore } y.$$

$$f \text{ è } \textit{ingettivo} \iff y \text{ ha periodo infinito.}$$

Infatti, per costruzione, sempre per (1), l'immagine $f(G)$ della funzione è data da

$$f(G) = \{y^k | \, k \in \mathbb{Z}\}$$

ovvero:

$$f(G) =< y > .$$

Quindi f è surgettivo se solo se $f(G) = H$ cioè $< y >= H$. Invece, f è ingettivo se e solo se tutte le immagini y^k sono distinte, ma ciò accade se e solo se y ha periodo infinito.

Esempio: Vi sono esattamente quattro omomorfismi $f : \mathbb{Z} \to \mathbb{Z}_4$, f_i, ottenuti in corrispondenza dei quattro elementi $y = \underline{0}, \underline{1}, \underline{2}, \underline{3}$. Essi sono determinati dalla condizione:

$$f(1) = y$$

e quindi

$$f_1(n) = n[0]_4 = 0, f_2(n) = n[1]_4 = [n]_4, \; f_3(n) = n[2]_4 = [2n]_4, \; f_4(n) = n[3]_4 = [3n]_4.$$

Dunque per esempio, $f_3(5) = [10]_4 = [2]_4$ e $f_4(-3) = [-9]_4 = [3]_4$.
Di questi, quelli surgettivi sono f_2 e f_4, costruiti in corrispondenza dei generatori di $\mathbb{Z}_4$, che sono $[1]_4$ e $[3]_4$. Ovviamente, nessuno di questo può essere ingettivo: ciò è in accordo col fatto che tutti gli elementi di $\mathbb{Z}_4$ hanno periodo finito.

Esempio: Vi sono infiniti omomorfismi $f_m : \mathbb{Z} \to \mathbb{Z}$, dati da

$$f_m(1) = m$$

al variare di $m \in \mathbb{Z}$.
Ad esempio, $f_{11} : \mathbb{Z} \to \mathbb{Z}$ è l'applicazione definita da

$$f_{11}(n) = 11n.$$

Poichè gli unici generatori di $\mathbb{Z}$ sono 1 e -1, gli unici tra questi ad essere surgettivi sono f_1 e f_{-1}:

$$f_1(n) = n, \; f_2(n) = -n.$$

Esempio: Vi è un unico omomorfismo $f : \mathbb{Z} \to \mathbb{Q}^*$ tale che $f(3) = \frac{1}{8}$. Per determinarlo, posto $f(1) = y$, deve aversi $f(3) = y^3$, cioè $y^3 = \frac{1}{8}$, da cui $y = \frac{1}{2}$. Poichè $\frac{1}{2}$ ha periodo infinito, l'omomorfismo in questione è ingettivo, ma non surgettivo, in quanto $\frac{1}{2}$ chiaramente non è generatore di $\mathbb{Q}^*$ (non tutti i numeri razionali sono sue potenze). Esso è dato da

$$f(n) = y^n = \frac{1}{2^n}.$$

Esempio: Non esistono omomorfismi surgettivi $\mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_2$, perchè $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico (lo si controlli!).

Studiamo ora gli omomorfismi $G \to H$ nel caso in cui G è un gruppo ciclico finito.

Teorema: *Sia $G =< a >$ in gruppo ciclico finito di ordine n e $(H, \cdot)$ un gruppo qualsiasi.*
Ogni omomorfismo

$$f : G \to H$$

è completamente determinato dal valore $f(a)$ che assume nel generatore a di G. Posto $y = f(a)$, allora y è un elemento di periodo finito, divisore di n e si ha:

$$f(a^k) = y^k. \tag{1}$$

Viceversa, assegnato un qualunque elemento y di H, il cui periodo è finito e divide n, esiste uno ed un solo omomorfismo $f : G \to H$ tale che

$$f(a) = y,$$

che è definito da (1).

A differenza quindi del caso in cui G è infinito, non tutti gli elementi di H possono essere scelti come immagine di a, per costruire un omomorfismo: occorre rispettare il vincolo enunciato sul periodo.

Sussistono inoltre i seguenti criteri: dato $f : G =< a >\to H$ con $y = f(a)$:

$$f \text{ è } \textit{surgettivo} \iff H \text{ è finito e } o(y) = |H|.$$
$$f \text{ è } \textit{ingettivo} \iff o(y) = n.$$

Esempio: Vi è un solo omomorfismo $\mathbb{Z}_n \to \mathbb{Z}$ che è quello costante

$$f([x]_n) = 0 \quad \forall [x] \in \mathbb{Z}_n.$$

Infatti, 0 è l'unico elemento di periodo finito di $\mathbb{Z}$.

Esempio: Gli omomorfismi $\mathbb{Z}_6 \to \mathbb{Z}_3$ sono tre, perchè ogni elemento di $\mathbb{Z}_3$ ha periodo finito, che è 1 o 3, e quindi divisore di 6. Essi si ottengono dalle condizioni

$$f_1([1]_6) = [0]_3,\ f_2([1]_6) = [1]_3,\ f_3([1]_6) = [2]_3.$$

Esplicitandoli abbiamo

$$f_1([n]_6) = [0]_3,\ f_2([n]_6) = [n]_3,\ f_2([n]_6) = [2n]_3.$$

Risulta che f_2 e f_3 sono surgettivi, in quanto sia $[1]_3$ che $[2]_3$ sono generatori di $\mathbb{Z}_3$.

Esempio: L'unico omomorfismo $\mathbb{Z}_5 \to \mathbb{Z}_4$ è quello costante $[n]_5 \mapsto [0]_4$, perchè non vi sono elementi di $\mathbb{Z}_4$ di periodo 5 (ricordarsi che il periodo di tutti gli elementi di $\mathbb{Z}_4$ è divisore di 4).

IL GRUPPO DELLE PERMUTAZIONI

Dato un insieme non vuoto A, denoteremo con $S(A)$ l'insieme di tutte le permutazioni di A, ovvero l'insieme di tutte le bigezioni $A \to A$:

$$S(A) = \{f : A \to A |\ f \text{ è bigettiva}\}.$$

Un elemento particolare di tale insieme è la funzione identità (o identica) Id_A, di cui abbiamo già parlato in precedenza: ricordiamo che si tratta della funzione tale che

$$Id_A(x) = x$$

per ogni $x \in A$. L'operazione di composizione di due funzioni, già studiata, determina un'operazione interna

$$\circ : S(A) \times S(A) \to S(A),\ \circ(f, g) := f \circ g$$

perchè sappiamo che la composizione di due bigezioni è ancora una bigezione.

Teorema: $(S(A), \circ)$ *è un gruppo. Esso si chiama* **gruppo delle permutazioni di** A.

Infatti, abbiamo:

- L'operazione $\circ$ è associativa: date le funzioni $f, g, h \in S(A)$ abbiamo

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

  Infatti, ambo i membri sono la funzione che opera in questo modo:

  $$x \in A \mapsto (f(g(h(x))) \in A.$$

- Id_A è l'elemento neutro di $(S(A), \circ)$. Infatti, sappiamo già che:

  $$f \circ Id_A = f = Id_A \circ f.$$

- Ogni elemento $f \in S(A)$ è invertibile; infatti, basta considerare la funzione inversa

  $$f^{-1} : A \to A,$$

  che è anch'essa bigettiva e soddisfa, come già visto precedentemente:

  $$f \circ f^{-1} = Id_A = f^{-1} \circ f.$$

IL GRUPPO SIMMETRICO

Studieremo ora in modo più sistematico le permutazioni di $I_n = \{1, 2, \ldots, n\}$, $n \geq 1$.
Il gruppo $S(I_n)$ si denota con

$$S_n$$

e si chiama **gruppo simmetrico** su n oggetti.

Nel contesto di S_n, la permutazione identica si denota semplicemente con Id o anche con il simbolo 1, trattandosi dell'elemento neutro del gruppo.

Una permutazione $f \in S_n$ si denota con una tabella (o **matrice**) del tipo:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

Esempio: Ad esempio

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

è la permutazione $I_4 \to I_4$ tale che

$$1 \mapsto 3, 2 \mapsto 4, \ 3 \mapsto 2, \ 4 \mapsto 1.$$

La sua inversa f^{-1} è :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Nel seguito, molto spesso, date due permutazioni $f, g \in I_n$ in luogo di $f \circ g$ scriveremo anche $f \cdot g$ o anche fg.
Notiamo che il gruppo S_n non è abeliano (tranne nei casi banali $n = 1$ e $n = 2$); date due permutazioni, solitamente c'è da aspettarsi che $f \circ g \neq g \circ f$.

Nota: Sappiamo che S_n è un gruppo finito, di ordine $|S_n| = n!$.

Ogni elemento $f \in S_n$ ha dunque periodo finito, divisore di $n!$. Ricordiamo che, operativamente, tale ordine è il più piccolo intero positivo k tale che $f^k = Id$.

Ricordiamo anche che, se $o(f) = k$, le potenze di f si ripetono secondo la regola:

$$f^s = f^t \text{ se e solo se } s \equiv t \pmod{k},$$

e abbiamo che il sottogruppo generato da f è il gruppo ciclico $< f >= \{Id, f, f^2, \cdots, f^{k-1}\}$ di ordine k.

CICLI E SCAMBI

Un classe importante di permutazioni è costituita dalle permutazioni **cicliche**:

Definizione: Una permutazione $f \in S_n$ si chiama **ciclo di lunghezza** k, $k \geq 1$, se esistono $a_1, \ldots, a_k \in I_n$ tali che

$$f(a_1) = a_2, \;\; f(a_2) = a_3, \;\; \ldots\ldots \;, f(a_{k-1}) = a_k, \;\; f(a_k) = a_1$$

e

$$f(x) = x \text{ per tutti gli } x \in I_n \setminus \{a_1, \ldots, a_s\}.$$

In tal caso si scrive

$$f = (a_1 \; a_2 \; \cdots \; a_k).$$

Esempio: Il ciclo di S_8

$$(7\; 6\; 4\; 3)$$

è la permutazione

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

Nota: Ogni ciclo (a_1) di lunghezza 1 coincide con la permutazione identica Id.

Def: I cicli di lunghezza 2 si dicono **scambi** (o **trasposizioni**).

Prop: *Ogni ciclo di lunghezza k è un elemento del gruppo S_n di periodo k.*

Esempio: Considerato il ciclo (3 4 5 7) in S_8, abbiamo abbiamo

$$(3\; 4\; 5\; 7)^9 = (3\; 4\; 5\; 7)$$

perchè tale ciclo ha periodo 4 e $9 \equiv 1 \pmod 4$.

Definizione: Due cicli $(a_1 \; a_2 \; \cdots \; a_s)$ e $(b_1 \; b_2 \; \cdots \; b_t)$ di S_n si dicono **disgiunti** se

$$\{a_1, \ldots, a_s\} \cap \{b_1, \ldots, b_t\} = \emptyset.$$

Nota importante: Due cicli disgiunti commutano, nel senso che se f e g sono cicli disgiunti, allora

$$f \circ g = g \circ f.$$

In generale, se due elementi x, y di un gruppo $(G, \cdot)$ commutano, nel senso che

$$x \cdot y = y \cdot x,$$

allora vale la consueta proprietà:

$$(x \cdot y)^k = x^k \cdot y^k$$

per ogni $k \in \mathbb{Z}$.
Attenzione: Se il gruppo non è abeliano, come nel caso di S_n, tale proprietà delle potenze non è applicabile se x e y non commutano.

DECOMPOSIZIONE IN CICLI

Teorema: *Ogni permutazione $f \in S_n$ non identica si scrive come composizione di un numero finito di cicli a due a due disgiunti di lunghezza almeno 2:*

$$f = c_1 \circ \cdots \circ c_s,$$

dove c_i e c_j sono cicli disgiunti per $i \neq j$. Tale scrittura è unica a meno dell'ordine dei fattori.

Inoltre, il periodo di f è dato da:

$$o(f) = \text{minimo comune multiplo di } o(c_1), \ldots, o(c_s).$$

Non diamo una dimostrazione formale di questo fatto, ma ci limitiamo a descrivere un metodo per ottenere la decomposizione.

1. A partire dal numero 1, si applicano a 1 in successione le potenze di f:

   $$f(1), f^2(1), \ldots, f^k(1)$$

   fino a che $f^k(1) = 1$. In tal modo si ottiene il primo ciclo c_1 della decomposizione:

   $$c_1 = (1\ f(1) \cdots\ f^{k-1}(1)).$$

2. Si ripete l'algoritmo a partire dal primo numero p non coinvolto nel ciclo già ottenuto, ottenendo un secondo ciclo $c_2 = (p\ f(p) \cdots\ f^s(p))$.

3. Si continua ripetendo il passo 2 finchè vi sono numeri che non compaiono nei cicli ottenuti nei passi precedenti.

Esempio: La decomposizione in cicli disgiunti della permutazione di S_9:

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

è

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

Essa si ottiene come segue: avendosi, applicando ripetutamente f:

$$1 \mapsto 3 \mapsto 5 \mapsto 1,$$

il primo passo fornisce il ciclo

$$\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}.$$

Quindi si ricomincia da 2, che è il primo numero non coninvolto nel primo passo: risulta, applicando sempre f:

$$2 \mapsto 4 \mapsto 2$$

quindi il secondo ciclo è lo scambio $\begin{pmatrix} 2 & 4 \end{pmatrix}$. Ripartendo da 6 si ottiene

$$6 \mapsto 8 \mapsto 9 \mapsto 6$$

da cui il terzo ciclo $\begin{pmatrix} 6 & 8 & 9 \end{pmatrix}$. Infine $7 \mapsto 7$; ciò dà luogo al ciclo banale $(7) = Id$, che si può ignorare.

Risulta quindi $o(f) = m.c.m(3, 2, 3) = 6$. La decomposizione ottenuta aiuta a calcolare le potenze di f: ad esempio

$$f^5 = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix}^5 \circ \begin{pmatrix} 2 & 4 \end{pmatrix}^5 \circ \begin{pmatrix} 6 & 8 & 9 \end{pmatrix}^2 = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix}^2 \circ \begin{pmatrix} 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 6 & 8 & 9 \end{pmatrix}^2 .$$

Possiamo usare sempre lo stesso algoritmo per decomporre ora $\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}^2$ e $\begin{pmatrix} 6 & 8 & 9 \end{pmatrix}^2$ in cicli disgiunti; teniamo presente che nel calcolare i valori assunti da $\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}^2$, semplicemente ci "spostiamo" di due passi in avanti, usando sempre $\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}$:

$$1 \mapsto 5 \mapsto 3 \mapsto 1.$$

Quindi si tratta ancora di un unico ciclo:

$$\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}^2 = \begin{pmatrix} 1 & 5 & 3 \end{pmatrix}.$$

Osserviamo che il risultato è un ciclo diverso! Analogamente per $\begin{pmatrix} 6 & 8 & 9 \end{pmatrix}^2$; ovviamente il primo numero da cui partire è 6, perchè tutti i numeri precedenti sono fissati e quindi darebbero luogo a cicli di lunghezza 1, tutti da scartare; abbiamo:

$$6 \mapsto 9 \mapsto 8 \mapsto 6$$

per cui

$$\begin{pmatrix} 6 & 8 & 9 \end{pmatrix}^2 = \begin{pmatrix} 6 & 9 & 8 \end{pmatrix}.$$

Conclusione:

$$f^5 = \begin{pmatrix} 1 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 6 & 9 & 8 \end{pmatrix}.$$

Notiamo infine che la decomposizione ottenuta ci informa che $o(f^5) = m.c.m(3, 2, 3) = 6$, in accordo con la formula generale $o(f^5) = \frac{6}{MCD(5,6)} = 6$. Sappiamo infatti che la permutazione in questione f^5 è l'altro generatore del gruppo ciclico $G =< f >$ generato da f.

PERMUTAZIONI PARI E DISPARI

Proposizione: *Ogni permutazione di S_n è prodotto di scambi (non in modo unico).*

Basta infatti notare che ogni ciclo è prodotto di scambi; infatti se il ciclo è $(a_1\ a_2\ \cdots\ a_s)$ risulta:

$$(a_1\ a_2\ \cdots\ a_s) = (a_1\ a_s) \circ (a_1 a_{s-1}) \circ \cdots \circ (a_1 a_2).$$

Es: Si ha $(4\ 5\ 7\ 9) = (4\ 9)(4\ 7)(4\ 5)$.

Si può provare che:
Teorema: *Le rappresentazioni di ogni $f \in S_n$ come prodotto di scambi hanno tutte un numero pari o tutte un numero dispari di fattori.*

Ad esempio, la permutazione identica $Id \in S_5$ si può scrivere $Id = (1\ 2)(1\ 2)$ ma anche $Id = (1\ 2)(1\ 2)(2\ 3)(2\ 3)$.

Ad esempio, la permutazione $f = (13)(12)(45)(67)$ di S_7 si può anche scrivere $f = (13)(12)(67)(23)(45)(32)$. In entrambi casi ho un numero **pari** di scambi, ed f **non** si può scrivere come prodotto di un numero dispari di scambi.

Def: Una permutazione $f \in S_n$ si dice di **classe pari** (risp. **dispari**) se si scrive come prodotto di un numero pari (risp. dispari) trasposizioni.

Si pone

$$A_n := \{ \text{ permutazioni } \textbf{pari} \text{ di } S_n \}$$

Fatto: *A_n è sottogruppo di S_n.*
La dimostrazione è immediata: componendo due permutazioni pari f_1 e f_2, decomposte in s risp. t scambi, allora essa risulta pari perchè prodotto di $s + t$ scambi.

Il gruppo $(A_n, \circ)$ si chiama **Gruppo Alterno** di grado n.

Fatto: Risulta $|A_n| = \frac{n!}{2} = \frac{|S_n|}{2}$.

Infatti, il sottogruppo A_n ammette come laterali solo A_n e l'insieme D_n delle permutazioni dispari: ciò perchè, se t è una qualsiasi permutazione di classe dispari, si ha

$$tA_n = D_n.$$

Quindi nella corrispondente partizione $S_n = A_n \cup D_n$ entrambi i blocchi hanno la stessa cardinalità $\frac{n!}{2}$

MATRICI

Sia $(\mathbb{K}, +, \cdot)$ un campo e siano m, n interi positivi.
Definizione: Una **matrice** A di tipo $m \times n$ (o di tipo (m, n)) ad elementi in $\mathbb{K}$ è una tabella rettangolare costituita da $m \cdot n$ elementi di $\mathbb{K}$ disposti in m righe ed n colonne, e rappresentata nel modo seguente:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \tag{1}$$

Si scrive anche in modo compatto

$$A = (a_{ij}).$$

Nella scrittura $A = (a_{ij})$ converremo sempre che il primo indice (risp. il secondo) indichi la riga (risp. la colonna) occupata dall'elemento a^i_j, che si dice elemento di posto (i, j) di A.

Es: Nel caso $m = 1$ si parla di **matrice riga** (o **vettore riga**) di lunghezza n; una tale matrice è dunque della forma

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

(il primo indice in tal caso è superfluo). Nel caso $n = 1$ si parla invece di **matrice colonna** (o **vettore colonna**) di lunghezza m, ed è una matrice del tipo

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}.$$

Es: $A = \begin{pmatrix} 2 & 1 & 0 \\ \frac{1}{2} & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$ è una matrice di tipo 3x3 a coefficienti in $\mathbb{Q}$ (oppure $\mathbb{R}$), mentre $B = \begin{pmatrix} \underline{1} & \underline{1} & \underline{0} \\ \underline{0} & \underline{0} & \underline{1} \end{pmatrix}$ è una matrice di tipo 2x3 a coefficienti nel campo $\mathbb{Z}_2$.

SOMMA DI MATRICI

Def: L'insieme di tutte le matrici di fissato tipo $m \times n$ ad elementi nel campo $\mathbb{K}$ verrà denotato col simbolo $M_{m,n}(\mathbb{K})$.

Due matrici dello stesso tipo $A, B \in M_{m,n}(\mathbb{K})$ si possono sommare come segue; se $A = (a_{ij})$ e $B = (b_{ij})$, allora per definizione si pone

$$A + B := (a_{ij} + b_{ij})$$

cioè la matrice somma $A + B$ è quella il cui elemento sulla righa i-ma e colonna j-ma è la somma (effettuata in $\mathbb{K}$) degli elementi delle due matrici che occupano la medesima posizione. Poichè $A+B$ è ancora di tipo $m \times n$, otteniamo un'operazione interna

$$+ : M_{m,n}(\mathbb{K}) \times M_{m,n}(\mathbb{K}) \to M_{m,n}(\mathbb{K}).$$

Osserviamo che l'operazione in questione eredita dall'operazione di somma del campo la proprietà commutativa.

Teorema: $(M_{m,n}(\mathbb{K}), +)$ *è un gruppo abeliano.*

Tralasciando la dimostrazione dettagliata, ci limitiamo a mettere in evidenza due fatti salienti: l'elemento neutro di tale gruppo è è la *matrice nulla* ovvero la matrice, denotata semplicemente con 0, i cui elementi sono tutti uguali allo zero di $\mathbb{K}$:

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

Ogni matrice $A = (a^i_j) \in M_{m,n}(\mathbb{K})$ risulta invertibile, perchè ammtte come suo opposto la matrice

$$-A := (-a^i_j).$$

Esesempio: Calcoliamo $A - B$ in $M_{2,3}(\mathbb{Z}_3)$, dove

$$A = \begin{pmatrix} \underline{2} & \underline{0} & \underline{1} \\ \underline{0} & \underline{2} & \underline{2} \end{pmatrix}, \; B = \begin{pmatrix} \underline{0} & \underline{0} & \underline{2} \\ \underline{0} & \underline{0} & \underline{1} \end{pmatrix}.$$

Abbiamo

$$-B = \begin{pmatrix} \underline{0} & \underline{0} & -\underline{2} \\ \underline{0} & \underline{0} & -\underline{1} \end{pmatrix} = \begin{pmatrix} \underline{0} & \underline{0} & \underline{1} \\ \underline{0} & \underline{0} & \underline{2} \end{pmatrix}$$

perchè $-[1]_3 = [-1]_3 = [2]_3$ e $-[2]_3 = [-2]_3 = [1]_3$. Quindi

$$A - B = A + (-B) = \begin{pmatrix} \underline{2} & \underline{0} & \underline{2} \\ \underline{0} & \underline{2} & \underline{1} \end{pmatrix}$$

tenendo conto che $\underline{2} + \underline{2} = \underline{1}$.

IL PRODOTTO RIGHE PER COLONNE

Definiamo ora un'operazione fondamentale tra matrici, detta prodotto righe per colonne.

In prima istanza, si definisce il prodotto tra una matrice riga ed una matrice colonna:

Def: Siano $A = (a_1 \ \dots \ a_n)$ una matrice riga e $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ una matrice colonna **della stessa lunghezza** $n \geq 1$. Si definisce il loro **prodotto** AB come lo scalare

$$AB := a_1b_1 + a_2b_2 + \cdots + a_nb_n \in \mathbb{K}.$$

Es: Abbiamo

$$(1 \ -2 \ 4 \ -1) \begin{pmatrix} 0 \\ -1 \\ 7 \\ 5 \end{pmatrix} = 1 \cdot 0 + (-2)(-1) + 4 \cdot 7 - 5 = 25.$$

Per definire il prodotto di matrici nel caso generale, conviene introdurre una notazione conveniente per rappresentarne le righe e le colonne. Denoteremo l'i-ma riga di una matrice A con il simbolo $A^{(i)}$, mentre useremo $A_{(j)}$ per denotarne la j-ma colonna. Dunque:

$$A^{(i)} = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}, \quad A_{(j)} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

Possiamo rappresentare A per colonne nel modo seguente:

$$A = \begin{pmatrix} A_{(1)} & A_{(2)} & \cdots & A_{(n)} \end{pmatrix},$$

oppure per righe:

$$A = \begin{pmatrix} A^{(1)} \\ A^{(2)} \\ \vdots \\ A^{(m)} \end{pmatrix}.$$

Es: Data la matrice $A = \begin{pmatrix} 5 & 1 & -4 & 2 & 5 \\ 0 & 1 & -1 & 0 & 2 \end{pmatrix}$, abbiamo

$$A^{(1)} = \begin{pmatrix} 5 & 1 & -4 & 2 & 5 \end{pmatrix}, \ A^{(2)} = \begin{pmatrix} 0 & 1 & -1 & 0 & 2 \end{pmatrix},$$

$$A_{(1)} = \begin{pmatrix} 5 \\ 0 \end{pmatrix}, \ A_{(2)} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \ A_{(3)} = \begin{pmatrix} -4 \\ -1 \end{pmatrix}, \ A_{(4)} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \ A_{(5)} = \begin{pmatrix} 5 \\ 2 \end{pmatrix}.$$

Ciò premesso, si introduce la seguente definizione:

Def: Siano $A \in M_{m,k}(\mathbb{K})$ e $B \in M_{k,n}(\mathbb{K})$ due matrici tali che il **numero di colonne di A coincida con il numero di righe di B**. Si definisce **prodotto righe per colonne** o semplicemente **prodotto** di A per B la matrice di tipo $m \times n$ il cui elemento di posto (i, j) è dato dal prodotto della riga i-ma di A per la colonna j-ma di B. In simboli:

$$A \cdot B := (A^{(i)} B_{(j)}).$$

Si noti che la riga $A^{(i)}$ e la colonna $B_{(j)}$ sono entrambe di lunghezza k. Molto spesso si scrive semplicemente AB per denotare il prodotto.

Es: Posto $A = \begin{pmatrix} 2 & 3 & -1 \\ 0 & 1 & 5 \end{pmatrix}$ e $B = \begin{pmatrix} 4 \\ -2 \\ 0 \end{pmatrix}$, risulta che AB è di tipo 2×1 e si calcola come segue:

$$AB = \begin{pmatrix} 2 \cdot 4 + 3 \cdot (-2) + (-1 \cdot 0) \\ 0 \cdot 4 + 1 \cdot (-2) + 5 \cdot 0 \end{pmatrix} = \begin{pmatrix} 2 \\ -2 \end{pmatrix}.$$

Es: Posto $A = \begin{pmatrix} 1 & 0 \\ 0 & 5 \\ -1 & 1 \end{pmatrix}$ e $B = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix}$, risulta che la matrice AB è ben definita ed è 3x3:

$$AB = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 5 \\ -1 & 0 & 2 \end{pmatrix}$$

Ad esempio, l'elemento di posto $(2, 3)$ si ottiene calcolando

$$A^{(2)} B_{(3)} = \begin{pmatrix} 0 & 5 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = 0 \cdot (-1) + 5 \cdot 1 = 5.$$

Nota: Osserviamo che, posto $A = (a_{is})$ e $B = (b_{sj})$ e $AB = (c_{ij})$, allora esplicitando la definizione, si ottiene che l'elemento generico c_{ij} della matrice prodotto AB è dato da

$$c_{ij} = \sum_{s=1}^{k} a_{is} b_{sj}.$$

Sussistono le seguenti proprietà di carattere generale:

1) Siano $A \in M_{m,k}(\mathbb{K})$, $B, C \in M_{k,n}(\mathbb{K})$. Allora
$$A(B + C) = AB + AC.$$

2) Siano $A, B \in M_{m,k}(\mathbb{K})$, $C \in M_{k,n}(\mathbb{K})$. Allora
$$(A + B)C = AC + BC.$$

3) Siano $A \in M_{m,k}(\mathbb{K}), B \in M_{k,n}(\mathbb{K})$ e $C \in M_{n,p}(\mathbb{K})$. Allora
$$A(BC) = (AB)C.$$

L'ANELLO DELLE MATRICI QUADRATE

Una matrice il cui numero di righe coincide con il numero di colonne si dice **quadrata**. In luogo di $M_{n,n}(\mathbb{K})$, si utilizzerà la notazione $M_n(\mathbb{K})$ per denotare l'insieme delle matrici di ordine n a coefficienti nel campo $\mathbb{K}$.

L'operazione di prodotto righe per colonne tra matrici quadrate dello stesso ordine produce matrici dello stesso tipo, ed è quindi un'operazione interna. Pertanto l'insieme $M_n(\mathbb{K})$ è munito di due operazioni

$$+ : M_n(\mathbb{K}) \times M_n(\mathbb{K}) \to M_n(\mathbb{K}),\ \cdot : M_n(\mathbb{K}) \times M_n(\mathbb{K}) \to M_n(\mathbb{K}).$$

Teorema: $(M_n(\mathbb{K}), +, \cdot)$ *è un anello.*

Sappiamo già che $(M_n(\mathbb{K}), +)$ è un gruppo abeliano e che, in base a quanto enunciato sopra, l'operazione di prodotto è associativa e valgono le proprietà distributive del prodotto rispetto alla somma.
Resta da chiarire che $(M_n(\mathbb{K}), \cdot)$ è un monoide, ovvero che esiste l'elemento neutro rispetto al prodotto: si tratta della **matrice identica** I_n; essa è la matrice i cui elementi sono tutti nulli, fatta eccezione per quelli "sulla diagonale" ovvero gli elementi con indice riga e colonna uguali. Tali elementi sono tutti uguali a 1 (l'unità del campo $\mathbb{K}$). Ad esempio:

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Più in generale

$$I_n := (\delta_{ij})$$

dove il simbolo (di Kronecker) δ_{ij} va interpretato come segue:

$$\delta_{ij} := \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Risulta quindi, per ogni $A \in M_n(\mathbb{K})$:

$$A \cdot I_n = A = I_n \cdot A.$$

Nota: L'anello delle matrici quadrate è (tranne casi particolarissimi) non commutativo: date due matrici quadrate dello stesso ordine, generalmente $AB \neq BA$.

Inoltre non si tratta di un corpo. Ad esempio, la matrice $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$ non è invertibile. Infatti, per ogni matrice $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ abbiamo

$$AB = \begin{pmatrix} a+c & b+d \\ -a-c & -b-d \end{pmatrix}$$

e tale matrice non può coincidere con $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, perchè altrimenti, confrontando i corrispondenti elementi, dovrebbe aversi:

$$a + c = 1,\ b + d = 0,\ -a - c = 0,\ -b - d = 1$$

da cui $1 = 0$.

Le matrici invertibili, ovvero gli elementi del gruppo $U(M_n(\mathbb{K}))$, si possono caratterizzare e studiare utilizzando importanti nozioni di algebra lineare (indipendenza lineare di vettori, rango, determinante) che non svilupperemo qui.

GRAFI

Def: Un **grafo (finito)** è una coppia (V, L) dove

- V è un insieme finito non vuoto;
- L è un insieme di sottoinsiemi di V di cardinalità 2.

  Gli elementi di V si chiamano **vertici**, mentre li elementi di L si chiamano **lati**.

Def: Due vertici v e w si dicono **adiacenti** se $\{v, w\}$ è un lato, cioè se $\{v, w\} \in L$. Se $l = \{v, w\}$ è un lato, i vertici (necessariamente distinti) si dicono gli **estremi** del lato stesso.
Infine, si dice che un vertice v è adiacente ad un lato se $v \in l$, cioè se è uno dei suoi estremi.

N.B: Due vertici adiacenti sono necessariamente diversi.

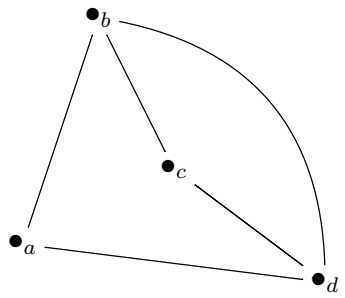
Oss: Una definizione equivalente di grafo è la segunte: un grafo può pensarsi come una coppia (V, R), dove $R \subset V \times V$ è una relazione *simmetrica* sull'insieme V, e tale che per ogni $v \in V$ $v \not R v$.

Un grafo $G = (V, L)$ si può rappresentare nel piano mediante un **diagramma** in cui i vertici sono punti e due vertici a e b sono collegati da un **segmento** o un **arco di curva** se e solo se $\{a, b\}$ sono adiacenti.
Tale rappresentazione grafica non è univoca, e non va confusa con il grafo in sè.

Esempio: Il grafo $G = (V, L)$ dato da

$$(V = \{a, b, c, d\}, L = \{\{a, b\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}$$

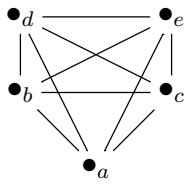
si può rappresentare come segue:



Def: Un grafo è **completo** se due qualunque suoi vertici distinti sono adiacenti.
In altri termini, L coincide con l'insieme di *tutti* i sottoinsiemi di V di cardinalità 2.
Ciò accade se e solo se $|L| = \binom{n}{2}$, dove $n = |V|$ è il numero di vertici del grafo.

Un grafo completo con n lati è di solito denotato con K_n.

Ad esempio, una possibile rappresentazione grafica di K_5 è:



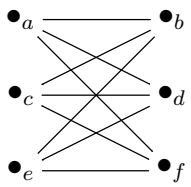
Es: Un grafo $G = (V, L)$ si dice **bipartito** se l'insieme dei vertici ammette una partizione $\{V_1, V_2\}$ con due blocchi, di modo che:

$$V = V_1 \cup V_2, \quad V_1 \cap V_2 = \emptyset$$

e per ogni lato $l = \{v, w\}$ si ha sempre che $v \in V_1, w \in V_2$ oppure $v \in V_2, w \in V_1$, cioè se i suoi estremi non stanno nello stesso blocco.

Se i lati sono tutti i possibili insiemi $\{v_1, v_2\}$ con $v_1 \in V_1$ e $v_2 \in V_2$ si parla di **grafo bipartito completo**.
In tal caso, se $|V_1| = m$ e $|V_2| = n$, un tale grafo è spesso denotato con il simbolo $K_{m,n}$.

Ecco una rappresentazione grafica di $K_{3,3}$:



In questo esempio $V_1 = \{a, c, e\}$, mentre $V_2 = \{b, d, f\}$.

GRADO DI UN VERTICE

Def: Sia $G = (V, L)$ un grafo. Si chiama **grado** o **valenza** di un vertice $v \in V$ il numero lati ad esso adiacenti. Esso si denota con $d(v)$.
Si osservi che $d(v)$ coincide anche col numero dei vertici adiacenti a v.

Def: Un vertice di grado 0 si dice **isolato** (da esso non parte e non arriva alcun lato).
Def: Se $d(v)$ è pari (risp. dispari), il vertice v si dice **pari** (risp. **dispari**).

Se G è un grafo con n vertici $v_1, \ldots, v_n$, la n-pla di interi $(d(v_1), \ldots, d(v_n))$ si chiama **sequenza grafica** di G.

Teoerema (Lemma delle strette di mano): *Per ogni grafo vale la formula*

$$|L| = \frac{1}{2} \sum_{v \in V} d(v).$$

Corollario: *Ogni grafo ha un numero pari di vertici dispari.*

Dimostrazione del Lemma delle strette di mano:

- Siano $v_1, \ldots, v_n$ i vertici. Sia L_i l'insieme dei lati incidenti il vertice v_i. Dunque, per definizione $d(v_i) = |L_i|$.
- Consideriamo la sequenza di insiemi $L_1 \ldots, L_n$, che complessivamente contengono tutti i lati, ovvero $L =_1 \cup \cdots L_n$.
- Ogni lato $l = \{v_i, v_j\}$ compare esattamente **due** volte negli insiemi della sequenza, precisamente una volta come elemento di L_i e l'altra come elemento di L_j. Quindi:
- $\sum_{v \in V} d(v) = d(v_1) + \cdots + d(v_n) = |L_1| + \cdots + |L_n| = 2|L|$.

Teorema: *In ogni grafo vi sono sempre due vertici che hanno lo stesso grado.*

Infatti, posto ancora $n = |V|$, se così non fosse, avremmo $d(v) \neq d(w)$ per ogni coppia di vertici $v \neq w$. Dunque la funzione

$$d : V \to \{0, \ldots, n-1\}$$

che associa ad ogni vertice il proprio grado sarebbe ingettiva. Poichè gli insiemi V e $\{0, \ldots, n-1\}$ hanno lo stesso numero di elementi, la funzione in questione sarebbe per forza bigettiva. In particolare (stante la surgettività) dovrebbero esistere due vertici v e w tali che

$$d(v) = 0, \quad d(w) = n - 1.$$

Dunque, v sarebbe isolato, mentre w sarebbe adiacente a tutti gli altri vertici; in particolare, w dovrebbe essere adiacente a v e questo è impossibile. Siamo pervenuti a una contraddizione.

CAMMINI E CIRCUITI

Sia $G = (V, L)$ un grafo.

Def: Un **cammino** in G è ogni sequenza di vertici

$$v_o, v_1, \ldots, v_k, \qquad k \geq 0$$

denotata spesso anche senza virgole:

$$v_o v_1 \cdots v_k$$

tale che:

1) due vertici **consecutivi** v_i e v_{i+1} sono sempre **adiacenti**;

2) i lati $\{v_i, v_{i+1}\}$ sono **tutti diversi** tra loro al variare di $i = 0, \ldots, k-1$.

Ci si esprime dicendo che il cammino **va da** v_o **a** v_k (o che **parte** dal vertice v_o e **termina** al vertice v_k).

Attenzione: non tutti i vertici sono per forza coinvolti in un cammino, e un vertice può comparire più volte nella sequenza.

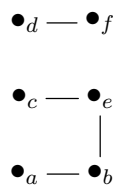
Def: Dato un cammino $v_o \ldots v_k$, ogni lato $\{v_i, v_{i+1}\}$ si dice **lato del cammino** (o lato appartenente ad esso). Il numero k è per definizione la **lunghezza** del cammino stesso.

Nota: Se $k = 0$, il cammino consiste di un solo vertice v_o e nessun lato. Questo tipo di cammino si chiama **cammino nullo** (da v_o a v_o).

Def: Un cammino si dice **circuito** o **ciclo** se il vertice iniziale e finale coincidono, cioè se $v_o = v_k$.

Def: Un grafo **connesso** è un grafo in cui per ogni coppia di vertici esiste almeno un cammino dal primo a secondo. Se ciò non è vero, si parla invece di grafo **sconnesso**.

Il seguente grafo è sconnesso:



CIRCUITI E CAMMINI EULERIANI

Def: Un cammino (in particolare circuito) si dice **Euleriano** se **tutti i lati** del grafo vi appartengono.

Percorrendo un cammino Euleriano, si passa da ogni lato una ed una sola volta.

Oss: Se un grafo non contiene vertici isolati ed ammette un circuito Euleriano, allora è connesso.
Se infatti $\mathcal{C} = v_o \cdots v_k$ è un tale circuito, ogni vertice $v \in V$, non essendo isolato, è adiacente a qualche lato l; ma tale lato appartiene al circuito. Quindi v è uno dei v_i. Da ciascun vertice quindi si può costruire un cammino che raggiunge ogni altro vertice, percorrendo i lati di $\mathcal{C}$.

Studieremo quindi il problema dell'esistenza di circuiti Euleriani nell'ambito della classe dei grafi connessi. Il seguente risultato è stato il punto di partenza della teoria dei grafi.

Teorema (di Eulero): *Sia G un grafo connesso. Allora G ammette un circuito Euleriano se o solo se tutti i suoi vertici hanno grado pari.*

Dimostrazione della condizione necessaria per l'esistenza di un circuito euleriano:

Sia $\mathcal{C} = v_0 \cdots v_k$ un circuito Euleriano nel grafo connesso G. Calcoliamo il grado di ciascun vertice v.

- Come si è già visto, poichè il grafo è connesso, nessun vertice è isolato, e quindi v è uno dei v_i.
- Se v è un vertice diverso da v_o e I è l'insieme degli indici $i > 0$ per cui $v = v_i$, allora tutti e soli i lati adiacenti ad esso sono

  $$\{v_{i-1}, v_i\}, \qquad \{v_i, v_{i+1}\} \tag{$*$}$$

  al variare di i in I.

  Quindi $d(v) = 2\,|I|$ che è un numero pari.
- Se $v = v_0$ e I è l'insieme degli indici i, $0 < i < k$, per cui $v = v_i$, allora tutti e soli i lati adiacenti ad esso sono gli stessi (*) di cui sopra (se I non è vuoto) ed i due lati iniziale e finale:

  $$\{v_o, v_1\},\ \{v_{k-1}, v_o\}.$$

  Quindi $d(v_0) = 2\,|I| + 2$.

L'ALGORITMO DI HIERHOLZER

Esibiamo un algoritmo che permette di costruire circuiti Euleriani che partono da un fissato vertice v, nelle ipotesi del Teorema di Eulero, ovvero che G sia connesso e che tutti i suoi vertici siano pari.

Conviene fissare un po' di terminologia.

- Se $\mathcal{C}$ è un ciclo di un grafo $G = (V, L)$, denotiamo con
$$G - \mathcal{C}$$
il grafo avente gli stessi vertici di G, che si ottiene da esso eliminando tutti i lati appartenenti al circuito.

- Se $\mathcal{C} = v_0 \dots v_{k-1} v_0$ è un circuito, $w = v_j$ è uno dei vertici del circuito, e $\mathcal{D} = w w_1 \dots w_{s-1} w$ è un altro circuito che parte da e ritorna a w, il circuito seguente:
$$v_0 \cdots v_{j-1} w w_1 \cdots w_{s-1} w v_{j+1} \cdots v_0$$
si dice ottenuto da $\mathcal{C}$ *inserendo* $\mathcal{D}$ *a partire da* w.

Ciò premesso, l'algoritmo è il seguente:

START: Scegliere un vertice v e scegliere un ciclo $\mathcal{C}$ che parte da e arriva a v.

1) Se $\mathcal{C}$ contiene tutti i lati del grafo, è un circuito euleriano: STOP.

Altrimenti eseguire 2) e 3) seguenti:

2) Scegliere un vertice w di $\mathcal{C}$ non isolato in $G - \mathcal{C}$, e scegliere un ciclo $\mathcal{D}$ in $G - \mathcal{C}$ da w a w.

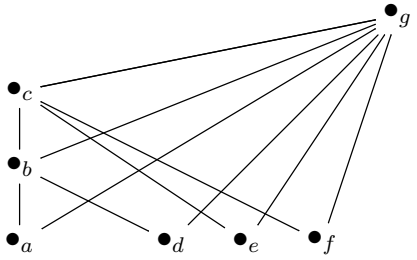
3) Inserire $\mathcal{D}$ in $\mathcal{C}$ a partire da w, formando un nuovo ciclo da v a v più lungo. Aggiornare $\mathcal{C}$ sostituendolo con tale ciclo e tornare al punto 1).

Notiamo che, ad ogni passo, il circuito iniziale $\mathcal{C}$ viene allungato inserendo nuovi lati non appartenenti ad esso; pertanto, essendo i lati del grafo in numero finito, dopo un numero finito di passi, esso "diventa" necessariamente un circuito Euleriano.

Nota: Non entreremo nei dettagli, ma facciamo notare che le ipotesi che sia G connesso e che tutti i vertici siano pari, servono a garantire che l'algoritmo non si arresti mai, in quanto tali ipotesi permettono di provare quanto segue:

a) In un grafo con vertici tutti pari, per ogni vertice non isolato c'è sempre almeno un ciclo che parte da esso.
b) Dopo aver eliminato i lati di $\mathcal{C}$, può succedere che $G - \mathcal{C}$ sia sconnesso, ma non tutti i vertici di $\mathcal{C}$ restano isolati in $G - \mathcal{C}$; inoltre tutti i vertici di $G - \mathcal{C}$ sono di grado pari. Per a), ciò permette di ripartire costruendo il nuovo ciclo $\mathcal{D}$ che serve ad allungare $\mathcal{C}$ "pescando" nuovi lati in $G - \mathcal{C}$.

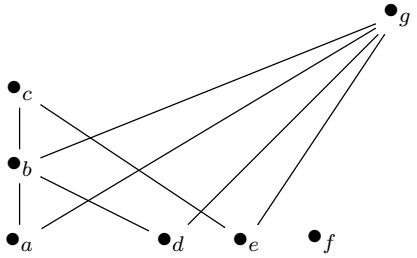
Esempio: Il grafo connesso seguente



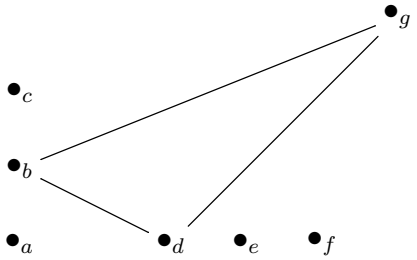
ammette cicli euleriani perchè

$$d(g) = 6,\ d(c) = d(b) = 4,\ d(a) = d(d) = d(e) = d(f) = 2.$$

Per determinarne uno, partiamo da g e scegliamo il circuito $gfcg$; eliminando i tre lati di tale circuito si ottiene il grafo:



Qui f è isolato; possiamo ripartire da c o ancora da g. Scegliendo g, consideriamo il ciclo $gecbag$. Eliminando i lati resta il grafo:



Prima di procedere aggiorniamo il ciclo iniziale inserendovi il secondo:

$$gfcg \longrightarrow gecbagfcg.$$

Possiamo ripartire da g o b (non da d, perchè non fa parte del ciclo ottenuto sin qui). Scegliamo b, e il ciclo $bdgb$; inserendolo nel precedente al posto di b otteniamo infine il ciclo Euleriano:

$$gecbdgbagfcg.$$

Naturalmente, si possono fare ad ogni passo scelte diverse, che portano a circuiti euleriani differenti (provare!).

CRITERIO DI ESISTENZA DI CAMMINI EULERIANI

Il teorema di Eulero fornisce come conseguenza anche il seguente criterio:

Corollario: *Sia G un grafo connesso. Allora G ammette cammini Euleriani se e solo se tutti i vertici sono pari, oppure i vertici dispari sono esattamente due.*

Ci limitiamo a osservare che, se G ha esattamente due vertici dispari v_1 e v_2, si può applicare il Teorema di Eulero al grafo G' che si ottiene aggiungendo un nuovo vertice z e i lati seguenti:

$$l_1 := \{z, v_1\},\ l_2 := \{z, v_2\}.$$

In tale grafo z ha grado 2, il grado di v_1 e v_2 è incrementato di 1, e resta inalterato il grado di tutti gli altri vertici. Quindi tutti i vertici di G' sono pari. Allora in G' esiste un circuito euleriano, in particolare esiste un tale circuito $\mathcal{C}'$ che parte da e ritorna a z. Poichè l_1 e l_2 sono gli unici lati di G' adiacenti a z, il primo lato di $\mathcal{C}'$ è necessariamente l_1, mentre l'ultimo dev'essere l_2; dunque esso è della forma:

$$zv_1 \cdots v_2 z.$$

Eliminando z dalla sequenza, resta un cammino $\mathcal{C} = v_1 \cdots v_2$ in G da v_1 a v_2 che è ovviamente Euleriano in G.

ALBERI

Def: Si chiama **albero** ogni grafo connesso privo di circuiti.

Gli alberi si possono caratterizzare in vari modi. La prima caratterizzazione che esimiamo riguarda i cammini:

Teorema: *Un grafo G è un albero se e solo se per ogni coppia di vertici v, w esiste uno ed un solo cammino da v a w.*

Dimostrazione: Osserviamo preliminarmente che, se v e w sono due vertici, ed è dato un cammino

$$v_0 \cdots v_k$$

da v a w, allora esso si può percorre a ritroso per ottenere un cammino da w a v; in termini più precisi, anche la sequenza:

$$v_k \cdots v_0$$

è un cammino, che va da w a v.

Supponiamo che G sia un albero e ammettiamo che esistano due diversi cammini $\mathcal{C}_1$ e $\mathcal{C}_2$ da v a a w; se tutti i lati di $\mathcal{C}_1$ sono diversi da quelli di $\mathcal{C}_2$, percorrendo prima $\mathcal{C}_1$ e poi il cammino $\mathcal{C}_2$ a ritroso si ottiene un circuito che parte da v e vi ritorna, contro l'ipotesi che il grafo sia un albero. Se qualche lato di $\mathcal{C}_2$ è anche lato di $\mathcal{C}_1$, si può ottenere ancora un circuito, percorrendo i lati di $\mathcal{C}_1$ fino al primo di questi lati in comune per poi continuare sempre su $\mathcal{C}_2$ a ritroso. In ogni caso si perviene ad una contraddizione.

Viceversa, supponiamo che dati due vertici vi sia un unico cammino dal primo al secondo. Allora non esistono circuiti, perchè dato un circuito

$$v_0\, v_1 \cdots v_{k-1} v_0,$$

esistono due cammini diversi da v_0 a v_1, che sono

$$v_0 v_1 \quad \text{e} \quad v_0 v_{k-1} \cdots v_1.$$

ALBERI E SEQUENZE GRAFICHE

Un'altra utile caratterizzazione degli alberi coinvolge il numero dei lati:

Teorema: *Sia $G = (V, L)$ un grafo connesso con n vertici. Allora G è un albero se e solo se*

$$|L| = n - 1.$$

Consegue, per il Lemma delle strette di mano, che per ogni albero con n vertici vale la relazione:

$$\sum_{v \in V} d(v) = 2(n-1).$$

Tale relazione permette in realtà di costruire alberi prescrivendo i gradi dei vertici; infatti si può provare quanto segue:

Teorema: *Sia assegnata una n-pla di interi strettamente positivi:*

$$(d_1, \ldots, d_n),\ d_1 \geq d_2 \cdots \geq d_n.$$

Allora esiste un albero con n vertici la cui sequenza grafica è $(d_1, \ldots, d_n)$ se e solo se

$$\sum_{i=1}^{n} d_i = 2(n-1).$$

Esempio: Esistono alberi con 10 vertici la cui sequenza grafica è

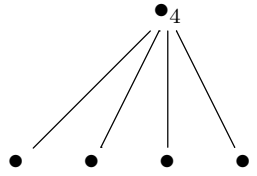
$$(4, 3, 3, 2, 1, 1, 1, 1, 1, 1).$$

Infatti:

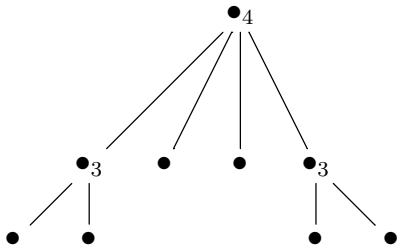
$$4 + 3 + 3 + 2 + 1 + 1 + 1 + 1 + 1 + 1 = 18 = 2(10 - 1).$$

Per ottenere un tale albero, si può procedere ad esempio partendo da un vertice di grado massimo, e introdurre nuovi vertici "figli" di questo, ad esso collegati, e poi procedere allo stesso modo con gli altri vertici di grado inferiore.
Contrassegnando i vertici con i gradi, abbiamo:

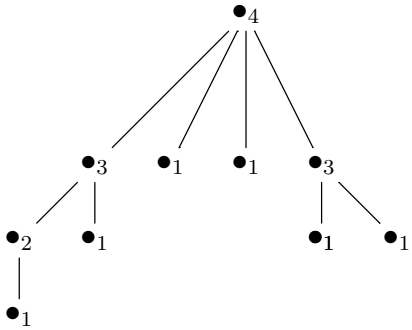
PRIMO STEP:



SECONDO STEP



TERZO STEP



ALGORITMO DI HAKIMI-HAVEL

Ci poniamo ora il problema più generale di costruire grafi (di qualsiasi natura, non necessariamente alberi o grafi connessi) di assegnata sequenza grafica.
Osserviamo che, se occorre, la sequenza grafica $(d(v_1), \ldots, d(v_n))$ di un grafo con n vertici, si può sempre supporre ordinata in modo decrescente, ovvero in modo che:

$$d(v_1) \geq d(v_2) \geq \cdots \geq d(v_n),$$

a meno di permutare i nomi dei vertici. Inoltre, detto s il grado maggiore, tale sequenza è sempre del tipo

$$(s, t_1, \ldots, t_s, d_1, \ldots, d_k)$$

con

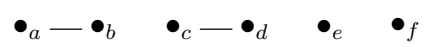
$$s \geq t_1 \geq \cdots \geq t_s \geq d_1 \geq \cdots \geq d_k \geq 0.$$

Ciò perchè, considerato un vertice di grado s, esso deve essere adiacente a s vertici diversi da esso; pertanto la sequenza deve contenere, oltre s, almeno altri s numeri.

Assegnata ora una sequenza di numeri naturali di questo tipo, diremo che essa è *grafica* se esiste un grafo la cui sequenza grafica coincide con essa. Ad esempio, la sequenza

$$(1, 1, 1, 1, 0, 0)$$

è grafica: un grafo che la realizza è



La sequenza

$$(4, 2, 1, 3)$$

sicuramente non è grafica perchè non rispetta il criterio di cui sopra (dopo il primo 4 vi sono solo tre numeri). Anche

$$(4, 3, 2, 1)$$

non lo è, perchè tutti i numeri sono diversi, mentre sappiamo che in ogni grafo vi sono almeno due vertici aventi lo stesso grado. Similmente $(5, 4, 3, 2, 2)$ non è grafica perchè compare un solo numero dispari (i numeri dispari devono essere in numero pari). La sequenza:

$$(3, 1, 0, 0, 0)$$

non è grafica, perchè in un grafo un vertice di grado 3 dev'essere adiacente a tre vertici, tutti necessariamente di grado almeno 1. Ogni sequenza

$$(0, 0, \ldots, 0)$$

è grafica, perchè è realizzata da un grafo con vertici tutti isolati (e nessun lato).

Il risultato seguente dà un criterio utile per stabilire se una data sequenza è grafica, riconducendo la questione al caso di una sequenza di lunghezza inferiore:

Teorema: *Una sequenza di numeri naturali*

$$(s, t_1, \ldots, t_s, d_1 \ldots, d_k)$$

con

$$s \geq t_1 \geq \cdots \geq t_s \geq d_1 \geq \cdots \geq d_k \geq 0$$

è grafica se e solo se lo è la sequenza

$$(t_1 - 1, \ldots, t_s - 1, d_1 \ldots, d_k).$$

Applicando più volte questo risultato, si può decidere facilmente in un numero finito di passi se una data sequenza è grafica o no: ad ogni passo si elimina il primo numero s e si sottrae 1 agli s numeri successivi. Se si perviene a una sequenza del tipo $(0, 0 \ldots, 0)$ la risposta è affermativa, mentre se si perviene a una sequenza con almeno un -1, la risposta è negativa. Chiaramente, in molte situazioni si può terminare anche prima, se si perviene a un certo step ad una sequenza che è manifestamente grafica oppure non grafica.

Attenzione: Il criterio enunciato nel Teorema di Hakimi-Havel è applicabile solo a sequenze di numeri in ordine **descrescente**; quindi ad ogni passo occorre riordinare la sequenza. Alternativamente, si può decidere di ordinare mentalmente i numeri, contrassegnare il numero più alto s e sottolineare altri s numeri più grandi di tutti gli altri, prima di procedere a eliminare s e sottrarre 1 ai numeri sottolineati.

Esempio: Vediamo se la sequenza $(7, 6, 6, 6, 4, 3, 3, 3, 3)$ è grafica:

$$\begin{array}{ccccccccc}
\textcircled{7} & \underline{6} & \underline{6} & \underline{6} & \underline{4} & \underline{3} & \underline{3} & \underline{3} & 3 \\
 & \textcircled{5} & \underline{5} & \underline{5} & \underline{3} & \underline{2} & 2 & 2 & \underline{3} \\
 & & \textcircled{4} & \underline{4} & \underline{2} & 1 & \underline{2} & \underline{2} & 2 \\
 & & & \textcircled{3} & 1 & 1 & \underline{1} & \underline{1} & \underline{2} \\
 & & & & \textcircled{1} & \underline{1} & 0 & 0 & 1 \\
 & & & & & 0 & 0 & 0 & 1
\end{array}$$

Poichè $(0, 0, 0, 1)$ è manifestamente non grafica, possiamo concludere che anche $(7, 6, 6, 6, 4, 3, 3, 3, 3)$ non lo è. Si osservi che se procedessimo con un ulteriore passo, avremmo

$$\begin{array}{cccc}
\underline{0} & 0 & 0 & \textcircled{1} \\
-1 & 0 & 0 &
\end{array}$$

pervenendo alla sequenza inammissibile $(-1, 0, 0)$.

Esempio: Consideriamo la sequenza $(5, 4, 2, 2, 1, 1, 1, 1, 1)$. Eseguendo l'algoritmo abbiamo:

$$\begin{array}{ccccccccc} \textcircled{5} & \underline{4} & \underline{2} & \underline{2} & \underline{1} & \underline{1} & 1 & 1 & 1 \\ & \textcircled{3} & \underline{1} & \underline{1} & 0 & 0 & \underline{1} & 1 & 1 \\ & & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}$$

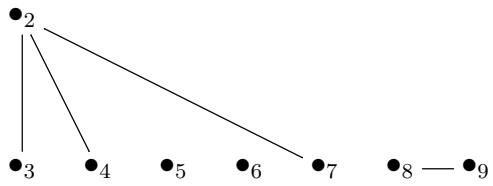
Chiramente $(0, 0, 0, 0, 0, 1, 1)$ è grafica, per cui tale è la sequenza considerata.

Il procedimento esposto può anche essere utilizzato per costruire effettivamente un grafo di assegnata sequenza grafica. Si osservi infatti che la dimostrazione della condizione sufficiente enunciata nel Teorema di Hakimi-Havel è la seguente: se la sequenza $(t_1 - 1, \ldots, t_s - 1, d_1, \ldots, d_k)$ è grafica, e G' è un grafo che la realizza, un grafo G che realizza la sequenza $(s, t_1, \ldots, t_s, d_1 \ldots, d_k)$ si può costruire semplicemente aggiungendo un nuovo vertice z e aggiungendo gli s lati $\{z, v_i\}$ dove i v_i sono i vertici di grado $t_1 - 1, \ldots, t_s - 1$ di G (lasciando tutto il resto invariato).

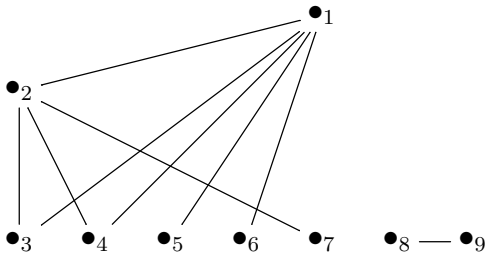
Seguendo questo schema, possiamo ricostruire il grafo come segue. I vertici saranno denotati con i numeri $1, \ldots, n$, dove n è la lunghezza delle sequenza data. Dopo aver eseguito l'algoritmo, si costruisce il grafo partendo dall'ultima sequenza grafica in basso, risalendo di una riga alla volta; per ogni riga, si aggiunge un vertice il cui numero è dato dalla colonna occupata dal numero cerchiato, che viene collegato con un lato con i vertici il cui numero è dato dalle colonne occupate dai numeri sottolineati sulla stessa riga.

Nel caso della seguenza esaminata sopra, il grafo si ottiene con i seguenti passi:
PRIMO STEP (ultima riga)

SECONDO STEP (seconda riga; vertice da aggiungere: 2; nuove connessioni con i vertici 3,4,7)



TERZO STEP (prima riga; vertice da aggiungere: 1; nuove connessioni con i vertici da 2 a 6)



ISOMORFISMI TRA GRAFI

Analogamente al caso delle strutture algebriche, anche i grafi possono presentarsi sotto forme diverse, ma equivalenti:

Def: Due grafi $G_1 = (V_1, L_1)$ e $G_2 = (V_2, L_2)$ si dicono **isomorfi** se esiste una bigezione tra gli insiemi dei vertici:

$$f : V_1 \to V_2$$

tale che, per ogni v, w vertici di G_1 si abbia:

$$v \text{ e } w \text{ sono adiacenti } \iff, \ f(v) \text{ e } f(w) \text{ sono adiacenti.}$$

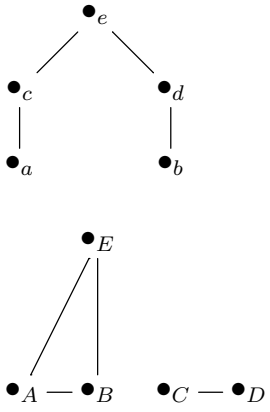
Ogni bigezione $f : V_1 \to V_2$ con questa proprietà prende il nome di **isomorfismo** tra i due grafi.

Nota importante: ogni isomorfismo *conserva i gradi dei vertici*, cioè per ogni vertice di v di G_1 si ha:

$$d(v) = d(f(v)).$$

Quindi: *condizione necessaria affinchè due grafi siano isomorfi è che abbiano la stessa sequenza grafica.*

Occorre notare che tale condizione non è sufficiente. Pertanto essa può essere utilizzata per escludere che due grafi siano isomorfi, se si verifica che le due sequenze non coincidono. Ma se coindono, occorre più lavoro, basato su altre considerazioni, per stabilire se i due grafi sono o non sono isomorfi. Ad esempio, i grafi seguenti con vertici $\{a, b, c, d, e\}$ e $\{A, B, C, D, E\}$, hanno la stessa sequenza grafica $(2, 2, 2, 1, 1)$:



ma non sono certamente isomorfi, perchè il primo è connesso (è un albero), mentre il secondo è sconnesso.

ANCORA SULLA CARATTERIZZAZIONE DEGLI ALBERI

Ai fini di acquisire meglio le nozioni basilari sui grafi, presentiamo una dimostrazione del criterio enunciato in precedenza per stabilire se un grafo *connesso* $G = (V, L)$ con n vertici è un albero:

$$G \text{ è un albero se e solo se ha } n-1 \text{ lati.}$$

Cominciamo a provare la condizione necessaria: ogni albero ha $n-1$ lati.
Ragioniamo per induzione sul numero n dei vertici.

• Passo base $n = 1$: in tal caso il grafo, costituito da un unico vertice isolato, ha 0 lati, per cui la tesi è vera.

• Passo induttivo: sia $n > 1$ e supponiamo che ogni albero con n vertici abbia $n-1$ lati; vogliamo provare che ogni albero con $n+1$ vertici ha n lati. Sia G un tale albero. Poichè i vertici sono in numero finito, tutti i possibili cammini sono in numero finito; le loro lunghezze costituiscono quindi un insieme finito di numeri naturali; pertanto esiste il massimo k di tali numeri. Chiaramente $k \geq 1$. Fissiamo allora un cammino $\mathcal{C}$ di lunghezza massima

$$v_0 v_1 \cdots v_k.$$

Concentriamoci sul vertice iniziale di tale cammino: affermiamo che necessariamente

$$d(v_0) = 1.$$

Infatti per prima cosa, v_0 non può ripetersi nel cammino, cioè $v_i \neq v_0$ per $0 < i \leq k$, perchè altimenti avremmo un circuito $v_0 \cdots v_i = v_0$, la cui presenza nel nostro albero è vietata per definizione.
Se fosse $d(v_0) > 1$, vi sarebbe un lato $\{v_0, w\}$ diverso da $\{v_0, v_1\}$ incidente v_0; siccome v_0 non si ripete in $\mathcal{C}$, tale lato non può essere nessuno dei lati di $\mathcal{C}$. Allora avremmo anche il cammino

$$w v_0 v_1 \cdots v_k$$

di lunghezza $k+1$, il che è una contraddizione.
Consideriamo ora il grafo $G' = (V - \{v_0\}, L - \{\{v_0, v_1\}\})$ ottenuto da G rimuovendo v_0 e il primo lato $\{v_0, v_1\}$ di $\mathcal{C}$. Esso è connesso. Infatti, consideriamo due vertici v e w di G', quindi entrambi diversi da v_0. Siccome G è connesso, esiste un cammino in G dal primo al secondo:

$$v u_1 \cdots u_{s-1} w.$$

Ora, nessuno dei vertici in questione può coincidere con v_0, perchè, ogni vertice u_i di tale cammino, diverso da v e w è incidente almeno due lati ($\{u_{i-1}, u_i\}$ e $\{u_i, u_{i+1}\}$), mentre $d(v_0) = 1$. Pertanto in tale cammino non è utilizzato neanche il lato $\{v_0, v_1\}$ e quindi esso è di fatto un cammino da v a w nel grafo G'.
Notiamo infine che G' non può contenere circuiti, perchè sarebbero anche circuiti di G: quindi è anch'esso un albero, con n vertici. Per l'ipotesi induttiva G' ha $n-1$ lati e quindi G ha $n-1+1 = n$ lati.

ALBERI DI SOSTEGNO

Prima di provare l'altra implicazione del criterio di caratterizzazione degli alberi, introuciamo un paio di concetti utili.

Def: Si chiama **sottografo** di un grafo $G = (V, L)$ ogni grafo $G' = (V', L')$ tale che:

$$V' \subset V, \quad L' \subset L,$$

cioè tutti i vertici di G' sono anche vertici di G e tutti i lati di G' sono anche lati di G.

Def: Si chiama **albero di sostegno** o **albero di supporto** di un grafo $G = (V, L)$ un suo sottografo $T = (V, L')$ che è un albero, e i cui vertici sono **tutti** i vertici di G.

Un albero di sostegno è quindi un albero ottenuto eliminando opportuni lati del grafo, ma conservandone tutti i vertici, in modo da eliminare tutti i circuiti.
Tale nozione è importante ad esempio nel caso di reti di telecomunicazione, laddove i circuiti corrispondono a collegamenti ridondanti, che è vantaggioso eliminare.

Proposizione: *Ogni grafo connesso ha almeno un albero di sostegno.*

L'osservazione chiave per giustificare ciò è la seguente:

Fatto: *cancellando un lato appartenente ad un circuito di un grafo connesso, si ottiene sempre un grafo connesso.*

Poichè togliere un tale lato da un circuito non sconnette mai il grafo, per individuarne un albero di sostegno basta iterare più volte tale operazione, un circuito alla volta (il circuito viene "spezzato"). Siccome i circuiti sono in numero finito, dopo un numero finito di passi si ottiene un sottografo connesso e senza circuiti, che è un albero di sostegno.

L'affermazione di cui sopra si giustifica facilmente: detto $\mathcal{C}$ un circuito

$$\mathcal{C} = v_0 v_1 \cdots v_{k-1} v_0$$

qualsiasi, e considerato un suo lato $l = \{v_i, v_{i+1}\}$, consideriamo due vertici u e w nel sottografo $G' = (V, L - \{l\})$. Vogliamo provare che esiste un cammino in G' dal primo al secondo.
Usando la connessione di G, abbiamo un cammino $\mathcal{D}$ in G da u a w. Se tale cammino non utilizza il lato l, allora esso è anche un cammino in G' e l'obiettivo è raggiunto; altrimenti possiamo sostituire l con il cammino

$$v_{i+1} \cdots v_{k-1} v_0 v_1 \cdots v_i,$$

percorso a ritroso da v_i a v_{i+1} lungo il circuito $\mathcal{C}$.

Come applicazione del concetto di albero si sostegno, torniamo alla caratterizzazione degli alberi, e proviamo la condizione sufficiente:

Ogni grafo connesso con n vertici e $n-1$ lati è un albero.

Infatti, fissiamo un grafo connesso $G = (V, L)$ con n vertici e $n-1$ lati e consideriamo un suo albero di sostegno $T = (V, L')$. Tale albero ha ancora n vertici, per cui sappiamo che deve avere $n-1$ lati; dunque

$$|L'| = n - 1 = |L|$$

e siccome L' è sottoinsieme di L, di fatto

$$L' = L,$$

ovvero G coincide con il suo albero di sostegno e quindi è esso stesso un albero.

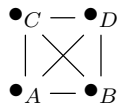
GRAFI PLANARI

Come si è detto, la nozione di grafo è di natura puramente astratta: si tratta di relazioni tra oggetti, che hanno significato a prescindere dalla loro rappresentazione grafica.
D'altra parte, nel contesto applicativo, può essere importante lavorare con grafi il cui disegno nel piano soddisfa determinati requisiti (si pensi ad esempio al design di circuiti elettrici). Da questo punto di vista, la più importante classe di grafi di interesse è data dai grafi planari, definiti come segue:

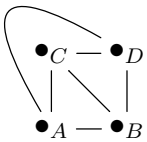
Def: Un grafo G si dice **planare** se può essere disegnato nel piano, in modo che gli archi di curva che rappresentano i lati non abbiano punti di intersezione, fatta eccezione al più per i punti che rappresentano i vertici.

Bisogna porre l'attenzione sul fatto che la definizione coinvolge tutte le possibili rappresentazioni grafiche dell'oggetto in questione, richiedendo che almeno in una di esse si risolva il problema degli incroci tra i lati. Pertanto è una condizione difficile da verificare "a occhio" se il grafo è piuttosto "intricato".

Esempio: Il grafo completo con quattro vertici,
$K_4 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\}\})$:



è planare, nonostante questa rappresentazione grafica non lo evidenzi (i lati $\{A, D\}$ e $\{B, C\}$ si intersecano in un punto che non è un vertice); la planarità diventa manifesta se disegniamo il grafo così:



Segnaliamo il seguente risultato utile che fornisce una condizione necessaria per la planarità:
Teorema: *Se un grafo $G = (V, L)$ con almeno 3 vertici è planare, allora deve aversi:*

$$|L| \leq 3|V| - 6.$$

Ad esempio, il grafo completo K_5 non soddisfa questa condizione, avendosi $|L| = (5 \cdot 4)/2 = 10$ e $3|V| - 6 = 9$. Pertanto K_5 non è planare. Attenzione: la disuguaglianza considerata nell'enunciato non è condizione sufficiente per la planarità.

IL TEOREMA DI KURATOWSKI

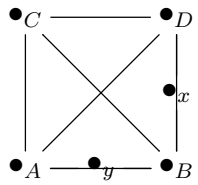
Def: Dato un grafo $G = (V, L)$, si fissi un suo lato $l = \{v, w\}$. L'operazione di **aggiungere un vertice** x **sul lato** l consiste nel costruire un nuovo grafo

$$G' = (V \cup \{x\}, L'),$$

dove $x \notin V$ e L' è costituito dai lati di G, eccetto l che viene sostituito con due nuovi lati $\{v, x\}$ e $\{x, w\}$.

Ogni grafo che si ottiene a partire da un grafo assegnato G ripetendo un numero finito di volte tale operazione di aggiunta di vertici si chiama **espansione** oppure **suddivisione del grafo** G.

Ad esempio, un'espansione di K_4 è



Si osservi che, nel passare da un grafo ad una sua espansione, i gradi dei vertici del grafo originale non vengono alterati. I vertici aggiunti sui lati hanno grado 2.

Con questa terminologia, sussiste il seguente risultato notevole:

Teorema (di Kuratowski): *Un grafo è planare se e solo se non contiene sottografi isomorfi a* K_5*, a* $K_{3,3}$ *o loro espansioni.*

Oss: Si noti che condizione necessaria affinchè un grafo contenga un sottografo isomorfo a K_5 (o una sua espansione) è che ammetta almeno 5 vertici di grado almeno 4, mutuamente adiacenti. Similmente, se un grafo contiene $K_{3,3}$ (o espansione di esso), allora deve contenere almeno 6 vertici di grado almeno 3. Ad esempio, in base al teorema, possiamo affermare che un grafo con sequenza grafica $(4, 4, 4, 4, 2, 2)$ è planare.

CARATTERIZZAZIONE DEI GRAFI BIPARTITI

Il concetto di circuito è utile anche per caratterizzare i grafi bipartiti. Si ha infatti:

Teorema: *Un grafo è bipartito se e solo se non contiene cicli di lunghezza dispari.*

Corollario: *Ogni albero è un grafo bipartito.*

Osservazione: Stabilire se è un grafo è bipartito equivale a stabilire se i suoi vertici possono essere colorati scegliendo tra due colori prefissati in modo che due vertici adiacenti abbiano sempre colore diverso. Una tale colorazione, se possibile, è detta 2-colorazione.

Più in generale, una colorazione dei vertici di un grafo con k colori prefissati, $k \geq 2$, che soddisfi la stessa condizione si chiama una k-colorazione. Si tratta cioè di una funzione

$$c : V \to \{1, \ldots, k\}$$

dove $c(v)$ è il colore del vertice v, tale che, per ogni coppia di vertici adiacenti v e w si abbia $c(v) \neq c(w)$.

Un risultato di notevole importanza, la cui dimostrazione è stata ottenuta con l'aiuto del computer, è il *Teorema dei 4 colori* che afferma che ogni grafo planare ammette una 4-colorazione. Ciò dimostra in modo rigoroso un'antica congettura (risalente alle metà del 1800), secondo la quale sono sufficienti 4 colori diversi per disegnare qualsiasi carta geografica, rispettando il vincolo che stati o regioni confinanti siano dipinti sempre con colori diversi.