**Università degli studi di Modena e Reggio Emilia**

**Dipartimento di Ingegneria Enzo Ferrari**

# Matematica Discreta

**Anno Accademico 2023/24**

# Indice

# Capitolo 1

# Complementi su insiemi e relazioni

## 1.1 Funzioni

Una **funzione** o **applicazione** tra due insiemi A e B è una legge per cui per ogni elemento del primo insieme esiste uno e un solo elemento del secondo insieme e viene rappresentata:

$$f : A \to B \; t.c. \; \forall a \in A \; \exists! b \in B \mid f(a) = b$$

$b$ è l'**immagine** di $a$.

### Proprietà delle Funzioni

1. la funzione si dice **iniettiva** se vale che: $\forall a, a' \in A,\ f(a) = f(a') \Rightarrow a = a'$.
2. la funzione si dice **suriettiva** sevale che: $\forall b \in B, \exists a \in A \mid f(a) = b$.
3. una funzione $f : A \to B$ si dice **biettiva** o **biunivoca** se è contemporaneamente *iniettiva* e *suriettiva* ovvero se:

$$\boxed{\forall b \in B} \quad \boxed{\exists! a \in A} \quad t.c. \; f(a) = b$$

il box rosso identifica l'**iniettività**, mentre il box verde identifica la **suriettività**.

## 1.2 Insiemi Discreti

Due insiemi A e B si dicono **equipotenti** (o con la stessa **cardinalità**) se:

$$f : A \to B,\ f\ biunivoca$$

Siccome $f$ è **biunivoca** avremo che ogni elemento di A avrà **uno e un solo** elemento di B distinto e B sarà formato da sole immagini di A portando i due insieme ad avere "lo stesso numero" di elementi, utilizzeremo come notazione: $\#A = \#B$. Un insieme A si dice **finito** se:

$$\exists n \in \mathbb{N},\ f : A \to \mathbb{N}_n,\ f\ biunivoca$$

| | |
|---|---|
| $A = \{\square, \boxdot, \blacksquare\}$ | contando i simboli dell'insieme A si va a creare |
| $\mathbb{N}_3 = \{1, 2, 3\}$ | un'associazione tra gli elementi di A e di $\mathbb{N}_3$ |

In questo caso diremo che la **cardinalità** di A è **n**: $\#A = \#\mathbb{N}_n = n$
Un insieme A si dice **numerabile** se:

$$\exists f : A \to \mathbb{N},\ f\ biunivoca$$

In questo caso si dice che A ha cardinalità numerabile e si può rappresentare attraverso la lettera **aleph** (è la prima lettera dell'alfabeto ebraico): $\#A = \#\mathbb{N} = \aleph_0$ (si ricordi: **il Paradosso dell'albergo di Hilbert**).
Alcuni esempi:

1. l'insieme $\mathbb{Z}$ è **numerabile** ($\#\mathbb{N} = \#\mathbb{Z}$):

$$\begin{array}{cc} & 0 \to 1 \\ 1 \to 2 & -1 \to 3 \\ 2 \to 4 & -2 \to 5 \end{array}$$

   possiamo quindi mappare i valori **positivi** dell'insieme $\mathbb{Z}$ sono mappati nei valori **pari** dell'insieme $\mathbb{N}$ e in maniera complementare i valori **negativi** dell'insieme $\mathbb{Z}$ sono mappati nei valori **dispari** dell'insieme $\mathbb{N}$. È quindi possibile verificare la biunivocità dell'applicazione che mappa i valori da $\mathbb{Z}$ a $\mathbb{N}$.

2. l'insieme dei numeri **pari** $\mathbb{P}$ può definirsi numerabile, infatti: $\#\mathbb{P} = \#\mathbb{N}$, in questo caso avremo l'applicazione biunivoca del tipo:

$$f : \mathbb{P} \to \mathbb{N} \mid \forall p = 2n \in \mathbb{P},\ f(p) = \frac{1}{2}p = n$$

> Un insieme A si dice **discreto** se è **finito** o **numerabile** (tutti gli insiemi *numerabili* sono infiniti, ma non tutti gli insimi infiniti sono numerabili)

Se A è finito di cardinalità **n**, i suoi elementi possono essere etichettati con gli elementi di $\mathbb{N}_n$:
$A = \{a_1, a_2, ..., a_n\}$

Se A è numerabile, gli elementi possono essere "etichettati" con gli elementi di $\mathbb{N}$:
$A = \{a_1, a_2, ..., a_n, ...\} = \{a_i \mid i \in \mathbb{N}\}$

**Funzione Caratteristica**: è un'applicazione ce determina se un elemento appartiene o meno ad un sottoinsieme Y di A ($Y \subseteq A$). Quindi diremo che dato un insieme discreto A ed un suo sottoinsieme $Y \subseteq A$ si dice **funzione caratteristica** di Y la funzione:

$$f_Y : A \to \{0,1\}\ \forall a \in A \qquad\qquad f_Y(a) = \begin{cases} 1 & se\ a \in A \\ 0 & se\ a \notin A \end{cases}$$

Nel caso in cui A sia un insieme finito avremo che: $\#A = \sum_{a \in A} f_Y(a)$.
Se A è un insieme discreto, ed $f : A \to \{0,1\}$ una applicazione a valori in $\{0,1\}$, risulta univocamente determinato il sottoinsieme $Y \subseteq A$ tale che $f$ sia una funzione caratteristica di $Y$:

$$Y = \{a \in A \mid f(a) = 1\}$$

Un esempio, definiamo $A = \mathbb{N}$ e sia $f : A \to \{0,1\}$ definita da una **funzione caratteristica** del tipo: $n \to \frac{1+(-1)^n}{2}$. In questo caso la funzione $f$ identifica, a partire dall'insieme $\mathbb{N}$, il sottoinsieme $\mathbb{P}$ dei numeri pari.
Utilizzando la **funzione caratteristica** si può ricavare la seguente proprietà degli insiemi discreti:

- se A è finito di cardinalità $n$, l'insieme $\mathcal{P}(a)$ delle **parti di A** è in corrispondenza biunivoca con l'**insieme delle n-ple** a valori in $\{0,1\}$.
- se A è numerabile, l'insieme $\mathcal{P}(a)$ delle parti di A è in corrispondenza biunivoca con l'**insieme delle successioni** a valori in $\{0,1\}$.

### 1.2.1 Proprietà 1

Se X e Y sono insiemi **finiti**, con $\#X = n$, $\#Y = m$ e con $X \cap Y = \emptyset$, allora $\#(X \cup Y) = n + m$.

**Dimostrazione**: per Hp. esistono due funzioni biettive $f : X \to \mathbb{N}_n$ e $g : Y \to \mathbb{N}_m$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}_{n+m}$. Possiamo porre $\forall c \in X \cup Y$ come:

$$h(c) = \begin{cases} f(c) & se\ c \in X \\ g(c) + n & se\ c \in Y \end{cases}$$

### 1.2.2 Proprietà 2

Se X è un insieme **finito** con $\#X = n$ ed Y è un insieme **numerabile**, con $X \cap Y = \emptyset$ allora $\#(X \cup Y)$ è **numerabile**.

**Dimostrazione**: per Hp. esistono due funzioni biettive $f : X \to \mathbb{N}_n$ e $g : Y \to \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}$. Possiamo porre $\forall c \in X \cup Y$ come:

$$h(c) = \begin{cases} f(c) & se\ c \in X \\ g(c) + n & se\ c \in Y \end{cases}$$

### 1.2.3 Proprietà 3

Se X e Y sono due insiemi **numerabili**, allora anche $X \cup Y$ è **numerabile**.

Dimostrazione: senza perdere di generalità, supponiamo che $X \cap Y = \emptyset$. Per ipotesi esistono due funzioni biettive $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}$. Ad esempio, $\forall c \in (X \cup Y)$, si può porre:

$$h(c) = \begin{cases} 2f(c) - 1 & se\ c \in X \\ 2g(c) & se\ c \in Y \end{cases}$$

Off-Topic:

**Paradosso del Grand Hotel di Hilbert**: il paradosso del *Grand Hotel* inventato dal matematico *David Hilbert* per mostrare alcune caratteristiche del concetto di infinito e le differenze fra opzioni con insieme finiti ed infiniti. Hilbert immagina un hotel con infinite stanze, tutte occupate, e afferma che qualsiasi sia il numero di altri ospiti che sopraggiungano, sarà sempre possibile ospitarli tutti, anche se il loro numero è infinito, purché numerabile.

Nel caso semplice, arriva un singolo nuovo ospite. Il furbo albergatore sposterà tutti i clienti nella camera successiva (l'ospite della 1 alla 2, quello della 2 alla 3, etc.); in questo modo, benché l'albergo fosse pieno è comunque, essendo infinito, possibile sistemare il nuovo ospite. Un caso meno intuitivo si ha quando arrivano infiniti nuovi ospiti. Sarebbe possibile procedere nel modo visto in precedenza, ma solo scomodando infinite volte gli ospiti (già spazientiti dal precedente spostamento): sostiene allora Hilbert che la soluzione sta semplicemente nello spostare ogni ospite nella stanza con numero doppio rispetto a quello attuale (dalla 1 alla 2, dalla 2 alla 4,etc.), lasciando ai nuovi ospiti tutte le camere con i numeri dispari, che sono essi stessi infiniti, risolvendo dunque il problema. Gli ospiti sono tutti dunque sistemati, benché l'albergo fosse pieno.

**Proposizione**: se X è un insieme numerabile e $Y \subseteq X$ allora Y è un insieme **discreto**.

### 1.2.4 Proprietà 4

Se $\{A_i \mid i \in \mathbb{N}\} = \{A_1, A_2, ..., A_i, ...\}$ è un **insieme numerabile** di **insiemi numerabili**, si ha che:

$$\#(\bigcup_{i\in\mathbb{N}} A_i) = \#\mathbb{N}$$

**Dimostrazione**: senza perdere di generalità, supponiamo che gli insiemi siano fra loro **disgiunto**: $A_i \cap A_j = \emptyset$, $\forall i \in j$. Per dimostrare la tesi, utilizziamo il *procedimento diagonale di **Cantor***, enumerando per righe gli elementi di ciascun insieme, dove avremo come primo indice l'identificativo dell'insieme e come secondo indice quello della colonna:

$$\begin{array}{ccccccc}
A_1: & a_{11} & a_{12} & a_{13} & \dots & a_{1h} & \dots \\
A_2: & a_{21} & a_{22} & a_{23} & \dots & a_{2h} & \dots \\
A_3: & a_{31} & a_{32} & a_{33} & \dots & a_{3h} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
A_i: & a_{i1} & a_{i2} & a_{i3} & \dots & a_{ih} & \dots \\
\dots & \dots & .. & \dots & \dots & \dots & \dots
\end{array}$$

Consideriamo le diagonali $D_1 = \{a_{11}\}$, $D_2 = \{a_{21}, a_{12}\}$, ..., $D_k$, ..., dove: $D_k = \{a_{ij} \mid i+j = k+1\}$, dove il valore delle $j$ identifica la posizione all'interno della diagonale $D_k$. Notiamo che sono composte da finiti elementi. Per dimostrare che $\#(\bigcup_{i\in\mathbb{N}} A_i)$ è **numerabile**, occorre costruire una applicazione biunivoca, tale che:

$$h : \bigcup_{i\in\mathbb{N}_n} A_i \to \mathbb{N}$$

Idealmente, vorremmo etichettare, ogni generico elemento $a_{ij}$ che apparterrà alla $k-$*esima* diagonale, in questo modo si creerà l'applicazione *biunivoca*.

$\#D_k = k$ $\quad\to$ ci serve la somma delle cardinalità delle diagonali precedenti alla diagonale tale che $a_{ij} \in D_k$ $\to$ $\sum_{k=1}^{i+j-2} \#D_k = \frac{(i+j-2)\cdot(i+j-1)}{2}$

In questo modo abbiamo "etichettato" tutti gli elementi appartenenti alle diagonali precedenti alla diagonale di riferimento $D_k$, ora ci mancano da "etichettare" gli elementi che precendo $a_{ij}$ sulla diagonale, ma sapendo che $a_{ij}$ è il **j-esimo** elemento allora basterà:

$$h(a_{ij}) = j + \frac{(i+j-2)(i+j-1)}{2}$$

In questo modo abbiamo "etichettato" anche tutti gli elementi che precedono il nostro $a_{ij}$, ma in direttamente abbiamo descritto un'applicazione **biunivoca** tra $\bigcup_{i \in \mathbb{N}_n} A_i$ e $\mathbb{N}$, ovvero $h(a_{ij})$ che quindi ci permette di dimostrare che anche $\bigcup_{i \in \mathbb{N}_n} A_i$ è **numerabile**.

**Conseguenze**:

- $\mathbb{Z}$ è numerabile: $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$.
- $\mathbb{N} \times \mathbb{N}$ è numerabile: $\mathbb{N} \times \mathbb{N} = \{(n, m) \mid n, m \in \mathbb{N}\} = \bigcup_{n \in \mathbb{N}} \{(n, m) \mid m \in \mathbb{N}\}$.
- $\mathbb{Q}$ è numerabile.

## 1.3 Confronto tra Cardinalità

Si dice che un insieme A ha **cardinalità minore o uguale** ad un insieme B (e si indica con: $\#A \leq \#B$) se: $\exists f : A \to B,\ f$ è *iniettiva*.

**Proprietà**:

- **riflessività**: $\forall A,\ \#A \leq \#A$.
- **transitività**: $\#A \leq \#B,\ \#B \leq \#C \Rightarrow \#A \leq \#C$.
- **antisimmetria**: $\#A \leq \#B,\ \#B \leq \#A \Rightarrow \#A = \#B$.
- **tricotomia**: $\forall A, B \Rightarrow \#A \leq \#B \ o \ \#B \leq \#A$.

La relazione "$\leq$" fra cardinalità è una relazione di ordine totale.

**Lemma**: $A \subseteq B \subseteq C$ con $\#A = \#B \Rightarrow \#A = \#B = \#C$.

**Teorema di Cantor-Bernstein-Schroeder**: Se $\exists f : A \to B,\ f$ *iniettiva* ed $\exists g : B \to A,\ g$ *iniettiva* allora $\exists h : A \to B,\ h$ *biunivoca*.

**Dimostrazione**: poiché $f$ e $g$ sono iniettive se le restriangamo alla loro immagine biunivoca:

$$\#A = \#f(A) \ con \ f(A) \subseteq B$$
$$\#B = \#g(B) \ con \ g(B) \subseteq A$$

Avremo:

$$g(f(A)) \subseteq g(B) \subseteq A \Rightarrow \#g(f(A)) = \#f(A) = \#A$$

e per il lemma possiamo dire che $\#g(B) = \#A$ e $\#g(B) = \#B$ e quindi avremo che $\#A = \#B$, questo implica che esiste una funzione $h : A \to B$ biunivoca.

**Teorema di Cantor**: se $A$ è un insieme **numerabile** allora $\mathcal{P}(A)$ ha cardinalità **maggiore** di $A$:

$$\#A \leq \#\mathcal{P}(A) \; con \; \#A \neq \#\mathcal{P}(A)$$

**Dimostrazione**:

- dimostriamo per prima cosa che $\#A \leq \#\mathcal{P}(A)$ basta trovare una funzione definita $f : A \to \mathcal{P}(A)$ che sia **iniettiva** e non biunivoca.

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

  Utilizziamo una **dimostrazione per assurdo**: sappiamo che $\mathcal{P}(A)$ è in corrispondenza biunivoca con le successioni a valori in $\{0, 1\}$; allora se $\mathcal{P}(A)$ fosse numerabile sarebbe possibile elencare tutte le successioni a valori in $\{0, 1\}$:

$$\begin{array}{ccccccc}
S_1\colon & S_{11} & S_{12} & S_{13} & \dots & S_{1n} & \dots \\
S_2\colon & S_{21} & S_{22} & S_{23} & \dots & S_{2n} & \dots \\
S_3\colon & S_{31} & S_{32} & S_{33} & \dots & S_{3n} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
S_j & S_{j1} & S_{j2} & S_{j3} & \dots & S_{jn} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{array}$$

Consideriamo la successione a valori in $\{0, 1\}$:

$$\bar{S} = \bar{S}_1,\ \bar{S}_2,\ \bar{S}_3,\ \dots,\ \bar{S}_j,\ \dots \;||\; \text{dove } \bar{S}_j \neq S_{jj}$$

In questo modo la successione $\bar{S}$ non coincide con nessuna delle successioni $s_j$, $\forall j \in \mathbb{N}$, poiché differisce dalla j-esima successione nel j-esimo elemento e quindi arriviamo ad un **assurdo**. Quindi l'insieme delle successioni a valori in $\{0, 1\}$ non può essere numerabile e, quindi, **non** è **numerabile** nemmeno $\mathcal{P}(A)$.

**La Cardinalità di** $\mathbb{R}$: anche $\mathbb{R}$ **non** è **numerabile**, infatti: $\#\mathbb{R} = \#]0,1[$, consideriamo un'applicazione biunivoca tale che $f : \mathbb{R} \to ]0,1[$, ad esempio:

$$f(x) = \tfrac{x}{|x|+1}\ \forall x \in \mathbb{R}$$

che stabilisce biunivocità tra $\mathbb{R}$ e $]-1,1[$ possiamo affermare che $\#\mathcal{P}(\mathbb{N}) = \#]0,1[$, infatti considerando $\forall x \in ]0,1[$ come la rappresentazione binaria (con virgola) di $x$; se $\epsilon_n$ è l'n-esima cifra dopo la virgola di tale sviluppo $(\epsilon_1, \epsilon_2, ..., \epsilon_n, ...)$ è una successioni a valori in $\{0,1\}$ quindi

$$0,\bar{9} = 1 \in \mathbb{R} \ ||\ \text{viene a perdersi la biunivocità}$$
$$\Rightarrow \#\mathbb{R} = \#\mathcal{P}(\mathbb{N})$$

Questa tipologia di cardinalità viene definita **cardinalità del continuo** e si denota con $\mathbf{c}$ o con $2^{\aleph_0}$.

**Congettura** (*ipotesi del continuo*)

non esistono cardinalità comprese fra $\#\mathbb{N}$ e $\#\mathbb{R}$.

**Congettura** (*ipotesi generalizzata del continuo*)

non esistono cardinalità comprese tra $\#X$ e $\mathcal{P}(X) = 2^{\#X}$ $\forall X$ di cardinalità non finita.

## 1.4 Relazioni di Equivalenza

Una **relazione** $\mathcal{R}$ tra due insiemi A e B è un **sottoinsieme** del **prodotto cartesiano** fra A e B, ovvero $\mathcal{R} \in A \times B$.

**Esempio**

$\mathcal{R} =' \leq'$ è relazione tra i due insiemi $A = \mathbb{N}$ e $B = \mathbb{N}$, poiché definisce un sottoinsieme del prodotto cartesiamo $\mathbb{N} \times \mathbb{N}$.

Ad esempio: $(1, 2) \in \mathcal{R}$ e $(2, 1) \notin \mathcal{R}$.

Una relazione $\mathcal{R}$ su A si dice **relazione di equivalenza** se sono vere le seguenti proprietà:

- *riflessività*: $\forall a \in A \Rightarrow a\mathcal{R}a$
- *simmetria*: $\forall a, b \in A \ : \ a\mathcal{R}b \Rightarrow b\mathcal{R}a$
- *transitività*: $\forall a, b, c \in A \ : \ a\mathcal{R}b$ e $b\mathcal{R}c \Rightarrow a\mathcal{R}c$

**Definizione**: sia $\mathcal{R}$ una **relazione di equivalenza** su A. Per ogni $a \in A$ si dice **classe di equivalenza** $[a] = \{x \in A \mid x\mathcal{R}a\}$.

**Proprietà**:

- $\forall a \in A, \ a \in [a]$

  **Dimostrazione**: è conseguenza diretta della proprietà riflessiva.

- $\forall a, b \in A, \ a \in [b] \Rightarrow [b] = [a]$

  **Dimostrazione**: poiché $a \in [b]$, $a\mathcal{R}b$. Se $x \in A$, $x \in [a]$, allora $x\mathcal{R}a$; per la **proprietà transitiva** segue $x\mathcal{R}v$ ovvero $x \in [b]$. Resta così dimostrato che $[a] \subseteq [b]$. Analogamente, se $y \in A$, $y \in [b]$, allora $y\mathcal{R}b$ per la **proprietà di simmetria**, $a\mathcal{R}b \Rightarrow b\mathcal{R}a$, per cui la transitività assicura $y\mathcal{R}a$, ovvero $y \in [a]$. Resta così dimostrato che $[b] \subseteq [a]$ e quindi $[b] = [a]$.

- $\forall a, b \in A, \ [a] = [b]$ *oppure* $[a] \cap [b] \neq \emptyset$

  **Dimostrazione**: se $\exists c \in [a] \cap [b]$, si ha $c \in [a] ec \in [b]$, ovvero $c\mathcal{R}a$ e $c\mathcal{R}b$. Applicando la **proprietà di simmetria** a $c\mathcal{R}a$ si ottiene $a\mathcal{R}c$, per cui la proprietà transitiva assicura $a\mathcal{R}b$, ovvero $a \in [b]$. La seconda proprietà implica $[a] = [b]$. Quindi, se due classi hanno un elemento in comune, le due classi coincidono.

**Insieme Quoziente**: sia A un insieme ed $\mathcal{R}$ una relazione di equivalenza su A. Si definisce **insieme quoziente** di A rispetto ad $\mathcal{R}$,

$$\frac{A}{\mathcal{R}} = \{[a] \mid a \in A\}$$

**Rappresentante di una classe d'equivalenza**: sia A un insieme ed $\mathcal{R}$ una relazione di equivalenza su A. Ogni elemento $x \in [a]$, si dice **Rappresentante** di $[a] \in \frac{A}{\mathcal{R}}$.
Sia $\mathcal{R}$ la relazione di equivalenza su $\mathbb{R}$ definita da:

$$(a, b) \in \mathbb{R} \text{ se e solo se } a - b \in \mathbb{Z}$$

L'insieme quoziente $\frac{\mathbb{R}}{\mathcal{R}}$ è in corrispondenza biunivoca con $[0, 1[$: ogni classe può infatti avere come rappresentante significativo il suo unico elemento nell'intervallo $[0, 1[$.

**Esempio**: sia $\mathcal{R}$ la **relazione di equivalenza** su $\mathbb{N}_0 \times \mathbb{N}_0$ definita da:

$$(a, b)\mathcal{R}(a', b') \text{ se e solo se } a + b' = a' + b$$

In generale:

- se $a = b$, $[(a, b)] = \{(n, n) \mid n \in \mathbb{N}\}$
- se $a < b$, $[(a, b)] = \{(n, n + b - a) \mid n \in \mathbb{N}\}$
- se $a > b$, $[(a, b)] = \{n + a - b, n \ \mid n \in \mathbb{N}\}$

Allora l'insieme quoziente $\frac{\mathbb{N}_0 \times \mathbb{N}_0}{\mathcal{R}}$ è in relazione biunivoca con $\mathbb{Z}$.

**Esempi**

Sia $\mathcal{R}$ la relazione di equivalenza su $\mathbb{N}$ definita da $(a, b) \in \mathcal{R}$ se e solo se $(-1)^a = (-1)^b$. L'**insieme quoziente** è formato da due classi $\frac{\mathbb{N}}{\mathcal{R}} = \{\mathbb{P}, \mathbb{D}\}$

Sia $\mathcal{R}$ la relazione di equivalenza su $\mathbb{R}$ definita da $(a, b) \in \mathbb{R}$ se e solo se $\lfloor a \rfloor = \lfloor b \rfloor$. L'**insieme quoziente** è in corrispondenza biunivoca con $\mathbb{Z}$ (il passaggio da $\mathbb{R}$ a $\frac{\mathbb{R}}{\mathcal{R}}$ è un esempio di **discretizzazione**): $\frac{\mathbb{R}}{\mathcal{R}} = \{[n, n+1[, n \in \mathbb{Z}\}$

## 1.5 Congruenza modulo n

**Definizione**: fissa un intero $n \in \mathbb{N}$, si definisce una relazione di equivalenza $\equiv_n$ su $\mathbb{Z}$:

$$x \equiv_n y \text{ se e solo se } \exists h \in \mathbb{Z} \mid y - x = h \cdot n$$

Verifichiamo che $\equiv_n$ è una **relazione di equivalenze**:

- **riflessività**: $\forall x \in \mathbb{Z},\ x \equiv_n x$ è verificato, poiché $x - x = h \cdot n$ considerando $h = 0 \in \mathbb{Z}$.
- **simmetria**: se $x \equiv_n y$, per definizione $\exists h \in \mathbb{Z}$ tale che $y - x = h \cdot n$. Per dimostrare che $y \equiv_n x$ devo trovare un $h' \in \mathbb{Z} \mid x - y = h' \cdot n$. Basta prendere $h' = -h$.
- **transitività**: se $x \equiv_n y$ e $y \equiv_n <$, allora $\exists h \in \mathbb{Z} \mid y - x = h \cdot n$ ed $\exists k \in \mathbb{Z} \mid z - y = k \cdot n$. Sommando membreo a membro, si ottiene $z - x = (h + k) \cdot n$; siccome $h + k \in \mathbb{Z}$ segue che $x \equiv_n z$.

**Insieme delle classi resto modulo n**: l'insieme quoziente $\mathbb{Z}/\equiv_n$ è detto **insieme delle classi resto modulo** $n$ ed è indicato con $\mathbb{Z}_n$: $\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv_n}$.
L'insieme delle classi resto modulo $n$ è costituito da:

$$\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$$

**Dimostrazione**: Per ogni $x \in \mathbb{Z}$, la divisione euclidea per $n$ assicura che $\exists q, r \in \mathbb{Z},\ 0 \leq r < n$ tali che $x = q \cdot n + r$, ovvero che $x - r = q \cdot n$. Quindi, $x \equiv_n r$, da cui $[x] = [r]$, con $r \in \{0, 1, ..., n-1\}$.
Occorre provare che le n classi $[0], [1], ..., [n-1]$ sono a due a due disgiunte, ovvero che $\forall r, s \in \mathbb{Z},\ 0 \leq r < s < n \Rightarrow [r] \neq [s]$. Per **assurdo** supponiamo $[r] = [s]$, questo significherebbe che che $\exists h \in \mathbb{Z} \mid s - r = h \cdot n$. Per ipotesi $s > r$, per cui $0 < s - r < n$; quindi $s - r$ **non** può essere multiplo intero di $n$.

> **Divisione euclidea**: $\forall a, b \in \mathbb{Z},\ b \neq 0 \Rightarrow \exists q, r \in \mathbb{Z},\ 0 \leq r < |b| \mid a = b \cdot q + r$.

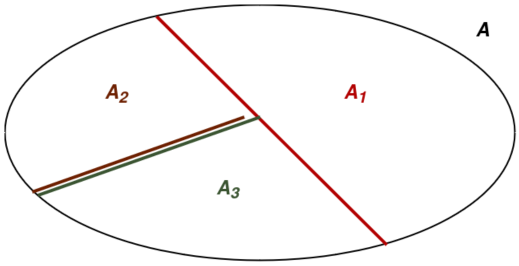



Figura 1.1: **Partizionamento**

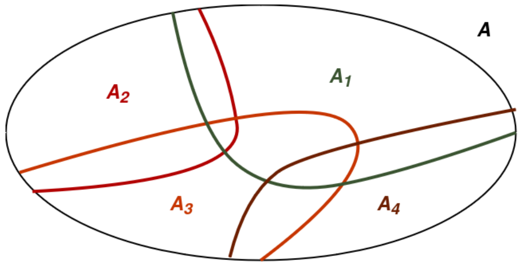



Figura 1.2: **Ricoprimento**

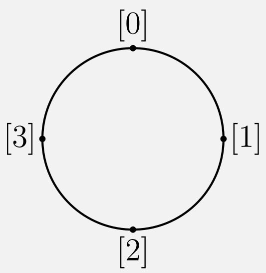
Sia A un insieme; un sottoinsieme $\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **partizione** di A se $\emptyset \notin \mathcal{B}$ e $\forall c \in A,\ \exists! B \in \mathcal{B} \mid x \in B$. Ovvero ogni sottoinsieme non ha intersezione con gli altri.

Sia A un insieme; un sottoinsieme $\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **ricoprimento** di A se $\forall x \in A,\ \exists B \in \mathcal{B} \mid x \in B$.

Se $\mathcal{R}$ è relazione di equivalenza su A, allora l'insieme quoziente $\frac{A}{\mathcal{R}} = \mathcal{B}$ è una partizione di A. Viceversa se $\mathcal{B}$ è una partizione di A, $\exists! \mathcal{R}$ relazione di equivalenza su A tale che $\frac{A}{\mathcal{R}} = \mathcal{B}$ allora $\mathcal{R}$ è definita da:

$$x \mathcal{R} y \Leftrightarrow \exists B \in \mathcal{B} \mid x, y \in B$$

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$




$\mathbb{Z}$ è più facilmente rappresentabile tramite una circonferenza

# Capitolo 2

# Parte 3

## 2.1 Strutture algebriche elementari

Una **operazione binaria intera** su un insieme G è un'applicazione

$$* \ : \ G \times G \to G$$

L'immagine della coppia $(x, y)$ si denoterà con $x * y$.

- $e \in G$ si dice **elemento neutro** rispetto a $*$ se:

$$g * e = e * g = g \ \forall g \in G$$

- un elemento $g \in G$ si dice invertibile se esiste $\bar{g} \in G$ tale che $g * \bar{g} = \bar{g} * g = e$

### 2.1.1 Gruppi

La coppia $(G, *)$, con $*$ operazione su G, si dice **gruppo** se vengono rispettate le seguenti proprietà:

- $*$ è **associativa**: $\forall g, g', g'' \in G$ si ha $(g * g') * g'' = g * (g' * g'')$
- esiste l'elemento **neutro**
- ogni elemento di G è invertibile

Il gruppo si dice **abeliano** o **commutativo** se:

$$\forall g, g' \in G, \ g * g' = g' * g \text{ (proprietà } \textbf{commutativa}\text{)}$$

Alcuni esempi:

- $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$ non sono gruppi. In quanto non né in $\mathbb{N}$ né in $\mathbb{Z}$ è presente per ogni elemento dell'insieme l'elemento inverso, in $\mathbb{N}$ non sono presenti elementi negativi, quindi nessun elemento avrà un'altro elemento che sommato a se stesso dia 0, viceversa l'insieme $\mathbb{Z}$ dove sono presenti elementi positivi e negativi viene, invece, definita l'operazione $\cdot$ che richiede i reciproci dei singoli elementi affiché possano essere definiti gli elementi inversi.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, \cdot)$ sono gruppi abeliani

### 2.1.2 Anelli

La terna $(\mathbb{A}, +, \cdot)$ con $\mathbb{A}$ un insieme e $+, \cdot$ (somma e prodotto) due operazione binarie interne a $\mathbb{A}$, si dice **anello** se:

- $(\mathbb{A}, +, \cdot)$ è un gruppo **abeliano** (con elemento neutro 0).
- il prodotto è **associativo**.
- per ogni $x, y, z \in \mathbb{K}$ si ha $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ e $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ (il prodotto è distribuito rispetto alla somma).

Un anello $(\mathbb{A}, +, \cdot)$ è detto **commutativa** se il prodotto è commutativo, mentre è detto **unitario** o con **unità** se $(\mathbb{A}, \cdot)$ ammette l'elemento neutro. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono anelli.

### 2.1.3 Campi

La terna $(\mathbb{K}, +, \cdot)$ con $\mathbb{K}$ un insieme e $+, \cdot$ (somma e prodotto) due operazioni binarie interne a $\mathbb{K}$, si dice **campo** se:

- $(\mathbb{K}, +)$ è un gruppo **abeliano** (con elemento neutro 0).
- $(\mathbb{K} - \{0\}, \cdot)$ è un gruppo **abeliano** (con elemento neutro 1).
- per ogni $x, y, z \in \mathbb{K}$ si ha $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ quindi il prodotto è distribuito rispetto alla somma.

In qualunque campo vale la **legge di annullamento del prodotto**:

$$x \cdot y = 0 \rightarrow x = 0 \text{ oppure } y = 0$$

### 2.1.4 Domini d'integrità

**Divisori dello zero**: sia $(A, +, \cdot)$ un anello. Due elementi $a, b \in A$ si dicono **divisori dello zero** se $a \neq 0$, $b \neq 0$, ma $a \cdot b = 0$. Ovvero, può succedere che in un anello due elementi non nulli il cui prodotto fa 0.

> Ad esempio l'anello delle matrici quadrate presenta dei divisori dello zero, infatti due matrici non nulle è possibile che il loro prodotto presenti la matrice nulla.
>
> $$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$
> $$A \cdot B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} (1 \cdot 1 + 1 \cdot -1) & (1 \cdot -1 + 1 \cdot 1) \\ (1 \cdot 1 + 1 \cdot -1) & (1 \cdot -1 + 1 \cdot 1) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

**Dominio di Integrità**: Un anello commutativo privo di divisori dello zero si dice **dominio di integrità**.

> Ad esempio $(\mathbb{Z}, +, \cdot)$ è un **anello commutativo unitario** privo di divisori dello zero. Quindi è dominio di integrità.

## 2.2 L'anello dei numeri interi

È noto che $\exists h \mid h : \mathbb{Z} \to \frac{\mathbb{N}_0 \times \mathbb{N}_0}{\mathcal{R}}$ dove la relazione di equivalenza che si vuole definire è $\equiv_n$. Su questo insieme vengono **ben poste** le seguenti operazioni:

$$\boxplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$((m, n), (m', n')) \mapsto [(m, n)] \boxplus [(m', n')] \overset{\text{def}}{=} [(m + m', n + n')]$$
$$\boxdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$((m, n), (m', n')) \mapsto [(m, n)] \boxdot [(m', n')] \overset{\text{def}}{=} [(mm' + nn', mn' + m'n)]$$

Definito questo possiamo dire che $(\mathbb{Z}, \boxplus, \boxdot)$ è **dominio di integrità**.

## 2.3 Teoria della Divisibilità

**Divisibilità**: dati due numeri $a, b \in \mathbb{Z}$, si dice che $a$ **divide** $b$ (e si scrive $a|b$) se: $\exists c \in \mathbb{Z} \mid b = a \cdot c$

**Esempi**

- $2|12,\ \exists c\ t.c.\ 2 \cdot c = 2 \cdot 6 = 12$
- $3|7m\ \nexists c\ t.c.\ 3 \cdot c = 7\ \forall c \in \mathbb{Z}$

**Proprietà**:

- **transitività**: se $n|m$ e $m|q$ allora $n|q$.

  **Dimostrazione**

  Hp. $\exists h \in \mathbb{Z} \mid m = h \cdot n \qquad \exists h' \in \mathbb{Z} \mid q = h' \cdot m$

  Sostituendo la prima relazione nella seconda si ottiene $q = h' \cdot h \cdot n$. Poichè $h' \cdot h \in \mathbb{Z}$ abbiamo definito che $n|q$.

- se $n|m$ e $m|n$, allora $m \pm n$.

  **Dimostrazione**

  Hp. $\exists h \in \mathbb{Z} \mid m = h \cdot n \qquad \exists h' \in \mathbb{Z} \mid n = h' \cdot m$

  Andiamo a sostituire la seconda alla prima equazione:

$$n = h' \cdot h \cdot m$$
$$n - h' \cdot h \cdot m = 0$$
$$n \cdot (1 - h' \cdot h) = 0$$

  Essendo che $\mathbb{Z}$ è un **dominio di integrità**, segue che o $n = 0$ oppure $(1 - h' \cdot h) = 0 \to (h' \cdot h) = 1$, consideriamo che $n \leq 0$ e che quindi $h' \cdot h = 1$ sappiamo che $h$ ammette un inverso $h'$, da cui $h = h' = 1$ o $h = h' = -1$ (in $\mathbb{Z}$, gli unici elementi che ammettono inverso sono 1 e $-1$). In questo modo sappiamo che $m = n$ oppure $m = -n$.

## 2.4 Massimo Comune Divisore

Dati $a, b \in \mathbb{Z}$ non entrambi nulli, si dice che $d \in \mathbb{Z}$ è **UN massimo comune divisore** tra $a$ e $b$ se valgono contemporaneamente le due proprietà:

$$d|a \text{ e } d|b \qquad \forall d' \in \mathbb{Z} \mid d'|a,\ d'|b \Rightarrow d'|d$$

Se $d$ e $d'$ sono due massimi comuni divisori tra $a$ e $b$ allora $d' = \pm d$.

**Dimostrazione**

$\forall d' \in \mathbb{Z} \ \Rightarrow\ d'|a,\ d|b \ \Rightarrow\ d'|d \ \Rightarrow\ d = \pm d'$

$\forall d \in \mathbb{Z}\ d|a,\ d|b \ \Rightarrow\ d|d'$

Dati $a, b \in \mathbb{Z}$ non entrambi nulli, si dice che $d \in \mathbb{Z}^+$ è **IL massimo comune divisore** (***Greatest Common Divisor***) tra $a, b$ se $d$ è un *massimo comune divisore* fra $a$ e $b$ (fra i due possibili **MCD** prendo il massimo, quindi quello positivo).

$$d = \gcd(a, b)$$

**Esempio**

Se $a|b$, allora $\gcd(a, b) = |a|$ e in particolare $\gcd(a, 0) = |a|\ \forall a \in \mathbb{Z} - \{0\}$

Dati $a, b \in \mathbb{Z}$ non entrambi nulla, allora $\boxed{\exists! \gcd(a, b)}$ e viene inoltre definita l'**Identità di *Bezout*** che rappresenta il massimo comun divisore come combinazione lineare di $a$ e $b$:

$$\gcd(a, b) = a \cdot \alpha + b \cdot \beta$$

Questi valori ($\alpha$ e $\beta$) però non sono strettamente univocamente determinata, infatti in generale una coppia di numeri interi hanno più di un $\alpha$ e un $\beta$ definiti.

**Dimostrazione**

Consideraiamo un insieme S costituito da tutte le combinazioni lineari intere di $a, b$ che abbia però risultati strettamente positivi.

$$S = \{\lambda \cdot a + \mu \cdot b \mid \lambda, \mu \in \mathbb{Z},\ \lambda \cdot a + \mu \cdot b > 0\}$$

Osserviamo che l'insieme S non è vuoto ($S \neq \emptyset$), infatti almeno uno tra $a$ e $b$ non è nullo, infatti ponendo $a \neq 0$ è possibile affermare che:

$$|a| = (\text{segno}) \cdot a + 0 \cdot b \ \rightarrow\ |a| \in S$$

Osserviamo che S contiene unicamente numeri naturali possiamo dire che $S \subseteq \mathbb{N}$ non vuoto e che quindi $\exists \min(s) = d$ ovvero l'insieme è limitato inferiormente. Siccome $d \in S$ questo vuol dire che è rappresentabile come **combinazione lineare**, ovvero $\boxed{\exists \overline{\lambda}, \overline{\mu} \in \mathbb{Z}\ t.c.\ d = \overline{\lambda} \cdot a + \overline{\mu} \cdot b}$.

Adesso cerchiamo di dimostrare che questo $d$ è proprio il massimo comune divisore che stavo cercando: $\boxed{\textbf{Th. } d = \gcd(a, b)}$ ovvero che $d|a$ e che $d|b$.

- partiamo dimostrando che $a|b$, andiamo a considerare la **divisione euclidea** tra $a$ e $d$.

$$\exists q \in \mathbb{Z},\ \exists r \in \mathbb{Z},\ 0 \leq r < d \mid a = q \cdot d + r$$

$$\begin{aligned} r &= a - q \cdot d \\ &= a - q \cdot (\overline{\lambda} \cdot a + \overline{\mu} \cdot b) \\ &= a - q \cdot \overline{\lambda} \cdot a + q \cdot \overline{\mu} \cdot b \\ &= a \cdot \underbrace{\boxed{(1 - q \cdot \overline{\lambda})}}_{\in \mathbb{Z}} + b \cdot \underbrace{\boxed{q \cdot \overline{\mu}}}_{\in \mathbb{Z}} \end{aligned}$$

  In questo modo abbiamo scritto $r$ come combinazione lineare di due interi, ma **se** $r \neq 0$ allora $r \in S$ siccome, però, $r < d$ e $d = \min(S)$ arriviamo ad un **assurdo**, quindi affinché vengano rispettati i vincoli bisogna che $r = 0 \quad \Rightarrow \quad a = q \cdot d + 0 = q \cdot d$ e quindi $\boxed{d|a}$

- in perfetta analogia si può dimostrare che $\boxed{d|b}$, partendo dalla **divisione euclidea** tra $b$ e $d$.

- bisogna ora dimostrare che $\forall d' \in \mathbb{Z} \mid d'|a,\ d'|b \Rightarrow d'|d$. Poiché $d = \overline{\lambda} \cdot a + \overline{\mu} \cdot b$ allora bisognerà che $\boxed{\exists h \in \mathbb{Z} \mid a = d' \cdot h}$ e $\boxed{\exists k \in \mathbb{Z} \mid b = d' \cdot k}$. Usando queste due relazioni, segue che:

$$\begin{aligned} d &= \overline{\lambda} \cdot d' \cdot h + \overline{\mu} \cdot d' \cdot k \\ &= d' \cdot \underbrace{\boxed{[(\overline{\lambda} \cdot h) + (\overline{\mu} \cdot k)]}}_{\in \mathbb{Z}} \end{aligned}$$

In questo modo siamo riusciti a dimostrare che $d'|d$.

Siamo riusciti a dimostrare il teorema di esistenza del **massimo comune divisore** in S, come il suo minimo: $d = \min(S) = \gcd(a, b)$

Siano $a, b \in \mathbb{Z}$, con $|a| \geq |b| > 0$. Se $a = b \cdot q + r$ è la **divisione euclidea** fra $a$ e $b$ allora avremo:

$$\{c \in \mathbb{Z} \mid c|a,\ c|b\} = \{c \in \mathbb{Z} \mid c|b,\ c|r\}$$

Ovvero l'insieme degli interi che dividono $a$ e $b$ sono gli stessi che dividono sia $b$ che $r$, conseguenza di questo fatto è che:

$$\gcd(a, b) = \gcd(b, r)$$

**Dimostrazione**

- partiamo dal primo insieme: $\{c \in \mathbb{Z} \mid c|a,\ c|b\}$ andiamo a dimostrare che $\boxed{\textbf{Th. } c|r}$ (perché che $c|b$ è implicito per la costruzione del problema). Poiché $c|a$ e $c|b$ allora:

$$\exists h \in \mathbb{Z} \text{ t.c. } a = c \cdot h \qquad \exists k \in \mathbb{Z} \text{ t.c. } b = c \cdot k$$

Consideriamo ora la **divisione euclidea** tra $a$ e $b$ avremo che:

$$\begin{aligned} r &= a - b \cdot q \\ &= c \cdot h - c \cdot k \cdot q \\ &= \underbrace{c \cdot (h - k \cdot q)}_{\in \mathbb{Z}} \end{aligned}$$

Quindi in questo modo abbiamo dimostrato che $c|r$.

- affrontiamo ora il secondo insieme $\{c \in \mathbb{Z} \mid c|b,\ c|r\}$ e andiamo a dimostrare che $\boxed{\textbf{Th. } c|a}$ (perché che $c|b$ è implicito per la costruzione del problema).

  Poichè $c|b$ e $c|r$ allora:

$$\exists h \in \mathbb{Z} \text{ t.c. } b = c \cdot h \qquad \exists k \in \mathbb{Z} \text{ t.c. } r = c \cdot k$$

  Consideriamo la **divisione euclidea** tra $a$ e $b$ avremo che:

$$\begin{aligned} a &= b \cdot q + r \\ &= c \cdot h \cdot q + c \cdot k \\ &= c \cdot \underbrace{(h \cdot q + k)}_{\in \mathbb{Z}} \end{aligned}$$

  Quindi in questo modo abbiamo dimostrato che $c|a$.

**Algoritmo delle Divisioni Successive (di Euclide)**