Università degli Studi della Basilicata

Dipartimento di Scienze di Base e Applicate - DISBA

Algebra

Appunti delle lezioni

Studente:
Donato Martinelli
Matr. 69060

Docente:
Prof. **Onofrio Di Vincenzo**

Anno Accademico 2025/2026

Contents

Nozione di Insieme ed Elementi Iniziamo lo studio dell'algebra introducendo il concetto fondamentale di insieme. Intuitivamente, possiamo pensare a un insieme come a un raggruppamento di oggetti ben definiti.

Definizione 0.1. Un **insieme** è una collezione di oggetti. Gli oggetti che costituiscono l'insieme sono chiamati **elementi**.

Per convenzione, si utilizzano le lettere maiuscole (come $A, B, \dots$) per indicare gli insiemi e le lettere minuscole (come $x, y, z, a, b, \dots$) per indicare gli elementi. La relazione fondamentale che lega un elemento a un insieme è l'appartenenza. Se un oggetto x è un elemento dell'insieme A, scriveremo:

$$x \in A$$

Questa scrittura si legge "x appartiene ad A" oppure "x è un elemento dell'insieme A".

Rappresentazione degli insiemi Per descrivere o rappresentare un insieme, abbiamo a disposizione due metodi principali: la rappresentazione per proprietà caratteristica e quella per elencazione.

La **proprietà caratteristica** è la condizione logica che contraddistingue in modo univoco gli elementi che fanno parte dell'insieme. Formalmente scriviamo:

$$A = \{x \mid x \text{ ha la proprietà } P\}$$

Dove P rappresenta la proprietà caratteristica dell'insieme A.

Alternativamente, se l'insieme è finito e gli elementi sono pochi, possiamo usare il **metodo per elencazione**, scrivendo esplicitamente la lista degli elementi racchiusa tra parentesi graffe:

$$A = \{a_1, a_2, a_3, a_4, a_5\}$$

Esempio pratico Vediamo come lo stesso insieme possa essere rappresentato in modi diversi e analizziamo la relazione di appartenenza.

Esempio 0.1. Consideriamo l'insieme A dei numeri naturali pari strettamente minori di 10. Possiamo scriverlo usando la proprietà caratteristica:

$$A = \{x \mid x \in \mathbb{N}, x \text{ è pari}, x < 10\}$$

Oppure possiamo rappresentarlo per elencazione:

$$A = \{0, 2, 4, 6, 8\}$$

Osserviamo che:

- $4 \in A$ (4 appartiene all'insieme perché è pari e minore di 10).
- $5 \notin A$ (5 non appartiene all'insieme).

Inclusione e Sottoinsiemi Per poter definire quando due insiemi sono uguali, dobbiamo prima introdurre il concetto di inclusione.

Definizione 0.2. Dati due insiemi A e B, si dice che A è **contenuto** in B (o che A è un **sottoinsieme** di B) se ogni elemento di A è anche un elemento di B. In simboli si scrive $A \subseteq B$. La definizione formale è:

$$A \subseteq B \iff \forall x \in A, \exists y \in B \mid x = y$$

(Ovvero: per ogni elemento x in A, esiste un elemento y in B che è uguale a x).

Uguaglianza tra insiemi Ora possiamo rispondere alla domanda: quando due insiemi A e B sono uguali? L'uguaglianza insiemistica non dipende dall'ordine degli elementi o da come vengono descritti, ma solo dal fatto che contengano esattamente gli stessi elementi.

Definizione 0.3. Due insiemi A e B si dicono uguali ($A = B$) se e solo se valgono contemporaneamente le due inclusioni:

$$A = B \iff A \subseteq B \text{ e } B \subseteq A$$

Questo significa che per dimostrare che due insiemi sono uguali, dobbiamo dimostrare che ogni elemento del primo sta nel secondo e viceversa:

$$\begin{cases} \forall x \in A \implies x \in B & (\text{quindi } A \subseteq B) \\ \forall y \in B \implies y \in A & (\text{quindi } B \subseteq A) \end{cases}$$

Operazioni con gli insiemi Definiamo ora le principali operazioni che permettono di costruire nuovi insiemi a partire da insiemi dati.

Definizione 0.4. Dati due insiemi A e B, definiamo:

- **Intersezione**: L'insieme degli elementi comuni ad entrambi.

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}$$

- **Unione**: L'insieme degli elementi che appartengono ad almeno uno dei due insiemi.

$$A \cup B = \{x \mid x \in A \text{ o } x \in B\}$$

- **Differenza**: L'insieme degli elementi che stanno in A ma non in B.

$$A - B = \{x \mid x \in A \text{ e } x \notin B\}$$

Un caso particolare della differenza è il complementare, che si definisce quando si opera all'interno di un insieme "contenitore" fissato.

Definizione 0.5. Se $B \subseteq A$, si definisce **complementare** di B in A (o rispetto ad A) l'insieme:

$$B^c = \{x \mid x \in A \text{ e } x \notin B\} = A - B$$

Nota 1. Due insiemi si dicono **disgiunti** se non hanno elementi in comune, ovvero se la loro intersezione è l'insieme vuoto:

$$X \cap Y = \emptyset$$

Proprietà Distributive Analizziamo ora come le operazioni di unione e intersezione interagiscono tra loro. La prima proprietà fondamentale è la distributività dell'intersezione rispetto all'unione.

Proposizione 0.1. *Dati tre insiemi A, B, C, vale la seguente uguaglianza:*

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

Proof. Per dimostrare l'uguaglianza tra due insiemi, dobbiamo provare la doppia inclusione tra il membro di sinistra (che chiameremo 1) e quello di destra (che chiameremo 2).

1) ($\subseteq$) Proviamo che $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Sia $x \in A \cap (B \cup C)$. Per definizione, ciò significa che:

$$x \in A \quad \text{e} \quad x \in (B \cup C)$$

Poiché $x \in B \cup C$, si ha che $x \in B$ oppure $x \in C$.

- Se $x \in B$, essendo anche $x \in A$, allora $x \in A \cap B$.

- Se $x \in C$, essendo anche $x \in A$, allora $x \in A \cap C$.

In entrambi i casi, x appartiene all'unione dei due insiemi risultanti. Dunque $x \in (A \cap B) \cup (A \cap C)$.

2) ($\supseteq$) Proviamo che $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Sia $y \in (A \cap B) \cup (A \cap C)$. Per definizione di unione, si verifica almeno una delle seguenti condizioni:

- $y \in A \cap B \implies y \in A$ e $y \in B$.
- $y \in A \cap C \implies y \in A$ e $y \in C$.

In ogni caso, y deve necessariamente appartenere ad A. Inoltre, y appartiene a B oppure a C, il che implica che $y \in B \cup C$. Unendo le due informazioni ($y \in A$ e $y \in B \cup C$) otteniamo che $y \in A \cap (B \cup C)$.

Poiché valgono entrambe le inclusioni, l'uguaglianza è dimostrata. □

L'Insieme delle Parti Un concetto centrale nella teoria degli insiemi è quello dell'insieme potenza, ovvero l'insieme formato da tutti i possibili sottoinsiemi.

Definizione 0.6. Dato un insieme A, si definisce **insieme delle parti** (o insieme potenza) di A, indicato con $\mathcal{P}(A)$, l'insieme di tutti i sottoinsiemi di A:

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}$$

Esempio 0.2. Calcoliamo l'insieme delle parti per insiemi di cardinalità crescente per dedurne una legge generale.

Sia $A_2 = \{1, 2\}$. I suoi sottoinsiemi sono:

$$P(A_2) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Notiamo che $|A_2| = 2$ e la cardinalità dell'insieme delle parti è $|P(A_2)| = 4$.

Sia $A_3 = \{1, 2, 3\}$. I suoi sottoinsiemi sono:

$$P(A_3) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Qui $|A_3| = 3$ e $|P(A_3)| = 8$.

Osservando questi risultati, possiamo ipotizzare la formula generale:

$$|A_n| = n \implies |P(A_n)| = 2^n$$

Esempio di costruzione ricorsiva Proviamo a calcolare $|P(A_4)|$ sfruttando quanto sappiamo su $P(A_3)$. Sia $A_4 = \{1, 2, 3, 4\}$. Possiamo dividere i suoi sottoinsiemi in due gruppi disgiunti:

1. I sottoinsiemi che **non contengono** il 4: questi coincidono esattamente con $P(A_3)$.
2. I sottoinsiemi che **contengono** il 4: questi si ottengono prendendo ogni elemento di $P(A_3)$ e aggiungendoci il 4.

Poiché questi due gruppi sono disgiunti (uno ha il 4, l'altro no), la cardinalità totale è la somma delle parti:

$$|P(A_4)| = |P(A_3)| + |\{x \cup \{4\} \mid x \in P(A_3)\}|$$

Essendo i due gruppi in corrispondenza biunivoca, hanno la stessa cardinalità:

$$|P(A_4)| = |P(A_3)| + |P(A_3)| = 2 \cdot 8 = 16 = 2^4$$

Proprietà elementari Ricordiamo brevemente le proprietà algebriche di base.

Proposizione 0.2. *Valgono le seguenti proprietà:* ***Intersezione:***

1. $A \cap A = A$ *(Idempotenza)*
2. $A \cap B = B \cap A$ *(Commutativa)*
3. $(A \cap B) \cap C = A \cap (B \cap C)$ *(Associativa)*

Unione:

1. $A \cup A = A$ *(Idempotenza)*
2. $A \cup B = B \cup A$ *(Commutativa)*
3. $(A \cup B) \cup C = A \cup (B \cup C)$ *(Associativa)*

Seconda Proprietà Distributiva Esiste una simmetria perfetta tra le operazioni: anche l'unione è distributiva rispetto all'intersezione.

Proposizione 0.3.

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

Proof. Dimostriamo la doppia inclusione.
1) ($\subseteq$) Sia $x \in A \cup (B \cap C)$. Allora $x \in A$ oppure ($x \in B$ e $x \in C$).

- Se $x \in A$, allora $x \in A \cup B$ e $x \in A \cup C$. Dunque x sta nella loro intersezione.
- Se $x \in B \cap C$, allora $x \in B$ (quindi $x \in A \cup B$) e $x \in C$ (quindi $x \in A \cup C$). Anche in questo caso x sta nell'intersezione.

Quindi $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
2) ($\supseteq$) Sia $x \in (A \cup B) \cap (A \cup C)$. Ciò implica che $x \in A \cup B$ e contemporaneamente $x \in A \cup C$.

- Se $x \in A$, allora banalmente $x \in A \cup (B \cap C)$.
- Se $x \notin A$, affinché $x \in A \cup B$ sia vera, deve essere $x \in B$. Analogamente, affinché $x \in A \cup C$ sia vera, deve essere $x \in C$. Dunque, se $x \notin A$, allora $x \in B \cap C$, che implica $x \in A \cup (B \cap C)$.

In ogni caso la tesi è verificata. □

Leggi di De Morgan Le leggi di De Morgan collegano le operazioni insiemistiche con il concetto di complementare.

Teorema 0.4. *Dati due insiemi A, B sottoinsiemi di un universo X, valgono le seguenti uguaglianze:*

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

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

Forniamo la dimostrazione per la prima legge: $(A \cup B)^c = A^c \cap B^c$.

Proof. Dobbiamo dimostrare la doppia inclusione.
1) ($\subseteq$) Sia $x \in (A \cup B)^c$. Per definizione di complementare, questo significa che x appartiene all'universo X ma non appartiene all'unione $A \cup B$:

$$x \in X \quad \text{e} \quad x \notin (A \cup B)$$

Se x non appartiene all'unione, significa che non deve appartenere a nessuno dei due insiemi:

$$x \notin A \quad \text{e} \quad x \notin B$$

Essendo $x \in X$, possiamo riscrivere queste condizioni come:

$$x \in X - A = A^c \quad \text{e} \quad x \in X - B = B^c$$

Poiché x appartiene a entrambi i complementari, appartiene alla loro intersezione:

$$x \in A^c \cap B^c$$

2) ($\supseteq$) Sia ora $x \in A^c \cap B^c$. Questo implica che:

$$x \in A^c \implies x \in X \text{ e } x \notin A$$

$$x \in B^c \implies x \in X \text{ e } x \notin B$$

Quindi x è un elemento dell'universo che non sta in A e non sta in B. Di conseguenza, non può stare nella loro unione:

$$x \in X \text{ e } x \notin (A \cup B)$$

Questo coincide con la definizione di complemento dell'unione:

$$x \in X - (A \cup B) \implies x \in (A \cup B)^c$$

Le due inclusioni provano l'uguaglianza. □

Coppie Ordinate Fino ad ora abbiamo trattato insiemi in cui l'ordine degli elementi non conta (ad esempio $\{a, b\} = \{b, a\}$). Per introdurre il concetto di prodotto cartesiano, abbiamo bisogno di un oggetto in cui l'ordine sia rilevante: la coppia ordinata. Esiste una definizione insiemistica rigorosa, dovuta a Kuratowski, che definisce la coppia usando solo il concetto di insieme.

Definizione 0.7. La **coppia ordinata** di primo elemento a e secondo elemento b, indicata con (a, b), è definita come l'insieme:

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

Questa definizione è costruita appositamente per garantire la proprietà fondamentale delle coppie ordinate: due coppie sono uguali se e solo se sono ordinatamente uguali.

Proposizione 0.5.

$$(a, b) = (c, d) \iff a = c \ e \ b = d$$

Proof. Dimostriamo le due implicazioni.

1) ($\impliedby$) Condizione Sufficiente. Se $a = c$ e $b = d$, allora è banale che gli insiemi $\{\{a\}, \{a, b\}\}$ e $\{\{c\}, \{c, d\}\}$ siano identici, quindi $(a, b) = (c, d)$.

2) ($\implies$) Condizione Necessaria. Supponiamo che $(a, b) = (c, d)$. Dobbiamo distinguere due casi.

I Caso: $a = b$ Se gli elementi della prima coppia sono uguali, la definizione diventa:

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

L'insieme singoletto (che contiene solo un elemento). Per ipotesi $(a, b) = (c, d)$, quindi anche (c, d) deve essere uguale a $\{\{a\}\}$.

$$\{\{c\}, \{c, d\}\} = \{\{a\}\}$$

Affinché questi due insiemi siano uguali, i loro elementi devono coincidere. L'insieme a sinistra ha come elementi $\{c\}$ e $\{c, d\}$, mentre quello a destra ha solo $\{a\}$. Ne consegue che:

$$\{c\} = \{a\} \quad \text{e} \quad \{c, d\} = \{a\}$$

Dalla prima uguaglianza $c = a$. Sostituendo nella seconda, $\{a, d\} = \{a\}$, il che implica $d = a$. Quindi $a = b = c = d$, il che verifica la tesi.

II Caso: $a \neq b$ In questo caso, nella definizione $(a, b) = \{\{a\}, \{a, b\}\}$, l'insieme $\{a\}$ è diverso da $\{a, b\}$ (perché il secondo ha due elementi distinti). Dato che $(a, b) = (c, d)$, abbiamo:

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

L'elemento $\{a\}$ deve appartenere all'insieme di destra.

- Se $\{a\} = \{c, d\}$, allora $c = d = a$, ma questo implicherebbe che anche il primo insieme si riduce a un singoletto, contraddicendo l'ipotesi $a \neq b$.
- Quindi deve essere necessariamente $\{a\} = \{c\}$, da cui ricaviamo $a = c$.

Ora sappiamo che $\{a, b\}$ deve essere uguale al rimanente elemento di destra, ovvero $\{c, d\}$. Poiché $a = c$, abbiamo:

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

Dato che $a \neq b$, affinché gli insiemi siano uguali, deve essere necessariamente $b = d$. □

Prodotto Cartesiano Possiamo ora definire l'operazione che genera l'insieme di tutte le coppie possibili.

Definizione 0.8. Dati due insiemi A e B, si definisce **prodotto cartesiano** $A \times B$ l'insieme:

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

Esempio 0.3. Siano $A = \{x, y\}$ e $B = \{1, 2, 3\}$.

$$A \times B = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$$

Se invertiamo l'ordine:

$$B \times A = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$$

Notiamo chiaramente che $A \times B \neq B \times A$. Il prodotto cartesiano non è commutativo.

Cardinalità del prodotto cartesiano Quanti elementi ha l'insieme $A \times B$? Se $|A| = m$ e $|B| = n$, allora:

$$|A \times B| = |A| \cdot |B| = m \cdot n$$

Proof. Sia $A = \{a_1, \ldots, a_m\}$ e $B = \{b_1, \ldots, b_n\}$. Possiamo vedere $A \times B$ come l'unione di m insiemi disgiunti, dove fissiamo il primo elemento a_i e facciamo variare il secondo:

$$A \times B = \bigcup_{i=1}^{m} A_i \quad \text{dove} \quad A_i = \{(a_i, b_j) \mid b_j \in B\}$$

Ogni insieme A_i contiene esattamente tanti elementi quanti sono quelli di B (cioè n), perché a_i è fisso. Inoltre, gli insiemi A_i sono a due a due disgiunti (perché hanno un primo elemento diverso). Quindi la cardinalità totale è la somma delle cardinalità:

$$|A \times B| = \sum_{i=1}^{m} |A_i| = \sum_{i=1}^{m} n = \underbrace{n + n + \cdots + n}_{m \text{ volte}} = m \cdot n$$

□

Relazioni tra insiemi Il concetto di relazione formalizza l'idea di associazione tra elementi di due insiemi.

Definizione 0.9. Siano A, B due insiemi. Una **relazione** R tra A e B è un qualsiasi sottoinsieme del prodotto cartesiano:

$$R \subseteq A \times B$$

Se $(a, b) \in R$, diciamo che "a è in relazione con b" e scriviamo aRb.

Esempio 0.4. Riprendiamo $A = \{x, y\}$ e $B = \{1, 2, 3\}$. Ecco alcuni esempi di relazioni possibili (sottoinsiemi di $A \times B$):

- $R_1 = \{(x, 1), (x, 2), (y, 3)\}$
- $R_2 = \{(x, 1), (x, 3), (y, 1)\}$

- $R_3 = A \times B$ (Relazione totale: tutti sono in relazione con tutti)
- $R_4 = \{(x,1),(x,2),(x,3)\}$ (Solo x ha relazioni)

Possiamo rappresentare le relazioni con delle tabelle (matrici di incidenza), mettendo un simbolo (es. $\bullet$) dove c'è una relazione:

R_1	1	2	3
x	$\bullet$	$\bullet$	
y			$\bullet$

R_2	1	2	3
x	$\bullet$		$\bullet$
y	$\bullet$		

R_3	1	2	3
x	$\bullet$	$\bullet$	$\bullet$
y	$\bullet$	$\bullet$	$\bullet$

R_4	1	2	3
x	$\bullet$	$\bullet$	$\bullet$
y			

Relazione Trasposta (o Inversa) Data una relazione da A verso B, possiamo sempre definire la relazione inversa da B verso A.

Definizione 0.10. Data la relazione $R \subseteq A \times B$, si definisce la relazione **trasposta** $R^t \subseteq B \times A$ ponendo:

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

Esempio 0.5. Calcoliamo le trasposte delle relazioni viste nell'esempio precedente:

- $R_1^t = \{(1,x),(2,x),(3,y)\}$
- $R_2^t = \{(1,x),(3,x),(1,y)\}$
- $R_3^t = B \times A$
- $R_4^t = \{(1,x),(2,x),(3,x)\}$

Graficamente, se rappresentassimo R con delle frecce da A a B, R^t si otterrebbe semplicemente invertendo il verso di tutte le frecce.

Composizione di Relazioni È possibile combinare due relazioni in sequenza per ottenerne una terza, detta relazione composta.

Definizione 0.11. Date due relazioni $R \subseteq A \times B$ e $S \subseteq B \times C$, si definisce la relazione composta $S \circ R \subseteq A \times C$ ponendo:

$$(a,c) \in S \circ R \iff \exists b \in B : (a,b) \in R \text{ e } (b,c) \in S$$

In notazione infissa:

$$a(S \circ R)c \iff \exists b \in B \mid aRb \text{ e } bSc$$

L'idea intuitiva è che esiste un elemento "ponte" b nell'insieme intermedio B che collega a con c.

Esempio 0.6. Consideriamo i seguenti insiemi e relazioni:

$$A = \{x,y\}, \quad B = \{1,2,3\}, \quad C = \{\alpha,\beta,\gamma\}$$
$$R = \{(x,1),(x,2),(y,3)\} \subseteq A \times B$$
$$S = \{(1,\alpha),(1,\beta),(2,\gamma),(3,\alpha),(3,\beta)\} \subseteq B \times C$$

Calcoliamo $S \circ R$:

- Per x:
  - $x \xrightarrow{R} 1 \xrightarrow{S} \alpha,\beta \implies (x,\alpha),(x,\beta) \in S \circ R$
  - $x \xrightarrow{R} 2 \xrightarrow{S} \gamma \implies (x,\gamma) \in S \circ R$
- Per y:
  - $y \xrightarrow{R} 3 \xrightarrow{S} \alpha,\beta \implies (y,\alpha),(y,\beta) \in S \circ R$

Quindi:

$$S \circ R = \{(x,\alpha),(x,\beta),(x,\gamma),(y,\alpha),(y,\beta)\}$$

Teorema della Trasposta della Composizione Una proprietà fondamentale lega l'operazione di composizione con quella di trasposizione (inversa).

Teorema 0.6. *Date $R \subseteq A \times B$ e $S \subseteq B \times C$, vale l'uguaglianza:*

$$(S \circ R)^t = R^t \circ S^t$$

Nota bene: l'ordine delle relazioni si inverte.

Analisi Preliminare Prima di procedere con la dimostrazione formale, verifichiamo che i domini e codomini siano coerenti. Sappiamo che $S \circ R \subseteq A \times C$, quindi la sua trasposta $(S \circ R)^t$ sarà un sottoinsieme di $C \times A$. Dall'altra parte:

- $S^t \subseteq C \times B$
- $R^t \subseteq B \times A$

Quindi la composizione $R^t \circ S^t$ (prima applico S^t poi R^t) è ben definita ed è anch'essa un sottoinsieme di $C \times A$. I domini coincidono. Ora dobbiamo dimostrare l'uguaglianza degli insiemi tramite la doppia inclusione.

Proof. Dobbiamo dimostrare due inclusioni: 1) $R^t \circ S^t \subseteq (S \circ R)^t$ 2) $(S \circ R)^t \subseteq R^t \circ S^t$

1) Dimostrazione che $R^t \circ S^t \subseteq (S \circ R)^t$ Siano $c \in C$ e $a \in A$ tali che $(c, a) \in R^t \circ S^t$. Per definizione di composizione, esiste un elemento intermedio $b \in B$ tale che:

$$(c, b) \in S^t \quad \text{e} \quad (b, a) \in R^t$$

Per definizione di relazione trasposta, questo implica che:

$$(b, c) \in S \quad \text{e} \quad (a, b) \in R$$

Possiamo riordinare queste affermazioni come: esiste $b \in B$ tale che $(a, b) \in R$ e $(b, c) \in S$. Questa è esattamente la definizione di composizione: $(a, c) \in S \circ R$. Infine, trasponendo nuovamente il risultato, otteniamo:

$$(c, a) \in (S \circ R)^t$$

Quindi la prima inclusione è verificata.

2) Dimostrazione che $(S \circ R)^t \subseteq R^t \circ S^t$ Sia $(c, a) \in (S \circ R)^t$. Per definizione di trasposta, ciò significa che $(a, c) \in S \circ R$. Per definizione di composizione, esiste $b \in B$ tale che:

$$(a, b) \in R \quad \text{e} \quad (b, c) \in S$$

Applicando la definizione di trasposta a queste singole relazioni:

$$(b, a) \in R^t \quad \text{e} \quad (c, b) \in S^t$$

Abbiamo quindi trovato un elemento b tale che $(c, b) \in S^t$ e $(b, a) \in R^t$. Questa è la definizione di composizione $R^t \circ S^t$:

$$(c, a) \in R^t \circ S^t$$

Anche la seconda inclusione è verificata.

Poiché valgono entrambe le inclusioni, l'uguaglianza è dimostrata. □

Nota 2. Vale anche la proprietà di involuzione della trasposta:

$$R^{tt} = R$$

Infatti: $(a, b) \in R^{tt} \iff (b, a) \in R^t \iff (a, b) \in R$.

Classificazione delle Relazioni Le relazioni binarie possono essere classificate in base alle loro proprietà e al dominio/codominio. In particolare, quando $A = B$ (ovvero $R \subseteq A \times A$), parliamo di **relazione in un insieme**. Queste si dividono principalmente in:

- **Relazioni di Equivalenza** (riflessiva, simmetrica, transitiva)
- **Relazioni d'Ordine** (riflessiva, antisimmetrica, transitiva)

Un altro tipo fondamentale di relazione, che può essere tra insiemi diversi, è l'**applicazione** (o **funzione**), che è una corrispondenza univoca tra elementi del dominio e del codominio.

Definizione di Funzione Tra tutte le possibili relazioni tra due insiemi, ne esiste una tipologia di fondamentale importanza: le funzioni (chiamate anche applicazioni o corrispondenze univoche).

Definizione 0.12. Una relazione $f \subseteq A \times B$ si dice **funzione** (o corrispondenza) tra A e B se e solo se per ogni elemento del dominio esiste uno ed un solo elemento del codominio ad esso associato. In simboli:

$$\forall a \in A, \exists! b \in B \mid (a, b) \in f$$

In tal caso, l'elemento b si chiama **immagine** di a mediante f e si utilizza la notazione funzionale $b = f(a)$.

Analisi degli esempi precedenti Riprendiamo le relazioni trasposte R^t esaminate nel paragrafo precedente per verificare quali di esse siano funzioni. Ricordiamo che per essere una funzione, ogni elemento del primo insieme deve avere un'unica freccia in uscita.

Esempio 0.7. Analizziamo i casi:

- $R_1^t = \{(1, x), (2, x), (3, y)\}$: Ogni elemento di $\{1, 2, 3\}$ ha un'immagine unica. **È una funzione**.
- $R_4^t = \{(1, x), (2, x), (3, x)\}$: Anche qui, ogni elemento ha un'unica immagine (tutti vanno in x, che è lecito). **È una funzione** (costante).
- $R_2^t = \{(1, 1), (3, x)\}$: Qui c'è un problema di dominio (se il dominio era $\{1, 2, 3\}$, il 2 non ha immagine) o di codominio (la coppia $(1, 1)$ non ha senso se il secondo insieme è $A = \{x, y\}$). Se consideriamo l'esempio originale inverso $R_2 = \{(x, 1), (x, 3), (y, 1)\}$, la sua trasposta ha $(1, x)$ e $(1, y)$. L'elemento 1 avrebbe due immagini distinte. **Non è una funzione**.
- $R_3^t = B \times A$: Ogni elemento di B è collegato a tutti gli elementi di A. L'unicità non è rispettata. **Non è una funzione**.

Invertibilità di una funzione Quando la relazione inversa (o trasposta) di una funzione è anch'essa una funzione? Data una funzione $f \subseteq A \times B$, la sua trasposta $f^t \subseteq B \times A$ è una funzione se e solo se:

$$\forall y \in B, \exists! x \in A : (y, x) \in f^t \iff (x, y) \in f \iff y = f(x)$$

Questo ci porta direttamente alla definizione di biettività.

Definizione 0.13. Una funzione $f : A \to B$ si dice **biettiva** (o biunivoca) se per ogni elemento del codominio B esiste uno ed un solo elemento del dominio A da cui proviene.

$$\forall y \in B, \exists! x \in A : y = f(x)$$

Per comprendere meglio questo concetto, è utile scomporlo in due proprietà distinte: l'iniettività e la suriettività.

Definizione 0.14. Sia $f : A \to B$ una funzione. Diciamo che f è:

- **Suriettiva**: se ogni elemento del codominio è raggiunto da *almeno un* elemento del dominio.

$$\forall y \in B, \exists x \in A : y = f(x)$$

- **Iniettiva**: se ogni elemento del codominio è raggiunto da *al più un* elemento del dominio (ovvero,

elementi distinti del dominio vanno in elementi distinti del codominio).

$$\forall y \in B, \exists \text{ al più un } x \in A : y = f(x)$$

Equivalentemente: $f(x_1) = f(x_2) \implies x_1 = x_2$.

Nota 3. Vale la seguente equivalenza fondamentale:

$$f \text{ è biettiva} \iff f \text{ è iniettiva e suriettiva}$$

Solo se una funzione è biettiva, la sua relazione inversa è una funzione (detta funzione inversa, f^{-1}).

Esempi di verifica dell'invertibilità Vediamo come determinare se una funzione reale di variabile reale è biettiva risolvendo l'equazione $y = f(x)$ rispetto a x.

Esempio 0.8. Consideriamo la funzione lineare:

$$f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 2x + 1$$

Possiamo scrivere l'insieme come $f = \{(x, 2x + 1) \mid x \in \mathbb{R}\}$. Per verificare se è biettiva, ci chiediamo: fissato un qualsiasi $y \in \mathbb{R}$ (parametro), esiste ed è unico l'x (incognita) tale che $y = f(x)$?

Impostiamo l'equazione:

$$y = 2x + 1$$

Isoliamo la x:

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

Poiché per ogni $y \in \mathbb{R}$ l'espressione $\frac{y-1}{2}$ restituisce un unico valore reale ben definito, l'equazione ammette una e una sola soluzione. Dunque f è biettiva.

Possiamo quindi definire la funzione inversa (che corrisponde alla relazione trasposta f^t):

$$f^t : \mathbb{R} \to \mathbb{R}, \quad y \mapsto \frac{y - 1}{2}$$

Esempio 0.9. Consideriamo ora la funzione esponenziale:

$$f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 2^x$$

Verifichiamo la biettività ponendo $y = 2^x$ con $y \in \mathbb{R}$.

Questa equazione non ha sempre soluzione. Sappiamo infatti che l'esponenziale è sempre strettamente positivo ($2^x > 0$).

- Se scegliamo un $y \leq 0$ (ad esempio $y = -5$), non esiste nessun x tale che $2^x = -5$.

Mancando la condizione "per ogni y", la funzione non è suriettiva, e di conseguenza non è biettiva.

Pertanto, la relazione inversa f^t non è una funzione da $\mathbb{R}$ in $\mathbb{R}$, poiché gli elementi negativi o nulli del dominio non avrebbero immagine.

Tuttavia, se $y > 0$, la soluzione esiste ed è unica: $x = \log_2 y$. Questo ci dice che la funzione è iniettiva. La relazione inversa sarebbe:

$$f^t = \{(y, \log_2 y) \mid y \in \mathbb{R}, y > 0\}$$

Questa è una funzione solo se restringiamo il dominio ai reali positivi.

Immagine di un Insieme Estendiamo il concetto di applicazione ai sottoinsiemi del dominio.

Definizione 0.15. Sia $f : X \to Y$ una funzione e sia $A \subseteq X$ un sottoinsieme del dominio. Si definisce **immagine** di A mediante f l'insieme:

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

Nota 4. Questa definizione ci permette di riformulare la suriettività in termini insiemistici: Una funzione $f : X \to Y$ è suriettiva se e solo se l'immagine dell'intero dominio coincide con il codominio, ovvero $f(X) = Y$.

Esempio 0.10. Consideriamo la funzione lineare $f : \mathbb{R} \to \mathbb{R}$ definita da $f(x) = 2x + 1$. Vogliamo determinare l'immagine dell'intervallo $A = [0, 1]$. Intuitivamente ci aspettiamo che sia l'intervallo $[1, 3]$. Dimostriamolo rigorosamente provando la doppia inclusione $f(A) = [1, 3]$.

1) Inclusione diretta: $f(A) \subseteq [1, 3]$ Sia $y \in f(A)$. Per definizione, esiste un $x \in A$ tale che $y = f(x)$. Poiché $x \in [0, 1]$, abbiamo:

$$0 \leq x \leq 1$$

Moltiplichiamo per 2 (mantenendo il verso della disuguaglianza):

$$0 \leq 2x \leq 2$$

Aggiungiamo 1:

$$1 \leq 2x + 1 \leq 3$$

Poiché $y = 2x + 1$, abbiamo $1 \leq y \leq 3$, ovvero $y \in [1, 3]$.

2) Inclusione inversa: $[1, 3] \subseteq f(A)$ Sia $y \in [1, 3]$. Dobbiamo mostrare che esiste un $x \in A$ tale che $f(x) = y$. Risolviamo l'equazione $y = 2x + 1$ rispetto a x:

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

Dobbiamo verificare che questo x appartenga effettivamente ad $A = [0, 1]$. Poiché $1 \leq y \leq 3$, sottraendo 1 otteniamo $0 \leq y - 1 \leq 2$. Dividendo per 2 otteniamo:

$$0 \leq \frac{y - 1}{2} \leq 1$$

Quindi $0 \leq x \leq 1$, cioè $x \in A$. Abbiamo dimostrato che ogni $y \in [1, 3]$ è immagine di un punto di A.

Esempi di Studio di Biettività Analizziamo ora alcune funzioni definite a tratti o razionali per determinarne l'invertibilità.

Esempio 0.11. Sia $f : \mathbb{R} \to \mathbb{R}$ definita da:

$$f(x) = \begin{cases} x^2 & x \geq 0 \\ x & x < 0 \end{cases}$$

Per verificare se è biettiva, studiamo l'equazione parametrica $y = f(x)$ al variare di $y \in \mathbb{R}$.

Caso $y < 0$ Se il valore atteso y è negativo, non può provenire dal ramo x^2 (che è sempre non negativo). Deve provenire dal ramo x (con $x < 0$). L'equazione diventa $y = x$. Dato che $y < 0$, la soluzione $x = y$ rispetta la condizione $x < 0$. C'è una sola soluzione.

Caso $y \geq 0$ Se y è non negativo, deve provenire dal ramo x^2 (poiché il ramo x darebbe valori negativi). L'equazione è $y = x^2$ con condizione $x \geq 0$. Le soluzioni algebriche sarebbero $x = \pm\sqrt{y}$, ma la condizione $x \geq 0$ ci obbliga a scartare $-\sqrt{y}$. Rimane l'unica soluzione $x = \sqrt{y}$.

In entrambi i casi, per ogni y esiste un'unica x. La funzione è biettiva. La funzione inversa f^t (o f^{-1}) è:

$$f^{-1}(y) = \begin{cases} y & y < 0 \\ \sqrt{y} & y \geq 0 \end{cases}$$

Esempio 0.12. Sia $f : \mathbb{R} \to \mathbb{R}$ definita da:

$$f(x) = \begin{cases} x + \frac{x+1}{x-1} & x \neq 1 \\ 0 & x = 1 \end{cases}$$

Ci chiediamo se è biettiva. Iniziamo controllando l'unicità della controimmagine per $y = 0$. Sappiamo per definizione che $f(1) = 0$. Esistono altri x tali che $f(x) = 0$? Se $x \neq 1$, poniamo:

$$0 = x + \frac{x + 1}{x - 1}$$

Moltiplicando per $(x-1)$:

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

L'equazione $x^2 = -1$ non ha soluzioni reali. Quindi l'unica controimmagine di 0 è 1. Fin qui l'iniettività regge.

Studiamo ora il caso generale $y = f(x)$ per $x \neq 1$.

$$y = x + \frac{x+1}{x-1} \implies y(x-1) = x(x-1) + x + 1$$

Svolgendo i calcoli arriviamo all'equazione di secondo grado in x:

$$x^2 - xy + (y+1) = 0$$

Risolviamo rispetto a x usando la formula ridotta/classica:

$$x = \frac{y \pm \sqrt{y^2 - 4(y+1)}}{2} = \frac{y \pm \sqrt{y^2 - 4y - 4}}{2}$$

Affinché esistano soluzioni reali, il discriminante deve essere non negativo:

$$\Delta = y^2 - 4y - 4 \geq 0$$

Le radici dell'equazione associata sono $y = 2 \pm 2\sqrt{2}$. Il discriminante è positivo (quindi esistono x) solo per valori "esterni":

$$y \leq 2 - 2\sqrt{2} \quad \vee \quad y \geq 2 + 2\sqrt{2}$$

Questo ha due conseguenze disastrose per la biettività: 1. **Non suriettiva**: Per tutti i valori di y nell'intervallo $(2 - 2\sqrt{2}, 2 + 2\sqrt{2})$ (eccetto forse lo 0 che abbiamo trattato a parte), non esiste alcuna x. 2. **Non iniettiva**: Dove il discriminante è strettamente positivo, esistono due soluzioni distinte ($x_1 \neq x_2$) per lo stesso y.

Conclusione: f non è né iniettiva né suriettiva, quindi non è biettiva.

Proprietà Associativa della Composizione Un risultato teorico fondamentale riguarda l'associatività dell'operazione di composizione, sia per le relazioni generali che per le funzioni.

Proposizione 0.7. *Date tre relazioni $F \subseteq A \times B$, $G \subseteq B \times C$, $H \subseteq C \times D$, vale la proprietà associativa:*

$$(H \circ G) \circ F = H \circ (G \circ F)$$

Proof. Dimostriamo la doppia inclusione. **1)** ($\subseteq$) Sia $(a,d) \in (H \circ G) \circ F$. Esiste un elemento intermedio $b \in B$ tale che $(a,b) \in F$ e $(b,d) \in H \circ G$. A sua volta, poiché $(b,d) \in H \circ G$, esiste $c \in C$ tale che $(b,c) \in G$ e $(c,d) \in H$. Raggruppando diversamente: abbiamo $(a,b) \in F$ e $(b,c) \in G$, quindi $(a,c) \in G \circ F$. Inoltre sappiamo che $(c,d) \in H$. Dunque $(a,d) \in H \circ (G \circ F)$.

2) ($\supseteq$) Sia $(\alpha,\delta) \in H \circ (G \circ F)$. Esiste $\gamma \in C$ tale che $(\alpha,\gamma) \in G \circ F$ e $(\gamma,\delta) \in H$. Da $(\alpha,\gamma) \in G \circ F$ segue che esiste $\beta \in B$ tale che $(\alpha,\beta) \in F$ e $(\beta,\gamma) \in G$. Ora consideriamo $(\beta,\gamma) \in G$ e $(\gamma,\delta) \in H$: questo implica $(\beta,\delta) \in H \circ G$. Infine, avendo $(\alpha,\beta) \in F$ e $(\beta,\delta) \in H \circ G$, concludiamo che $(\alpha,\delta) \in (H \circ G) \circ F$. □

Proposizione 0.8. *La proprietà associativa vale in particolare per le applicazioni. Se $f : A \to B, g : B \to C, h : C \to D$ sono funzioni, allora:*

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Proof. Per le funzioni, l'uguaglianza si dimostra semplicemente verificando che le immagini coincidano per ogni elemento del dominio. Sia $a \in A$. Calcoliamo il membro sinistro:

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$

Calcoliamo il membro destro:

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$$

Le espressioni sono identiche per ogni a, dunque le funzioni composte sono uguali. □

Esempio 0.13. Verifichiamo l'associatività con tre funzioni specifiche:

$$f(x) = 2x + 1, \quad g(x) = |x|, \quad h(x) = \sqrt{x}$$

Composizione a sinistra $(h \circ g) \circ f$: 1. Prima calcoliamo $h \circ g$: $x \mapsto |x| \mapsto \sqrt{|x|}$. 2. Poi componiamo con f: $x \mapsto 2x + 1 \xrightarrow{h \circ g} \sqrt{|2x + 1|}$.

Composizione a destra $h \circ (g \circ f)$: 1. Prima calcoliamo $g \circ f$: $x \mapsto 2x + 1 \mapsto |2x + 1|$. 2. Poi applichiamo h al risultato: $y \mapsto \sqrt{y} \implies \sqrt{|2x + 1|}$.

Il risultato finale è lo stesso, cambia solo l'ordine dei passaggi intermedi.

Proprietà della Composizione di Funzioni La composizione di funzioni preserva le proprietà fondamentali delle funzioni componenti? Analizziamo come si comportano suriettività, iniettività e biettività.

Proposizione 0.9. *Date due applicazioni $f : A \to B$ e $g : B \to C$, consideriamo l'applicazione composta $g \circ f : A \to C$. Valgono le seguenti proprietà:*

1. *Se f e g sono suriettive, allora $g \circ f$ è suriettiva.*
2. *Se f e g sono iniettive, allora $g \circ f$ è iniettiva.*
3. *Se f e g sono biettive, allora $g \circ f$ è biettiva.*

Proof. Dimostriamo le tre affermazioni separatamente.

1) Suriettività Dobbiamo provare che ogni elemento del codominio finale C è raggiunto da almeno un elemento del dominio iniziale A. Ovvero: $\forall c \in C, \exists a \in A : c = (g \circ f)(a)$.

- Per ipotesi g è suriettiva, quindi $\forall c \in C, \exists b \in B : c = g(b)$.
- Per ipotesi f è suriettiva, quindi per quel $b \in B$, $\exists a \in A : b = f(a)$.

Sostituendo: $c = g(b) = g(f(a)) = (g \circ f)(a)$. Dunque $g \circ f$ è suriettiva.

2) Iniettività Ricordiamo che una funzione è iniettiva se trasforma argomenti diversi in immagini diverse, o equivalentemente: se le immagini sono uguali, allora gli argomenti di partenza devono essere uguali ($f(x_1) = f(x_2) \implies x_1 = x_2$). Siano $a_1, a_2 \in A$ tali che $(g \circ f)(a_1) = (g \circ f)(a_2)$.

$$g(f(a_1)) = g(f(a_2))$$

- Poiché g è iniettiva, $g(y_1) = g(y_2) \implies y_1 = y_2$. Applicandolo qui (con $y = f(a)$), otteniamo $f(a_1) = f(a_2)$.
- Poiché anche f è iniettiva, $f(a_1) = f(a_2) \implies a_1 = a_2$.

Abbiamo dimostrato che $a_1 = a_2$, quindi $g \circ f$ è iniettiva.

3) Biettività Se f e g sono biettive, sono per definizione sia iniettive che suriettive. Per i punti (1) e (2), la loro composizione $g \circ f$ sarà sia suriettiva che iniettiva. Di conseguenza, $g \circ f$ è biettiva. □

L'Applicazione Identica Esiste una funzione "neutra" che non modifica gli elementi su cui agisce.

Definizione 0.16. Dato un insieme non vuoto $A \neq \emptyset$, si definisce **applicazione identica** su A la funzione:

$$id_A : A \to A, \quad x \mapsto x$$

In termini di relazione (sottoinsieme di $A \times A$), essa coincide con la diagonale:

$$id_A = \{(x, x) \mid x \in A\} \subseteq A \times A$$

Questa applicazione agisce come elemento neutro rispetto all'operazione di composizione.

Proposizione 0.10. *Sia $f : A \to B$ una funzione qualsiasi. Allora:*

1. $id_B \circ f = f$ *(Elemento neutro a sinistra)*
2. $f \circ id_A = f$ *(Elemento neutro a destra)*

Proof. Verifichiamo semplicemente l'azione sui singoli elementi. **1)** Per ogni $a \in A$:

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

Poiché l'immagine è la stessa per ogni elemento, le funzioni coincidono.

2) Per ogni $a \in A$:

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

Anche qui le funzioni coincidono. □

Calcolo Combinatorio delle Applicazioni Nel caso di insiemi finiti, possiamo contare esattamente quante funzioni esistono tra due insiemi. Siano $|A| = m$ e $|B| = n$, con $A = \{a_1, \dots, a_m\}$.

Per definire una funzione $f : A \to B$, dobbiamo scegliere un'immagine per ciascuno degli m elementi di A. Possiamo rappresentare la funzione con una matrice a due righe:

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_m \\ f(a_1) & f(a_2) & \dots & f(a_m) \end{pmatrix}$$

Esempio 0.14. Sia $A = \{x, y\}$ ($m = 2$) e $B = \{1, 2, 3\}$ ($n = 3$). Una possibile funzione è quella che manda tutto in 1:

$$f = \begin{pmatrix} x & y \\ 1 & 1 \end{pmatrix}$$

Per costruire una generica funzione:

- Per $f(x)$ ho 3 scelte possibili (1, 2 o 3).
- Per $f(y)$ ho 3 scelte possibili.

In totale ho $3 \times 3 = 9$ funzioni possibili.

Proposizione 0.11. *Il numero totale di applicazioni da A a B è dato da $|B|^{|A|} = n^m$. L'insieme di tutte le funzioni da A a B si indica spesso con la notazione esponenziale B^A.*

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

Nota 5. Confrontiamo questo numero con il numero totale di *relazioni* tra A e B. Le relazioni sono i sottoinsiemi del prodotto cartesiano $A \times B$. Poiché $|A \times B| = m \cdot n$, l'insieme delle parti $\mathcal{P}(A \times B)$ ha cardinalità:

$$2^{|A \times B|} = 2^{mn}$$

Questo numero è molto più grande di n^m.

Permutazioni (Applicazioni Biettive su se stesso) Consideriamo ora le funzioni biettive da un insieme A in se stesso ($f : A \to A$), dette anche **permutazioni**. L'insieme di tali funzioni si indica con $S(A)$ (Gruppo Simmetrico).

Se $|A| = n$, quante sono queste funzioni? Per il primo elemento a_1 ho n scelte possibili. Per il secondo a_2, non posso scegliere l'immagine già usata per a_1 (per l'iniettività), quindi ho $n - 1$ scelte. Per l'ennesimo elemento, mi rimarrà 1 sola scelta.

$$|S(A)| = n \cdot (n-1) \cdot \dots \cdot 1 = n!$$

Introduzione alle Strutture Algebriche L'algebra astratta studia gli insiemi dotati di una o più operazioni.

Definizione 0.17. Dato un insieme non vuoto X, un'(interna) è un'applicazione che associa a ogni coppia di elementi di X un terzo elemento di X:

$$\omega : X \times X \to X, \quad (a, b) \mapsto a\omega b$$

Simboli comuni: $+, \cdot, *, \circ, \Delta$.

Esempi di Strutture 1. Composizione di funzioni: Sia $M(A) = A^A$ l'insieme delle funzioni da A in A. L'operazione di composizione $\circ$ è un'operazione binaria su $M(A)$.

$$(f, g) \mapsto f \circ g$$

La struttura $(M(A), \circ)$ è un monoide (associativa, con elemento neutro id_A).

2. Operazioni insiemistiche: Sia $\mathcal{P}(A)$ l'insieme delle parti di A. Possiamo definire diverse operazioni binarie su $\mathcal{P}(A)$:

- Intersezione $\cap$: $(X, Y) \mapsto X \cap Y$. È commutativa e associativa.
- Unione $\cup$: $(X, Y) \mapsto X \cup Y$. È commutativa e associativa.
- Differenza $-$: $(X, Y) \mapsto X - Y$.

Esempio 0.15. Analizziamo la differenza insiemistica per un insieme $A = \{a, b\}$ (quindi $\mathcal{P}(A)$ ha 4 elementi: $\emptyset, \{a\}, \{b\}, \{a, b\}$).

$-$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$
$\{b\}$	$\{b\}$	$\{b\}$	$\emptyset$	$\emptyset$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	$\emptyset$

Dalla tabella notiamo subito che l'operazione non è commutativa:

$$\{a\} - \{b\} = \{a\} \quad \text{ma} \quad \{b\} - \{a\} = \{b\}$$

Inoltre non è associativa.

Proprietà fondamentali delle operazioni Quando studiamo una struttura algebrica (S, ω), dove S è un insieme e ω un'operazione binaria, ci interessano particolarmente alcune proprietà che l'operazione può soddisfare.

Definizione 0.18. Sia (S, ω) una struttura algebrica.

- L'operazione ω si dice **commutativa** se:

$$a\omega b = b\omega a \quad \forall a, b \in S$$

- L'operazione ω si dice **associativa** se:

$$a\omega(b\omega c) = (a\omega b)\omega c \quad \forall a, b, c \in S$$

Elemento Neutro Un concetto centrale è quello di un elemento che "non fa nulla" quando operato con altri.

Definizione 0.19. Diciamo che $e \in S$ è un **elemento neutro** per (S, ω) se:

$$e\omega x = x = x\omega e \quad \forall x \in S$$

Nota 6. La notazione per l'elemento neutro cambia a seconda del contesto:

- In notazione moltiplicativa (uso di $\cdot, *, \circ$), si indica solitamente con 1_S.
- In notazione additiva (uso di $+$), si indica solitamente con 0_S.

Proposizione 0.12. *Se in una struttura (S, ω) esiste un elemento neutro, esso è unico.*

Proof. Supponiamo per assurdo che esistano due elementi neutri distinti, e_1 ed e_2. Poiché e_1 è neutro, per ogni x vale $x\omega e_1 = x$. Applicando questa proprietà con $x = e_2$, otteniamo:

$$e_2 \omega e_1 = e_2$$

Poiché e_2 è neutro, per ogni x vale $e_2 \omega x = x$. Applicando questa proprietà con $x = e_1$, otteniamo:

$$e_2 \omega e_1 = e_1$$

Confrontando le due uguaglianze, si ha necessariamente $e_1 = e_2$. □

Esempi di Elementi Neutri Ecco una tabella riassuntiva di alcune strutture note e dei loro elementi neutri (se esistono).

Insieme	Operazione	Elemento Neutro
$\mathbb{R}$ (Reali)	$+$ (Somma)	0
$\mathbb{Q}$ (Razionali)	$\cdot$ (Prodotto)	1
$\mathcal{P}(X)$ (Parti di X)	$\cap$ (Intersezione)	X
$\mathcal{P}(X)$ (Parti di X)	$\cup$ (Unione)	$\emptyset$
$\mathcal{P}(X)$ (Parti di X)	$-$ (Differenza)	$\emptyset$ (solo a destra: $A - \emptyset = A$)
$M(X)$ (Funzioni su X)	$\circ$ (Composizione)	id_X (Identità)
$S(X)$ (Permutazioni)	$\circ$ (Composizione)	id_X (Identità)

Elementi Invertibili In una struttura dotata di elemento neutro, possiamo chiederci se è possibile "tornare indietro" dopo aver applicato un'operazione.

Definizione 0.20. Sia (S, ω) una struttura con elemento neutro 1_S (usiamo la notazione moltiplicativa per generalità). Un elemento $a \in S$ si dice **invertibile** se esiste un elemento $b \in S$ tale che:

$$a\omega b = 1_S = b\omega a$$

In tal caso, b si chiama **inverso** di a.

Si noti la simmetria della definizione: se b è l'inverso di a, allora anche a è l'inverso di b.

Proposizione 0.13. *In un monoide associativo, se un elemento a è invertibile, il suo inverso è unico.*

Proof. Siano b_1 e b_2 due inversi di a. Per definizione:

$$a\omega b_1 = 1_S \quad \text{e} \quad b_2 \omega a = 1_S$$

Sfruttando l'associatività, calcoliamo il prodotto $b_2 \omega a \omega b_1$ in due modi:

$$b_2 \omega (a \omega b_1) = b_2 \omega 1_S = b_2$$

$$(b_2 \omega a) \omega b_1 = 1_S \omega b_1 = b_1$$

Ne consegue che $b_1 = b_2$. □

Nota 7. La notazione per l'inverso dipende dall'operazione:

- Moltiplicativa: a^{-1} (si legge "a alla meno uno" o "inverso di a"). Vale $(a^{-1})^{-1} = a$.
- Additiva: $-a$ (si legge "meno a" o "opposto di a"). Vale $-(-a) = a$.

Classificazione delle Strutture Algebriche Possiamo ora classificare le strutture (S, ω) in base alle proprietà che soddisfano.

Definizione 0.21. Una struttura (S, ω) si dice:

- **Semigruppo**: se l'operazione è associativa.

$$\forall a, b, c \in S, \quad a\omega(b\omega c) = (a\omega b)\omega c$$

- **Monoide**: se è un semigruppo dotato di elemento neutro.

$$\exists 1_S \in S : \forall x \in S, \quad 1_S \omega x = x = x\omega 1_S$$

- **Gruppo**: se è un monoide in cui ogni elemento è invertibile.

$$\forall a \in S, \exists a^{-1} \in S : a\omega a^{-1} = 1_S = a^{-1}\omega a$$

Se l'operazione è anche commutativa, si parla di Semigruppo/Monoide/Gruppo Commutativo (o Abeliano nel caso dei gruppi).

Proprietà dell'inverso nel prodotto Nei gruppi (o monoidi), l'inverso di un prodotto non è semplicemente il prodotto degli inversi, ma il prodotto degli inversi in ordine scambiato.

Proposizione 0.14. *Siano a, b due elementi invertibili di un monoide $(S, *)$. Allora anche il loro prodotto $a * b$ è invertibile e il suo inverso è dato da:*

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

Proof. Per dimostrare che $y = b^{-1} * a^{-1}$ è l'inverso di $x = a * b$, dobbiamo verificare che $x * y = 1_S$ e $y * x = 1_S$.

1) Verifica a destra:

$$(a * b) * (b^{-1} * a^{-1})$$

Usando l'associatività:

$$= a * (b * b^{-1}) * a^{-1}$$

Poiché $b * b^{-1} = 1_S$:

$$= a * 1_S * a^{-1} = a * a^{-1} = 1_S$$

2) Verifica a sinistra:

$$(b^{-1} * a^{-1}) * (a * b)$$

Usando l'associatività:

$$= b^{-1} * (a^{-1} * a) * b$$

Poiché $a^{-1} * a = 1_S$:

$$= b^{-1} * 1_S * b = b^{-1} * b = 1_S$$

La tesi è dimostrata. □

Il Gruppo degli Elementi Invertibili $U(S)$ Dato un monoide (S, ω), non è detto che tutti i suoi elementi siano invertibili. Possiamo però sempre considerare il sottoinsieme formato da quelli che lo sono.

Definizione 0.22. Sia (S, ω) un monoide. Definiamo $U(S)$ come l'insieme degli elementi invertibili di S:

$$U(S) = \{a \in S \mid a \text{ è invertibile}\}$$

Nota 8. $U(S)$ non è mai vuoto perché l'elemento neutro 1_S è sempre invertibile (il suo inverso è se stesso: $1_S \omega 1_S = 1_S$).

Proposizione 0.15. *L'insieme $U(S)$ è chiuso rispetto all'operazione e all'inversione:*

1. *Se $a, b \in U(S)$, allora anche il loro prodotto $a\omega b$ è in $U(S)$. L'inverso del prodotto è dato da $(a\omega b)^{-1} = b^{-1}\omega a^{-1}$.*
2. *Se $a \in U(S)$, allora anche il suo inverso a^{-1} è in $U(S)$. L'inverso dell'inverso è l'elemento stesso: $(a^{-1})^{-1} = a$.*

In notazione additiva, queste proprietà diventano: $-(a+b) = (-b) + (-a)$ e $-(-a) = a$.

La proprietà di chiusura ci porta a un risultato strutturale molto importante:

Proposizione 0.16. *Se $(S, *)$ è un monoide, allora la struttura $(U(S), *)$ è un **Gruppo**.*

Proof. Verifichiamo le proprietà di gruppo per $(U(S), *)$: 1. Operazione ben definita: L'operazione ristretta a $U(S) \times U(S)$ restituisce un elemento di $U(S)$ (per la proposizione precedente). 2. Associatività: È ereditata direttamente dal monoide S. 3. Elemento neutro: $1_S \in U(S)$ e funge da neutro anche in $U(S)$. 4. Inverso: Per ogni $a \in U(S)$, il suo inverso a^{-1} esiste (in S) e appartiene a $U(S)$. Quindi ogni monoide contiene al suo interno un gruppo. □

Esempi di Gruppi degli Invertibili Analizziamo $U(S)$ per diverse strutture numeriche e insiemistiche.

Insieme	**Operazione**	**Elemento Neutro**	**Gruppo Invertibili** $U(S)$
$\mathbb{N}$	$+$	0	$\{0\}$ (Solo lo zero ha opposto in $\mathbb{N}$)
$\mathbb{N}$	$\cdot$	1	$\{1\}$ (Solo 1 ha inverso intero)
$\mathbb{Z}$	$+$	0	$\mathbb{Z}$ (È già un gruppo!)
$\mathbb{Z}$	$\cdot$	1	$\{\pm 1\}$
$\mathbb{Q}$	$+$	0	$\mathbb{Q}$ (È già un gruppo!)
$\mathbb{Q}$	$\cdot$	1	$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
$\mathbb{R}$	$+$	0	$\mathbb{R}$ (È già un gruppo!)
$\mathbb{R}$	$\cdot$	1	$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
$\mathcal{P}(X)$	$\cap$	X	$\{X\}$
$\mathcal{P}(X)$	$\cup$	$\emptyset$	$\{\emptyset\}$

Approfondimento sugli Insiemi delle Parti Vediamo perché gli invertibili di $\mathcal{P}(X)$ sono così pochi.

1. Intersezione ($\cap$) L'elemento neutro è X. Un insieme A è invertibile se esiste B tale che $A \cap B = X$. Poiché l'intersezione è sempre contenuta nei due insiemi di partenza, $X = A \cap B \subseteq A$. Ma sappiamo che $A \subseteq X$. Quindi l'unica possibilità è $A = X$. Dunque $U(\mathcal{P}(X), \cap) = \{X\}$.

2. Unione ($\cup$) L'elemento neutro è $\emptyset$. Un insieme A è invertibile se esiste B tale che $A \cup B = \emptyset$. Poiché l'unione contiene entrambi gli insiemi, $A \subseteq A \cup B = \emptyset$. L'unico sottoinsieme dell'insieme vuoto è il vuoto stesso, quindi $A = \emptyset$. Dunque $U(\mathcal{P}(X), \cup) = \{\emptyset\}$.

Invertibilità delle Funzioni Consideriamo il monoide $(M(X), \circ)$ delle funzioni da X in X. Chi sono gli elementi invertibili $U(M(X))$? La domanda si estende naturalmente a funzioni tra insiemi diversi $f : A \to B$.

Definizione 0.23. Una funzione $f : A \to B$ si dice **invertibile** se esiste una funzione $h : B \to A$ tale che:

$$h \circ f = id_A \quad \text{e} \quad f \circ h = id_B$$

Tale funzione h, se esiste, è unica e si chiama **inversa** di f, indicata con f^{-1}.

L'unicità si dimostra esattamente come nei monoidi: se g fosse un'altra inversa, $g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h$.

Proposizione 0.17. *Una funzione $f : A \to B$ è invertibile se e solo se è biettiva.*

$$f \text{ invertibile} \iff f \text{ biettiva}$$

Proof. Dimostriamo le due implicazioni.

1) ($\implies$) **Se f è invertibile, allora è biettiva.** Per ipotesi esiste $h : B \to A$ che funge da inversa destra e sinistra.

- Suriettività: Dato un qualsiasi $b \in B$, possiamo scrivere $b = id_B(b) = (f \circ h)(b) = f(h(b))$. Posto $a = h(b)$, abbiamo trovato un elemento $a \in A$ tale che $f(a) = b$. Quindi f è suriettiva.
- Iniettività: Siano $x_1, x_2 \in A$ tali che $f(x_1) = f(x_2)$. Applichiamo h a entrambi i membri: $h(f(x_1)) = h(f(x_2))$. Per la proprietà dell'inversa: $(h \circ f)(x_1) = (h \circ f)(x_2) \implies id_A(x_1) = id_A(x_2) \implies x_1 = x_2$. Quindi f è iniettiva.

Essendo iniettiva e suriettiva, f è biettiva.

2) ($\impliedby$) **Se f è biettiva, allora è invertibile.** Se f è biettiva, la relazione inversa $f^t \subseteq B \times A$ è una funzione. Mostriamo che f^t soddisfa le proprietà dell'inversa.

- Calcoliamo $f^t \circ f$: Per ogni $a \in A$, sia $b = f(a)$. Per definizione di inversa, questo significa $f^t(b) = a$. Allora $(f^t \circ f)(a) = f^t(f(a)) = f^t(b) = a$. Quindi $f^t \circ f = id_A$.
- Calcoliamo $f \circ f^t$: Per ogni $b \in B$, sia $a = f^t(b)$. Per definizione, questo significa $f(a) = b$. Allora $(f \circ f^t)(b) = f(f^t(b)) = f(a) = b$. Quindi $f \circ f^t = id_B$.

Dunque f^t è l'inversa di f, e f è invertibile. □

Corollario sull'Invertibilità Iniziamo con un risultato generale sulla composizione di funzioni invertibili.

Corollario 1. *Siano $f : A \to B$ e $g : B \to C$ due applicazioni invertibili. Allora la loro composizione $g \circ f : A \to C$ è anch'essa invertibile.*

Proof. Poiché f e g sono invertibili, sono entrambe biettive. Sappiamo che la composizione di funzioni biettive è a sua volta biettiva. Essendo $g \circ f$ biettiva, essa è invertibile. L'espressione esplicita dell'inversa è data da:

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

Nota: L'ordine si inverte. Questo è coerente con quanto visto per le relazioni: $(g \circ f)^t = f^t \circ g^t$. Verifichiamo che questa sia effettivamente l'inversa a destra e a sinistra:

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

Analogamente si verifica che $(f^{-1} \circ g^{-1}) \circ (g \circ f) = id_A$. □

Il Gruppo Simmetrico $S(X)$ Applicando quanto sopra al caso in cui dominio e codominio coincidono $(X \to X)$, scopriamo che l'insieme delle funzioni biettive su X forma un gruppo rispetto all'operazione di composizione.

Definizione 0.24. L'insieme di tutte le applicazioni biettive da un insieme X in se stesso è denotato con $S(X)$. La struttura $(S(X), \circ)$ è un gruppo, detto *Gruppo Simmetrico* su X. La sua cardinalità dipende dalla cardinalità di X:

$$|X| = n \implies |S(X)| = n!$$

Gli elementi di $S(X)$ si chiamano *permutazioni* e si rappresentano spesso in forma matriciale:

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix}$$

Esempio 0.16. Sia $X = \{1, 2, 3, 4\}$. Un esempio di permutazione è:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Questo significa: $1 \to 3$, $2 \to 2$ (fisso), $3 \to 4$, $4 \to 1$. L'inversa f^{-1} si ottiene leggendo la mappa al contrario (scambiando righe e riordinando):

$$f^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \xrightarrow{\text{riordino}} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

L'elemento neutro del gruppo è l'identità:

$$1_{S(X)} = id_X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Calcolo della Composizione Attenzione all'ordine di applicazione: $(f \circ g)(x) = f(g(x))$. Prima agisce g, poi f.

Esempio 0.17. Siano $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ e $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Calcoliamo $f \circ g$:

- $1 \xrightarrow{g} 4 \xrightarrow{f} 1$
- $2 \xrightarrow{g} 3 \xrightarrow{f} 4$
- $3 \xrightarrow{g} 2 \xrightarrow{f} 2$
- $4 \xrightarrow{g} 1 \xrightarrow{f} 3$

Risultato: $f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

Il Gruppo S_3 (Permutazioni su 3 elementi) Analizziamo nel dettaglio il caso $X = \{1, 2, 3\}$. Il gruppo ha cardinalità $3! = 6$. Ecco i 6 elementi in notazione matriciale:

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Notazione Ciclica Una notazione molto più compatta è quella dei *cicli*. Un ciclo $(a_1\ a_2 \dots a_k)$ indica che $a_1 \to a_2$, $a_2 \to a_3$, ..., $a_k \to a_1$, mentre gli altri elementi restano fissi.

Ecco la corrispondenza per S_3:

Matrice	**Cicli**	**Nome**	**Inverso**
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	(1)(2)(3) o id	Identità	id
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	(1 2 3)	3-ciclo	(1 3 2)
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	(1 3 2)	3-ciclo	(1 2 3)
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	(2 3)	Scambio	(2 3)
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	(1 3)	Scambio	(1 3)
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	(1 2)	Scambio	(1 2)

Tabella di Moltiplicazione di S_3 Costruiamo la tabella delle composizioni. L'elemento di riga viene composto a sinistra, quello di colonna a destra (ma attenzione alla convenzione: qui la tabella sembra costruita come "Riga ∘ Colonna" o viceversa a seconda dell'autore. Analizzando un incrocio: (1 2 3) ∘ (1 2). $1 \xrightarrow{(12)} 2 \xrightarrow{(123)} 3$. $2 \xrightarrow{(12)} 1 \xrightarrow{(123)} 2$. $3 \xrightarrow{(12)} 3 \xrightarrow{(123)} 1$. Risultato (1 3). Nella tabella sotto, l'incrocio Riga (123) e Colonna (12) dà (13). Quindi la convenzione è **Riga ∘ Colonna** (applico prima la colonna, poi la riga).

∘	id	(123)	(132)	(23)	(13)	(12)
id	id	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	id	(13)	(23)	(12)
(132)	(132)	id	(123)	(12)	(12)	(13)
(23)	(23)	(13)	(12)	id	(123)	(132)
(13)	(13)	(12)	(23)	(132)	id	(123)
(12)	(12)	(23)	(13)	(123)	(132)	id

Nota 9. Osservando la tabella notiamo che non è simmetrica rispetto alla diagonale principale. Questo conferma che il gruppo S_3 non è commutativo. Ad esempio:

$$(12) \circ (123) = (23) \quad \neq \quad (123) \circ (12) = (13)$$

Traslazioni (Moltiplicazioni) nel Gruppo Possiamo interpretare le righe della tabella come funzioni. Fissato un elemento $g \in G$, definiamo la traslazione sinistra l_g:

$$l_g : G \to G, \quad x \mapsto g \circ x$$

Questa funzione corrisponde esattamente alla riga della tabella associata all'elemento g. Il fatto fondamentale è che in ogni riga e in ogni colonna compaiono tutti gli elementi del gruppo esattamente una volta. In termini funzionali, questo significa che l'applicazione l_g è biettiva:

$$\forall y \in G, \exists! x \in G : y = g \circ x$$

La soluzione unica è $x = g^{-1} \circ y$.

Traslazioni nel Gruppo Un concetto fondamentale per comprendere la struttura interna di un gruppo è osservare come un singolo elemento agisca su tutti gli altri tramite l'operazione del gruppo. Fissando un elemento g, possiamo definire una funzione che "sposta" (o trasla) tutti gli elementi del gruppo.

Definizione 0.25. Sia $(G, \cdot)$ un gruppo e sia $g \in G$ un elemento fissato. Si definisce l'applicazione l_g, detta *moltiplicazione a sinistra per g* (o traslazione sinistra), come:

$$\begin{aligned} l_g : G &\longrightarrow G \\ x &\longmapsto g \cdot x \end{aligned}$$

Questa applicazione gode di una proprietà importantissima: non "perde" informazioni e copre tutto il gruppo. In termini formali:

Proposizione 0.18. *L'applicazione l_g è biettiva da G in G.*

Proof. Per dimostrare la biettività, verifichiamo separatamente suriettività e iniettività.

1) Suriettività Dobbiamo provare che per ogni $y \in G$ esiste un $x \in G$ tale che $y = l_g(x)$. L'equazione $y = l_g(x)$ corrisponde a:

$$y = g \cdot x$$

Dove y è il parametro (il valore che vogliamo raggiungere) e x è l'incognita. Poiché siamo in un gruppo, g è invertibile. Moltiplichiamo a sinistra per g^{-1}:

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x)$$

Utilizzando la proprietà associativa e la definizione di inverso:

$$g^{-1} \cdot y = (g^{-1} \cdot g) \cdot x = 1_G \cdot x = x$$

Abbiamo trovato la soluzione: $x = g^{-1} \cdot y$. Verifichiamo che questa soluzione funzioni:

$$l_g(g^{-1} \cdot y) = g \cdot (g^{-1} \cdot y) = (g \cdot g^{-1}) \cdot y = 1_G \cdot y = y$$

Poiché per ogni y abbiamo trovato una controimmagine, l_g è suriettiva.

2) Iniettività Dobbiamo provare che se due elementi hanno la stessa immagine, allora sono uguali. Siano $x_1, x_2 \in G$ tali che $l_g(x_1) = l_g(x_2)$.

$$g \cdot x_1 = g \cdot x_2$$

Moltiplichiamo a sinistra entrambi i membri per g^{-1}:

$$g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2)$$

$$(g^{-1} \cdot g) \cdot x_1 = (g^{-1} \cdot g) \cdot x_2$$

$$1_G \cdot x_1 = 1_G \cdot x_2 \implies x_1 = x_2$$

L'applicazione è dunque iniettiva. □

Analogamente, possiamo definire l'operazione che agisce dall'altro lato.

Definizione 0.26. Sia $(G, \cdot)$ un gruppo e $g \in G$ fissato. Si definisce l'applicazione P_g, detta *moltiplicazione a destra per* g, come:

$$P_g : G \to G$$
$$x \mapsto x \cdot g$$

Proposizione 0.19. *Anche l'applicazione P_g è biettiva da G in G.*

Proof. La dimostrazione è perfettamente speculare a quella per l_g, moltiplicando però per g^{-1} a destra invece che a sinistra. □

Tabelle di Moltiplicazione La biettività delle traslazioni l_g e P_g ha una conseguenza visiva immediata sulle tabelle di moltiplicazione dei gruppi finiti: in ogni riga (rappresentata da l_g) e in ogni colonna (rappresentata da P_g) ogni elemento del gruppo compare *esattamente una volta*.

Analizziamo i gruppi di cardinalità piccola.

Gruppi di ordine 2 ($|G| = 2$) Sia $G = \{1_G, a\}$. Poiché l'elemento neutro 1_G deve lasciare invariati gli altri, e ogni elemento deve comparire una volta sola, la tabella è obbligata:

$*$	1_G	a
1_G	1_G	a
a	a	1_G

L'unica possibilità per l'ultima casella $(a \cdot a)$ è 1_G, poiché a è già presente nella riga. Quindi a è l'inverso di se stesso ($a^2 = 1_G$).

Esempio 0.18. Un esempio concreto è il gruppo degli invertibili di $\mathbb{Z}$, $U(\mathbb{Z}) = \{1, -1\}$ con l'operazione di moltiplicazione:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Gruppi di ordine 3 ($|G| = 3$) Sia $G = \{1_G, a, b\}$. Anche qui la struttura è "rigida". Dobbiamo completare la riga di a. Abbiamo già $a \cdot 1_G = a$. Rimangono da piazzare 1_G e b. Se fosse $a \cdot a = 1_G$, allora per esclusione $a \cdot b = b$, ma questo implicherebbe $a = 1_G$, impossibile. Quindi necessariamente $a \cdot a = b$ e $a \cdot b = 1_G$. La tabella risultante è:

$\cdot$	1_G	a	b
1_G	1_G	a	b
a	a	b	1_G
b	b	1_G	a

Ogni gruppo di 3 elementi è isomorfo a questa struttura (gruppo ciclico).

Esempio 0.19. Un esempio concreto è il sottogruppo delle permutazioni pari su 3 elementi, detto **Gruppo Alterno** A_3, che corrisponde alle rotazioni di un triangolo.

$$A_3 = \{id, (123), (132)\} \subseteq S_3$$

Osserviamo la tabella parziale:

$\circ$	id	(123)	(132)
id	id	(123)	(132)
(123)	(123)	(132)	id
(132)	(132)	id	(123)

Sottogruppi Spesso all'interno di un gruppo è possibile individuare un sottoinsieme che costituisce a sua volta un gruppo con la stessa operazione.

Definizione 0.27. Sia $(G, \cdot)$ un gruppo e sia $H \subseteq G$ un sottoinsieme non vuoto ($H \neq \emptyset$). Diciamo che H è un *sottogruppo* di G se verifica le seguenti condizioni di chiusura:

1. *Chiusura rispetto all'operazione:* $\forall x, y \in H \implies x \cdot y \in H$.
2. *Chiusura rispetto all'inverso:* $\forall x \in H \implies x^{-1} \in H$.

Analisi della definizione Verifichiamo che queste condizioni siano sufficienti a rendere H un gruppo. L'operazione in H è quella *indotta* da G, ovvero la restrizione della funzione prodotto:

$$H \times H \longrightarrow G \longrightarrow H$$

Grazie alla condizione (1), il codominio è effettivamente H (l'operazione è ben definita interna ad H).

Dobbiamo verificare gli assiomi di gruppo per $(H, \cdot)$:

- **Associatività:** Poiché l'operazione è associativa su tutto G ($a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni $a, b, c \in G$), lo è automaticamente anche per gli elementi di H. L'associatività è *ereditaria*.
- **Esistenza dell'inverso:** È garantita dalla condizione (2).
- **Esistenza dell'elemento neutro:** Questo va dimostrato, ma segue dalle proprietà precedenti.

Proposizione 0.20. *Se H è un sottogruppo di G, allora $1_G \in H$.*

Proof. Poiché $H \neq \emptyset$, esiste almeno un elemento $a \in H$. Per la condizione (2) (chiusura rispetto all'inverso), deve esistere in H anche l'inverso di a, ovvero $a^{-1} \in H$. Ora applichiamo la condizione (1) (chiusura rispetto al prodotto) agli elementi a e a^{-1}:

$$a \cdot a^{-1} \in H$$

Ma sappiamo che $a \cdot a^{-1} = 1_G$. Quindi $1_G \in H$. □

Concludendo, $(H, \cdot)$ soddisfa tutti gli assiomi ed è quindi un gruppo a tutti gli effetti.

Definizione Alternativa di Sottogruppo Possiamo caratterizzare i sottogruppi in un modo leggermente diverso, ma equivalente, concentrandoci sulla struttura interna.

Definizione 0.28. Sia $(G, \cdot)$ un gruppo e $H \subseteq G$ un sottoinsieme non vuoto. Diciamo che H è un **sottogruppo** di G se e solo se:

1. H è **chiuso** (o **stabile**) rispetto all'operazione di G (cioè $\forall x, y \in H \implies x \cdot y \in H$).
2. La struttura $(H, \cdot)$, con l'operazione indotta, è essa stessa un gruppo.

Questa definizione implica che H deve avere un suo elemento neutro 1_H e che ogni elemento deve avere un inverso in H. **Ma questi coincidono con quelli di G?**

Proposizione 0.21. *Se H è un sottogruppo di G: 1. L'elemento neutro di H coincide con quello di G ($1_H = 1_G$). 2. L'inverso di un elemento in H coincide con il suo inverso in G.*

Proof. **1) Dimostrazione che** $1_H = 1_G$ Per definizione di elemento neutro in H, vale $1_H \cdot 1_H = 1_H$. Consideriamo questa uguaglianza in G. Sia $a = 1_H$. L'equazione diventa $a \cdot a = a$ (proprietà di idempotenza). Moltiplichiamo entrambi i membri per a^{-1} (l'inverso di a in G):

$$a^{-1} \cdot (a \cdot a) = a^{-1} \cdot a$$

$$(a^{-1} \cdot a) \cdot a = 1_G$$

$$1_G \cdot a = 1_G \implies a = 1_G$$

Quindi $1_H = 1_G$.

2) Dimostrazione sull'inverso Sia $x \in H$. Poiché $(H, \cdot)$ è un gruppo, esiste $y \in H$ tale che $x \cdot y = 1_H$. Ma abbiamo appena dimostrato che $1_H = 1_G$, quindi $x \cdot y = 1_G$. Per l'unicità dell'inverso in un gruppo, y deve essere necessariamente l'inverso di x in G (x^{-1}). Quindi l'inverso "interno" coincide con quello "esterno". □

Analisi dei Sottogruppi di S_3 Cerchiamo di individuare tutti i possibili sottogruppi del gruppo simmetrico S_3. Ricordiamo gli elementi e i loro inversi:

$$S_3 = \{id, (123), (132), (12), (13), (23)\}$$

Inversi:

- $id^{-1} = id$
- $(123)^{-1} = (132)$ e viceversa.
- Gli scambi (trasposizioni) sono inversi di se stessi: $(12)^{-1} = (12)$, ecc.

Classificazione per Cardinalità Un sottogruppo H deve contenere l'identità e deve dividere l'ordine del gruppo (Teorema di Lagrange, che vedremo più avanti, ci dice che $|H|$ divide $|G| = 6$). Le cardinalità possibili per H sono quindi: 1, 2, 3, 4, 5, 6.

1. Ordine 1 ($|H| = 1$) L'unico sottogruppo possibile deve contenere l'elemento neutro.

$$H_1 = \{id\}$$

È il sottogruppo banale.

2. Ordine 2 ($|H| = 2$) Deve essere del tipo $H = \{id, \alpha\}$. Affinché sia un gruppo, deve essere chiuso rispetto all'inverso. Quindi α^{-1} deve stare in H. Se $\alpha^{-1} = id$, allora $\alpha = id$ (impossibile perché $|H| = 2$). Quindi deve essere $\alpha^{-1} = \alpha$ (l'elemento è inverso di se stesso, ha ordine 2). Gli elementi di ordine 2 in S_3 sono i tre scambi: $(12), (13), (23)$. Troviamo 3 sottogruppi:

- $H_2 = \{id, (12)\}$
- $H_3 = \{id, (13)\}$
- $H_4 = \{id, (23)\}$

Le tabelle di moltiplicazione confermano la chiusura (es. $(12)(12) = id$).

3. Ordine 3 ($|H| = 3$) Deve essere del tipo $H = \{id, \alpha, \beta\}$. Gli elementi devono essere chiusi rispetto all'inverso. Consideriamo l'inverso di α:

- Se $\alpha^{-1} = \alpha$, allora α è uno scambio. Questo costringerebbe anche β ad essere uno scambio ($\beta^{-1} = \beta$). Ma il prodotto di due scambi distinti non è uno scambio (es. $(12)(13) = (132)$), quindi usciremmo dall'insieme $\{id, (12), (13)\}$. Un insieme di soli scambi più l'identità non è chiuso.
- Quindi deve essere $\alpha^{-1} = \beta$ (e viceversa). Gli unici elementi che sono l'uno l'inverso dell'altro sono i 3-cicli: (123) e (132).

Troviamo un solo sottogruppo:

$$H_5 = A_3 = \{id, (123), (132)\}$$

Questo è il Gruppo Alterno. La tabella conferma la chiusura (il prodotto di due rotazioni è una rotazione).

4. Ordine 4 ($|H| = 4$) $H = \{id, \alpha, \beta, \gamma\}$. Proviamo a costruirlo:

- Se contiene un 3-ciclo, per chiusura inversa deve contenere anche l'altro. Quindi avremmo $\{id, (123), (132), \gamma\}$. Qualunque scambio scegliamo per γ (es. (12)), il prodotto con un 3-ciclo genera un altro scambio mancante (es. $(123)(12) = (13)$), portando la cardinalità oltre 4. Non è chiuso.
- Se non contiene 3-cicli, deve contenere solo scambi: $\{id, (12), (13), (23)\}$. Ma come visto prima, il prodotto di scambi genera 3-cicli (es. $(12)(13) = (132)$), che non sono nell'insieme. Non è chiuso.

Non esistono sottogruppi di ordine 4 in S_3.

5. Ordine 5 ($|H| = 5$) Impossibile. Se aggiungiamo un elemento a un sottogruppo di ordine 4 (che non esiste) o due a uno di ordine 3, la chiusura fallisce inevitabilmente generando l'intero gruppo. Inoltre 5 non divide 6.

Sottogruppi di S_4 Analizziamo la struttura dei sottogruppi all'interno del gruppo simmetrico S_4, che rappresenta le permutazioni su 4 elementi e ha cardinalità $|S_4| = 24$. Ricordiamo la notazione: $H \leq G$ indica che H è un sottogruppo di G. Per verificare questa proprietà per un sottoinsieme finito, dobbiamo controllare due condizioni fondamentali:

- *Chiusura:* $\forall x, y \in H \implies x \circ y \in H$
- *Esistenza degli inversi:* $\forall x \in H \implies x^{-1} \in H$

1. Sottogruppo di ordine 2 Consideriamo il sottoinsieme $H_1 = \{id, (24)\}$. Verifichiamo che sia un sottogruppo.

- *Inversi:* L'identità è inversa di se stessa. L'elemento (24) è uno scambio (trasposizione), e ogni scambio coincide con il proprio inverso: $(24)^{-1} = (24) \in H_1$.
- *Chiusura:* Costruiamo la tabella di moltiplicazione:

$\circ$	id	(24)
id	id	(24)
(24)	(24)	id

Poiché il risultato di ogni operazione ricade nell'insieme (troviamo solo id e (24)), l'insieme è chiuso. *Conclusione:* $H_1 \leq S_4$.

Esempio di NON sottogruppo Per contrasto, consideriamo l'insieme $A = \{(12)\}$. Questo insieme non è un sottogruppo per due motivi: 1. Manca l'elemento neutro id. 2. Non è chiuso: $(12) \circ (12) = id$, e $id \notin A$.

2. Sottogruppo di ordine 4 (Tipo Klein) Esaminiamo ora un sottogruppo generato da due trasposizioni disgiunte:

$$H_2 = \{id, (12), (34), (12)(34)\}$$

Notiamo subito una proprietà importante: poiché (12) e (34) operano su indici diversi (sono disgiunti), essi commutano, ovvero $(12)(34) = (34)(12)$. Inoltre, ogni elemento di questo insieme ha ordine 2 (il quadrato è l'identità), quindi ogni elemento è l'inverso di se stesso.

Tabella di moltiplicazione di H_2:

$\circ$	id	(12)	(34)	$(12)(34)$
id	id	(12)	(34)	$(12)(34)$
(12)	(12)	id	$(12)(34)$	(34)
(34)	(34)	$(12)(34)$	id	(12)
$(12)(34)$	$(12)(34)$	(34)	(12)	id

La tabella è chiusa, quindi $H_2 \leq S_4$.

3. Il Gruppo di Klein V_4 Esiste un altro sottogruppo di ordine 4 in S_4, molto famoso, composto dall'identità e dalle tre possibili doppie trasposizioni disgiunte.

$$K = \{id, (12)(34), (13)(24), (14)(23)\}$$

Per facilitare i calcoli, assegniamo dei nomi agli elementi:

$$1 = id, \quad \alpha = (12)(34), \quad \beta = (13)(24), \quad \gamma = (14)(23)$$

Verifichiamo la chiusura calcolando esplicitamente il prodotto $\alpha \circ \beta$:

$$\alpha \circ \beta = (12)(34) \circ (13)(24)$$

Seguiamo il percorso degli elementi da destra a sinistra:

- $1 \xrightarrow{\beta} 3 \xrightarrow{\alpha} 4$
- $4 \xrightarrow{\beta} 2 \xrightarrow{\alpha} 1$
- $2 \xrightarrow{\beta} 4 \xrightarrow{\alpha} 3$
- $3 \xrightarrow{\beta} 1 \xrightarrow{\alpha} 2$

Il risultato è la permutazione che scambia (14) e (23), che corrisponde esattamente a γ. Analogamente si verifica che $\beta \circ \alpha = \gamma$ (commutatività).

Poiché $\alpha^2 = \beta^2 = \gamma^2 = 1$ (ogni elemento è inverso di se stesso), la tabella assume questa forma simmetrica:

$\circ$	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

Questo gruppo è noto come **Gruppo di Klein** (V_4). È un gruppo abeliano (commutativo) non ciclico.

Interpretazione Geometrica di V_4 Possiamo visualizzare V_4 come il gruppo delle simmetrie di un rettangolo (o le simmetrie non rotazionali di un quadrato) con vertici etichettati $1, 2, 3, 4$.

- $\alpha = (12)(34)$: Corrisponde alla riflessione rispetto all'asse verticale (scambia i vertici in alto tra loro e quelli in basso tra loro).
- $\beta = (13)(24)$: Corrisponde alla riflessione rispetto all'asse orizzontale.
- $\gamma = (14)(23)$: Corrisponde alla simmetria centrale (o rotazione di 180°).

4. Confronto con il Gruppo Ciclico (Rotazioni del Quadrato) Consideriamo ora un altro sottoinsieme di S_4 di ordine 4, generato dalla rotazione di un quadrato:

$$C_4 = \{id, (1234), (13)(24), (1432)\}$$

Geometricamente corrisponde alle rotazioni di $0°, 90°, 180°, 270°$.

Poniamo $1 = id$, $\alpha = (1234)$. Notiamo che:

- $\alpha^2 = (1234) \circ (1234) = (13)(24)$ (che è la rotazione di 180°).
- $\alpha^3 = (1432)$ (che è la rotazione inversa, o di 270°).
- $\alpha^4 = id$.

La tabella di moltiplicazione di questo gruppo è:

$\circ$	1	α	α^2	α^3
1	1	α	α^2	α^3
α	α	α^2	α^3	1
α^2	α^2	α^3	1	α
α^3	α^3	1	α	α^2

Conclusione: Isomorfismo Confrontiamo il gruppo di Klein V_4 con questo gruppo C_4.

- Entrambi hanno ordine 4.
- Entrambi sono commutativi (abeliani).
- Tuttavia, le loro tabelle di moltiplicazione (e quindi le loro strutture) sono diverse.

In V_4, ogni elemento (tranne l'identità) ha ordine 2 ($x^2 = 1$). Nella tabella di V_4 la diagonale principale è composta interamente da 1. In C_4, esistono elementi di ordine 4 (α e α^3). Nella tabella di C_4, la diagonale non contiene sempre 1 (infatti $\alpha \cdot \alpha = \alpha^2 \neq 1$).

Dunque, pur avendo la stessa cardinalità, V_4 e C_4 *non sono isomorfi*.

Classificazione dei Gruppi di ordine 4 Un risultato classico della teoria dei gruppi riguarda la struttura dei gruppi con cardinalità ridotta. Se un gruppo ha 4 elementi, la sua struttura è fortemente vincolata.

Proposizione 0.22. *Se $(G, *)$ è un gruppo con cardinalità $|G| = 4$, allora si verifica una delle seguenti due possibilità :*

1. *G è isomorfo al Gruppo di Klein $(V_4, \circ)$.*
2. *G è isomorfo al Gruppo Ciclico $(\mathbb{C}_4, \circ)$ (spesso indicato con Z_4 o C_4).*

In termini pratici, ciò significa che la tavola di moltiplicazione di G sarà identica a quella di uno di questi due gruppi.

Ricordiamo i modelli di riferimento in S_4:

$$V_4 = \{id, (12)(34), (13)(24), (14)(23)\} \quad \text{(tutti elementi di ordine 2)}$$

$$\mathbb{C}_4 = \{id, (1234), (13)(24), (1432)\} \quad \text{(gruppo ciclico)}$$

Proof. Sia $G = \{1_G, a, b, c\}$. Per classificare il gruppo, analizziamo le proprietà degli inversi dei suoi elementi. Distinguiamo due casi possibili.

Caso 1: Ogni elemento è inverso di se stesso Supponiamo che $g = g^{-1}$ per ogni $g \in G$. Ciò implica che $g^2 = 1_G$ per tutti gli elementi. Nella tabella di moltiplicazione, questo significa che la diagonale principale è interamente composta dall'elemento neutro 1_G.

Costruiamo la tabella per $G = \{1_G, a, b, c\}$:

- La prima riga e la prima colonna sono copie degli elementi (per proprietà dell'elemento neutro).
- La diagonale è 1_G.

- Per riempire le caselle rimanenti, usiamo la proprietà che ogni riga e colonna deve contenere tutti gli elementi una sola volta (biettività delle traslazioni). Ad esempio, per $a \cdot b$: non può essere 1_G (perché l'inverso di a è a), non può essere a (perché $b \neq 1_G$), non può essere b (perché $a \neq 1_G$). Quindi necessariamente $a \cdot b = c$.

La tabella risultante è:

$\circ$	1_G	a	b	c
1_G	1_G	a	b	c
a	a	1_G	c	b
b	b	c	1_G	a
c	c	b	a	1_G

Questa struttura è identica a quella di V_4 (Gruppo di Klein).

Caso 2: Esiste almeno un elemento diverso dal proprio inverso Supponiamo che $\exists a \in G$ tale che $a \neq a^{-1}$. Poiché l'inverso è unico e diverso da a, e ovviamente diverso da 1_G, questo elemento deve essere un altro elemento del gruppo, diciamo c. Quindi $c = a^{-1}$ e, reciprocamente, $a = c^{-1}$. Rimane l'elemento b. Qual è il suo inverso? Gli inversi devono accoppiarsi. Abbiamo già le coppie $(1_G, 1_G)$ e (a, c). L'elemento b è rimasto solo, quindi deve essere inverso di se stesso: $b = b^{-1}$.

Riassumendo gli inversi:

g	g^{-1}
1_G	1_G
a	c
b	b
c	a

Compiliamo la tabella sfruttando queste informazioni:

- $a \cdot c = 1_G$ e $c \cdot a = 1_G$.
- $b \cdot b = 1_G$.
- Consideriamo $a \cdot a$ (posizione a, a). Non può essere 1_G (altrimenti $a = a^{-1}$ contro ipotesi). Non può essere a o c. Dunque $a \cdot a = b$.
- Di conseguenza $a \cdot b$ deve essere c, e così via.

La tabella risultante è:

$\circ$	1_G	a	b	c
1_G	1_G	a	b	c
a	a	b	c	1_G
b	b	c	1_G	a
c	c	1_G	a	b

Questa struttura corrisponde a quella di $\mathbb{C}_4$ (nota che $a^2 = b, a^3 = c, a^4 = 1_G$). □

Nota 10. La compilazione delle tabelle è stata resa possibile dal fatto che, fissato g, le applicazioni:

- $l_g(x) = gx$ (moltiplicazione a sinistra)
- $P_g(x) = xg$ (moltiplicazione a destra)
- $i(x) = x^{-1}$ (inversione)

sono tutte *biettive*. Questo garantisce che non ci siano ripetizioni nelle righe o nelle colonne.

Sottogruppi di $(\mathbb{R}^*, \cdot)$ Analizziamo alcuni sottoinsiemi del gruppo moltiplicativo dei numeri reali non nulli per vedere se sono sottogruppi.

Esempio 0.20. Sia $A = [0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$. Questo insieme è *stabile* rispetto alla moltiplicazione. Infatti, presi due elementi qualsiasi $x, y \in A$, valgono le disuguaglianze:

$$0 \leq x \leq 1 \quad \text{e} \quad 0 \leq y \leq 1$$

Moltiplicando i membri (essendo tutto non negativo):

$$0 \leq x \cdot y \leq y \leq 1 \implies x \cdot y \in [0, 1]$$

Quindi il prodotto rimane nell'insieme.]

Esempio 0.21. Sia $B = [-1, 1]$. Anche questo insieme è *stabile* in $\mathbb{R}$ rispetto alla moltiplicazione. Proviamolo analizzando i casi per il segno di y (assumendo senza perdita di generalità $-1 \leq x \leq 1$).

Caso 1: y non negativo ($0 \leq y \leq 1$) Poiché $-1 \leq x \leq 1$ e $y \geq 0$, moltiplicando per y le disuguaglianze non cambiano verso:

$$-1 \cdot y \leq x \cdot y \leq 1 \cdot y \implies -y \leq xy \leq y$$

Dato che $0 \leq y \leq 1$, abbiamo che $-1 \leq -y$ e $y \leq 1$. Quindi: $-1 \leq -y \leq xy \leq y \leq 1$, il che implica $xy \in B$.

Caso 2: y negativo ($-1 \leq y \leq 0$) Poiché $-1 \leq x \leq 1$ e $y \leq 0$ (o meglio $-y \geq 0$), moltiplicando per y si inverte il verso delle disuguaglianze:

$$-1 \cdot y \geq x \cdot y \geq 1 \cdot y \implies -y \geq xy \geq y$$

Dato che $-1 \leq y \leq 0$, allora $0 \leq -y \leq 1$. Quindi: $1 \geq -y \geq xy \geq y \geq -1$. Anche in questo caso $-1 \leq xy \leq 1$, quindi $xy \in B$.

Esempio 0.22. Consideriamo invece $C = [0, 2]$. Questo insieme *non* è stabile rispetto alla moltiplicazione. Basta fornire un controesempio: Siano $x = 2$ e $y = 2$. Entrambi appartengono a C. Tuttavia:

$$x \cdot y = 4 \notin [0, 2]$$

La chiusura non è rispettata.

Esempio 0.23. Consideriamo l'intervallo $A^* =]0, 1]$. È un sottogruppo di $(\mathbb{R}^*, \cdot)$? La risposta è **NO**. Verifichiamo le condizioni:

- *Chiusura rispetto al prodotto:* Se $a, b \in]0, 1]$, allora $0 < a \leq 1$ e $0 < b \leq 1$, quindi il loro prodotto ab è ancora ≤ 1. La chiusura è verificata.
- *Chiusura rispetto all'inverso:* Qui fallisce. Prendiamo ad esempio $a = \frac{1}{2} \in A^*$. Il suo inverso è $a^{-1} = 2$. Ma $2 \notin]0, 1]$.

Esempio 0.24. Consideriamo ora l'insieme dei reali positivi $D =]0, +\infty[= \mathbb{R}^{*+}$. È un sottogruppo? **SÌ**.

- Il prodotto di due numeri positivi è positivo.
- L'inverso (reciproco) di un numero positivo è positivo.

Il Gruppo delle Funzioni Affini Costruiamo un gruppo molto importante in geometria, formato da funzioni che trasformano la retta reale. Siano $a, b \in \mathbb{R}$ con $a \neq 0$. Definiamo l'applicazione $f_{a,b}$:

$$\begin{aligned} f_{a,b} : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto ax + b \end{aligned}$$

Proposizione 0.23. *L'applicazione $f_{a,b}$ è biettiva (e dunque appartiene al gruppo simmetrico $S(\mathbb{R})$).*

Proof. Verifichiamo iniettività e suriettività. **1) Iniettività:** Dobbiamo provare che $f_{a,b}(x) = f_{a,b}(y) \implies x = y$.

$$ax + b = ay + b \implies ax = ay$$

Poiché per ipotesi $a \neq 0$, possiamo dividere per a, ottenendo $x = y$.

2) Suriettività: Dobbiamo provare che $\forall y \in \mathbb{R}, \exists x \in \mathbb{R} : y = f_{a,b}(x)$. Impostiamo l'equazione nell'incognita x:

$$y = ax + b$$

Isolando la x:

$$ax = y - b \implies x = \frac{y - b}{a}$$

La soluzione esiste sempre ed è unica (dato che $a \neq 0$). □

Possiamo quindi scrivere esplicitamente l'applicazione inversa $f_{a,b}^{-1}$:

$$y \longmapsto \frac{y - b}{a} = \frac{1}{a}y - \frac{b}{a}$$

In termini della nostra notazione parametrica, l'inversa corrisponde a una funzione dello stesso tipo con nuovi parametri:

$$f_{a,b}^{-1} = f_{\frac{1}{a}, -\frac{b}{a}}$$

Il Gruppo H Consideriamo l'insieme di tutte queste funzioni:

$$H = \{f_{a,b} \mid a, b \in \mathbb{R}, a \neq 0\} \subseteq S(\mathbb{R})$$

Vogliamo dimostrare che H è un sottogruppo di $(S(\mathbb{R}), \circ)$. Abbiamo già visto che l'inverso di un elemento di H sta ancora in H (poiché $1/a \neq 0$). Resta da verificare la chiusura rispetto alla composizione.

Calcolo della Composizione Siano $f_{a,b}$ e $f_{c,d}$ due elementi di H. Calcoliamo $(f_{a,b} \circ f_{c,d})(x)$. Attenzione all'ordine: prima agisce $f_{c,d}$, poi $f_{a,b}$.

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b$$

Il risultato è una funzione della forma $Ax + B$ dove:

- Nuovo coefficiente moltiplicativo: $A = ac$ (che è $\neq 0$ perché $a, c \neq 0$).
- Nuovo termine noto: $B = ad + b$.

Quindi:

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b} \in H$$

L'insieme è chiuso, dunque $H \leq S(\mathbb{R})$.

Commutatività di H Il gruppo H è commutativo (abeliano)? Controlliamo se $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}$. Abbiamo calcolato sopra il primo membro. Calcoliamo il secondo:

$$(f_{c,d} \circ f_{a,b})(x) = f_{c,d}(ax + b) = c(ax + b) + d = cax + cb + d = f_{ca,cb+d}$$

Affinché coincidano per ogni x, i parametri devono essere uguali:

$$\begin{cases} ac = ca & \text{(Vero, prodotto in } \mathbb{R}) \\ ad + b = cb + d & \text{(Condizione critica)} \end{cases}$$

L'uguaglianza vale solo se $ad+b = cb+d$. Basta un controesempio per mostrare che non vale sempre. Scegliamo $a = 1, c = 2, b = 1, d = 0$:

$$\text{Membro SX (ad+b): } 1(0) + 1 = 1$$
$$\text{Membro DX (cb+d): } 2(1) + 0 = 2$$

Poiché $1 \neq 2$, il gruppo non è commutativo.

Analizziamo ora due importanti sottogruppi di H: il gruppo delle traslazioni T e il gruppo delle omotetie S.

1. Il Sottogruppo delle Traslazioni T Consideriamo l'insieme delle funzioni con coefficiente angolare unitario:

$$T = \{f_{1,b} \mid b \in \mathbb{R}\}$$

Verifichiamo che $T \leq (S(\mathbb{R}), \circ)$:

1. *Stabilità (Chiusura):* Siano $f_{1,b}, f_{1,d} \in T$. Applicando la regola di composizione con $a = 1, c = 1$:

$$f_{1,b} \circ f_{1,d} = f_{1 \cdot 1, 1 \cdot d + b} = f_{1,d+b}$$

   Poiché $d + b \in \mathbb{R}$, il risultato appartiene a T.

2. *Inverso:* Sia $f_{1,b} \in T$. Applicando la formula dell'inverso con $a = 1$:

$$f_{1,b}^{-1} = f_{\frac{1}{1}, -\frac{b}{1}} = f_{1,-b}$$

   Poiché $-b \in \mathbb{R}$, l'inverso appartiene a T.

Dunque T è un sottogruppo. Inoltre, osserviamo che T è *commutativo* (poiché $b + d = d + b$).

Proposizione 0.24. *Il gruppo $(T, \circ)$ è isomorfo al gruppo additivo dei reali $(\mathbb{R}, +)$.*

Proof. Definiamo l'applicazione $\varphi : \mathbb{R} \to T$ ponendo $\varphi(b) = f_{1,b}$.

1. *Biettività:* L'applicazione è chiaramente suriettiva per definizione di T. È iniettiva perché se $\varphi(b) = \varphi(\beta)$, allora $f_{1,b} = f_{1,\beta}$, il che implica $1x + b = 1x + \beta$ per ogni x, da cui $b = \beta$.
2. *Omomorfismo (Conservazione dell'operazione):* Dobbiamo provare che $\varphi(b + d) = \varphi(b) \circ \varphi(d)$.

$$\varphi(b + d) = f_{1,b+d}$$

$$\varphi(b) \circ \varphi(d) = f_{1,b} \circ f_{1,d} = f_{1,d+b}$$

Le due espressioni coincidono.

Quindi φ è un isomorfismo. □

2. Il Sottogruppo delle Omotetie S Consideriamo l'insieme delle funzioni con termine noto nullo:

$$S = \{f_{a,0} \mid a \in \mathbb{R}^*\}$$

Verifichiamo che $S \leq (S(\mathbb{R}), \circ)$:

1. *Stabilità (Chiusura):* Siano $f_{a,0}, f_{c,0} \in S$. Applicando la regola di composizione con $b = 0, d = 0$:

$$f_{a,0} \circ f_{c,0} = f_{ac,a\cdot 0+0} = f_{ac,0}$$

Poiché $ac \neq 0$ (essendo $a, c \in \mathbb{R}^*$), il risultato è in S.

2. *Inverso:* Sia $f_{a,0} \in S$.

$$f_{a,0}^{-1} = f_{\frac{1}{a},-\frac{0}{a}} = f_{\frac{1}{a},0}$$

L'inverso appartiene a S.

Dunque S è un sottogruppo. Anche S è *commutativo* (poiché $ac = ca$).

Proposizione 0.25. *Il gruppo $(S, \circ)$ è isomorfo al gruppo moltiplicativo dei reali non nulli $(\mathbb{R}^*, \cdot)$.*

Proof. Definiamo l'applicazione $\Psi : \mathbb{R}^* \to S$ ponendo $\Psi(a) = f_{a,0}$.

1. *Biettività:* Analoga al caso precedente. $f_{a,0} = f_{\alpha,0} \implies ax = \alpha x \implies a = \alpha$ (scegliendo $x = 1$).
2. *Omomorfismo:* Dobbiamo provare che $\Psi(ac) = \Psi(a) \circ \Psi(c)$.

$$\Psi(ac) = f_{ac,0}$$

$$\Psi(a) \circ \Psi(c) = f_{a,0} \circ f_{c,0} = f_{ac,0}$$

L'uguaglianza è verificata.

Quindi Ψ è un isomorfismo. □

Struttura del Gruppo H Abbiamo visto che T e S sono sottogruppi commutativi. Tuttavia, il gruppo H che li contiene *non* è commutativo. Possiamo descrivere H attraverso l'isomorfismo con il prodotto cartesiano $\mathbb{R}^* \times \mathbb{R}$ dotato di una specifica operazione.

Consideriamo la biiezione:

$$\Theta : \mathbb{R}^* \times \mathbb{R} \longrightarrow H$$
$$(a, b) \longmapsto f_{a,b}$$

Vogliamo definire un'operazione $*$ su $\mathbb{R}^* \times \mathbb{R}$ tale che Θ sia un isomorfismo:

$$\Theta((a, b) * (c, d)) = \Theta(a, b) \circ \Theta(c, d)$$

Sostituendo le funzioni:

$$\Theta((a, b) * (c, d)) = f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$$

Affinché questo corrisponda a $\Theta(ac, ad + b)$, dobbiamo definire l'operazione come:

$$(a, b) * (c, d) = (ac, ad + b)$$

Nota 11. Verifichiamo rapidamente gli assiomi di gruppo per la struttura $(\mathbb{R}^* \times \mathbb{R}, *)$:

- *Associatività:* $[(a, b) * (c, d)] * (e, f) = (ac, ad + b) * (e, f) = (ace, (ac)f + ad + b)$. $(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, cf + d) = (ace, a(cf + d) + b) = (ace, acf + ad + b)$. (Coincidono).
- *Elemento Neutro:* È la coppia $(1, 0)$, che corrisponde a $f_{1,0} = id$.
- *Inverso:* L'inverso di (a, b) è $(\frac{1}{a}, -\frac{b}{a})$, coerente con l'inverso funzionale.

Gli Assiomi di Peano Alla base dell'aritmetica e della costruzione dei numeri naturali vi è il sistema assiomatico proposto da Giuseppe Peano. Questo sistema definisce $\mathbb{N}$ tramite cinque proprietà fondamentali.

Definizione 0.29. L'insieme dei numeri naturali $\mathbb{N}$ è un insieme che soddisfa i seguenti cinque assiomi:

1. *Esistenza dello zero*: 0 è un numero naturale ($0 \in \mathbb{N}$).
2. *Esistenza del successivo*: Esiste una funzione $\sigma : \mathbb{N} \to \mathbb{N}$ (detta funzione successivo) che associa ad ogni numero n il suo successivo $\sigma(n)$.
3. *Iniettività*: La funzione σ è iniettiva.
$$\forall n, m \in \mathbb{N},\ \sigma(n) = \sigma(m) \implies n = m$$
(Numeri diversi hanno successivi diversi).
4. *Elemento minimo*: Lo zero non è il successivo di alcun numero naturale.
$$0 \notin \sigma(\mathbb{N}) \quad (\text{ovvero } \nexists n \in \mathbb{N} : \sigma(n) = 0)$$
5. *Principio di Induzione*: Se un sottoinsieme $A \subseteq \mathbb{N}$ contiene lo zero ed è chiuso rispetto all'operazione di successione (cioè se contiene un numero, contiene anche il suo successivo), allora A coincide con tutto $\mathbb{N}$.
$$(0 \in A \ \wedge\ \sigma(A) \subseteq A) \implies A = \mathbb{N}$$

Caratterizzazione dei Naturali non nulli Il quarto assioma ci dice che 0 non è nell'immagine della funzione σ. Ci chiediamo: l'immagine $\sigma(\mathbb{N})$ copre tutti gli altri numeri? La risposta è sì.

Proposizione 0.26. *Sia $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ l'insieme dei numeri naturali non nulli. Allora:*

$$\mathbb{N}^* = \sigma(\mathbb{N})$$

In altre parole, ogni numero diverso da zero è il successivo di qualche numero.

Proof. Consideriamo l'insieme A definito come l'unione dello zero e dell'immagine della funzione successivo:

$$A = \{0\} \cup \sigma(\mathbb{N})$$

Per costruzione, $A \subseteq \mathbb{N}$. Vogliamo dimostrare che $A = \mathbb{N}$ utilizzando il quinto assioma (induzione).

1. *Base:* $0 \in A$ per definizione stessa di A.
2. *Passo induttivo:* Dobbiamo mostrare che $\sigma(A) \subseteq A$. Sappiamo che $A \subseteq \mathbb{N}$, quindi applicando la funzione σ otteniamo $\sigma(A) \subseteq \sigma(\mathbb{N})$. Ma $\sigma(\mathbb{N})$ è un sottoinsieme di A (poiché $A = \{0\} \cup \sigma(\mathbb{N})$). Quindi, per transitività: $\sigma(A) \subseteq \sigma(\mathbb{N}) \subseteq A$.

Poiché A soddisfa le condizioni del Principio di Induzione, concludiamo che $A = \mathbb{N}$. Abbiamo quindi:

$$\mathbb{N} = \{0\} \cup \sigma(\mathbb{N})$$

Dato che per il quarto assioma $0 \notin \sigma(\mathbb{N})$, questa è un'unione disgiunta. Sottraendo $\{0\}$ da entrambi i membri otteniamo:

$$\mathbb{N} \setminus \{0\} = \sigma(\mathbb{N})$$

□

Definizioni per Induzione (o per Ricorrenza) Il principio di induzione non serve solo per dimostrare proprietà, ma è lo strumento fondamentale per *definire* concetti che dipendono da un parametro naturale n.

Supponiamo di voler definire un oggetto o una proprietà $D(n)$ per ogni $n \in \mathbb{N}$. Il procedimento standard consiste nel: 1. Definire il caso base $D(0)$. 2. Definire il caso generico $D(\sigma(n))$ supponendo di aver già definito $D(n)$.

Esempio 0.25. *Potenze in un monoide.* Sia $(S, \cdot)$ un monoide con elemento neutro 1_S e sia $x \in S$. Vogliamo definire la potenza x^n. La definizione per ricorrenza è:

$$\begin{cases} x^0 = 1_S & \text{(Base)} \\ x^{n+1} = x^n \cdot x & \text{(Passo ricorsivo, dove } n+1 \text{ sta per } \sigma(n)) \end{cases}$$

Giustificazione teorica Perché siamo sicuri che questa procedura definisca $D(n)$ per *tutti* i numeri naturali senza lasciare buchi o ambiguità? Ce lo garantisce proprio il Principio di Induzione.

Consideriamo l'insieme A costituito dai numeri naturali per i quali la definizione è ben posta:

$$A = \{n \in \mathbb{N} \mid D(n) \text{ è definita}\} \subseteq \mathbb{N}$$

- $0 \in A$: infatti abbiamo dato esplicitamente la definizione per $D(0)$.
- Supponiamo che $n \in A$ (cioè $D(n)$ è data). La regola ricorsiva ci spiega come costruire $D(\sigma(n))$ a partire da $D(n)$. Poiché $D(n)$ esiste, allora possiamo costruire $D(\sigma(n))$. Ne consegue che $\sigma(n) \in A$. In termini insiemistici: $\sigma(A) \subseteq A$.

Per il Principio di Induzione, $A = \mathbb{N}$. Dunque, per ogni $m \in \mathbb{N}$, la definizione $D(m)$ è validamente assegnata.

Dimostrazioni per Induzione L'utilità principale del quinto assioma di Peano risiede nella possibilità di dimostrare che una certa proprietà $E(n)$ è valida per tutti i numeri naturali. Il metodo procede in due step logici:

1. **Base dell'Induzione:** Si verifica che l'enunciato sia vero per il primo numero, $E(0)$.
2. **Passo Induttivo:** Si dimostra l'implicazione $E(n) \implies E(n+1)$ (o $E(\sigma(n))$). Ovvero, si suppone che l'enunciato sia vero per un generico n (*Ipotesi Induttiva*) e si prova che, di conseguenza, deve essere vero anche per il successivo $n+1$ (*Tesi*).

La giustificazione insiemistica è immediata: se chiamiamo A l'insieme dei numeri per cui E è vera, la base ci dice che $0 \in A$, e il passo induttivo ci dice che A è chiuso rispetto al successivo ($\sigma(A) \subseteq A$). Per l'assioma di Peano, allora $A = \mathbb{N}$.

Esempio 0.26. Somma dei primi n numeri naturali Vogliamo dimostrare la formula di Gauss:

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}$$

1. Base dell'induzione ($n = 0$) Sostituiamo $n = 0$ nella formula:

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

L'uguaglianza è verificata.

2. Passo Induttivo Supponiamo vera l'ipotesi per n:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \quad \text{(Ipotesi Induttiva)}$$

Vogliamo dimostrare la tesi per $n + 1$:

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

Procediamo sommando il termine successivo alla somma parziale:

$$\underbrace{0 + 1 + \cdots + n}_{\text{somma fino a } n} + (n+1)$$

Usando l'ipotesi induttiva, sostituiamo la somma fino a n:

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

Facciamo il denominatore comune:

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

Raccogliamo il fattore comune $(n + 1)$:

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

La tesi è dimostrata.

Esempio 0.27. Somma dei primi m numeri dispari Dimostriamo che la somma dei primi m numeri dispari è uguale al quadrato di m:

$$1 + 3 + \cdots + (2m-1) = m^2 \quad \forall m \in \mathbb{N}, m \geq 1$$

1. Base dell'induzione ($m = 1$)

$$1 = 1^2 \implies 1 = 1 \quad \text{(Vero)}$$

2. Passo Induttivo Ipotesi $E(n)$: $1 + \cdots + (2n-1) = n^2$. Tesi $E(n+1)$: La somma fino al successivo dispari $(2(n+1)-1)$ deve fare $(n+1)^2$.

$$\underbrace{1 + \cdots + (2n-1)}_{\text{Ipotesi}} + (2n + 2 - 1) = n^2 + (2n+1)$$

Riconosciamo il quadrato del binomio:

$$= n^2 + 2n + 1 = (n+1)^2$$

La tesi è dimostrata per ogni $m \geq 1$.

Definizione delle Operazioni in $\mathbb{N}$ Dopo aver definito i naturali assiomaticamente, dobbiamo definire le operazioni aritmetiche (somma, prodotto) usando solo la funzione successivo σ. Questo si fa per induzione (ricorrenza).

Definizione 0.30. Fissato un numero $a \in \mathbb{N}$, definiamo l'applicazione **Traslazione** $T_a : \mathbb{N} \to \mathbb{N}$ mediante le due condizioni:

1. $T_a(0) = a$ (Spostare 0 di a passi porta in a)
2. $T_a(\sigma(x)) = \sigma(T_a(x))$ (La traslazione del successivo è il successivo della traslazione)

Questa definizione ci permette di definire formalmente l'addizione.

Definizione 0.31. Dati due numeri naturali a, b, definiamo la loro **c**ome l'applicazione della traslazione di a al numero b:

$$a + b := T_a(b)$$

Esplicitando le proprietà ricorsive della traslazione, otteniamo le regole operative della somma:

1. $a + 0 = a$ (Elemento neutro a destra)
2. $a + \sigma(b) = \sigma(a + b)$ (La somma col successivo è il successivo della somma) *Equivalentemente:* $a + (b + 1) = (a + b) + 1$

L'addizione diventa quindi un'operazione binaria interna a $\mathbb{N}$:

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a + b$$

Struttura algebrica dei Naturali Vogliamo dimostrare che l'insieme dei numeri naturali $\mathbb{N}$, dotato dell'operazione di somma definita per ricorrenza, possiede una struttura ben precisa.

Proposizione 0.27. *La struttura* $(\mathbb{N}, +)$ *è un monoide commutativo.*

Per affermarlo dobbiamo verificare tre proprietà:

1. Esistenza dell'elemento neutro.
2. Proprietà Associativa.
3. Proprietà Commutativa.

1. Elemento Neutro Dalla definizione ricorsiva di somma sappiamo già che $x + 0 = x$ per ogni x (lo zero è neutro a destra). Dobbiamo dimostrare che lo è anche a sinistra.

Proposizione 0.28. *Lo zero è l'elemento neutro di* $(\mathbb{N}, +)$*, ovvero:*

$$\forall x \in \mathbb{N},\ x + 0 = x = 0 + x$$

Proof. La parte destra $x + 0 = x$ è vera per definizione. Dimostriamo la parte sinistra $0 + x = x$ per induzione su x.

Base Induttiva ($x = 0$): Dobbiamo verificare che $0 + 0 = 0$. Applicando la definizione di somma ($a + 0 = a$) con $a = 0$, otteniamo $0 + 0 = 0$. L'uguaglianza è verificata.

Passo Induttivo: Supponiamo vero l'enunciato per m (*Ipotesi*): $0 + m = m$. Vogliamo dimostrarlo per $\sigma(m)$ (*Tesi*): $0 + \sigma(m) = \sigma(m)$.

Dimostrazione:

$$0 + \sigma(m) \underset{\text{Def. somma}}{=} \sigma(0 + m) \underset{\text{Ip. Ind.}}{=} \sigma(m)$$

La tesi è dimostrata. Quindi 0 è elemento neutro bilatero. □

2. Proprietà Associativa Passiamo ora alla proprietà che permette di non usare parentesi nelle somme multiple.

Proposizione 0.29. *L'addizione è associativa:*

$$(a+b)+c = a+(b+c) \quad \forall a,b,c \in \mathbb{N}$$

Proof. Procediamo per induzione sulla variabile c.
Base Induttiva ($c=0$): Dobbiamo verificare che $(a+b)+0 = a+(b+0)$.

- Membro sinistro: $(a+b)+0 = a+b$ (per definizione di somma).
- Membro destro: $a+(b+0) = a+b$ (per definizione di somma interna).

L'uguaglianza regge.
Passo Induttivo: *Ipotesi*: $(a+b)+m = a+(b+m)$. *Tesi*: $(a+b)+\sigma(m) = a+(b+\sigma(m))$.
Dimostrazione: Partiamo dal membro sinistro:

$$(a+b)+\sigma(m) \underset{\text{Def. somma}}{=} \sigma((a+b)+m)$$

Usiamo l'ipotesi induttiva sull'argomento:

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

Ora guardiamo il membro destro della tesi. Per definizione di somma ($x+\sigma(y) = \sigma(x+y)$):

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

Le due espressioni coincidono. □

3. Proprietà preliminare dell'unità Prima di dimostrare la commutatività, definiamo $1 = \sigma(0)$ e dimostriamo un lemma utile: sommare 1 equivale a prendere il successivo.

Proposizione 0.30. *Per ogni $x \in \mathbb{N}$ vale:*

$$x+1 = \sigma(x) \quad e \quad 1+x = \sigma(x)$$

Proof. Caso 1: $x+1 = \sigma(x)$

$$x+1 = x+\sigma(0) \underset{\text{Def. somma}}{=} \sigma(x+0) = \sigma(x)$$

Vero per definizione.
Caso 2: $1+x = \sigma(x)$ Dimostriamo per induzione su x.

- *Base* ($x=0$): $1+0 = 1 = \sigma(0)$. Vero.
- *Passo Induttivo*: *Ipotesi*: $1+m = \sigma(m)$. *Tesi*: $1+\sigma(m) = \sigma(\sigma(m))$. Calcolo:

$$1+\sigma(m) \underset{\text{Def. somma}}{=} \sigma(1+m) \underset{\text{Ip. Ind.}}{=} \sigma(\sigma(m))$$

La tesi è verificata. □

4. Proprietà Commutativa Infine, dimostriamo che l'ordine degli addendi non conta.

Proposizione 0.31. *L'addizione è commutativa:*

$$a+b = b+a \quad \forall a,b \in \mathbb{N}$$

Proof. Procediamo per induzione su b (fissando a).

Base Induttiva ($b = 0$): Dobbiamo verificare $a + 0 = 0 + a$. Sappiamo che $a + 0 = a$ e abbiamo dimostrato al punto 1 che $0 + a = a$. Quindi l'uguaglianza è vera.

Passo Induttivo: *Ipotesi*: $a + m = m + a$. *Tesi*: $a + \sigma(m) = \sigma(m) + a$.

Dimostrazione: Sviluppiamo il membro sinistro usando la definizione di somma e il lemma precedente ($\sigma(x) = x + 1$):

$$a + \sigma(m) = a + (m + 1)$$

Usiamo l'associatività:

$$= (a + m) + 1$$

Usiamo l'ipotesi induttiva (scambiamo $a + m$ con $m + a$):

$$= (m + a) + 1$$

Usiamo di nuovo l'associatività:

$$= m + (a + 1)$$

Usiamo il lemma per scambiare $a + 1$ con $1 + a$:

$$= m + (1 + a)$$

Associatività ancora:

$$= (m + 1) + a$$

Riscriviamo $m + 1$ come $\sigma(m)$:

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

Abbiamo ottenuto il membro destro della tesi. □

Ulteriori Proprietà di $(\mathbb{N}, +)$ Esploriamo ora alcune proprietà cruciali che legano l'addizione alla struttura di $\mathbb{N}$, come la legge di annullamento e la cancellazione.

Proposizione 0.32. ***Legge di annullamento della somma*** *In $\mathbb{N}$, una somma è zero se e solo se entrambi gli addendi sono zero.*

$$x + y = 0 \iff x = 0 \ \wedge \ y = 0$$

Proof. La dimostrazione procede per doppia implicazione. ($\Longleftarrow$) Se $x = 0$ e $y = 0$, allora $x + y = 0 + 0 = 0$ (banale).

($\Longrightarrow$) Supponiamo per assurdo che $x + y = 0$ ma $y \neq 0$. Se $y \neq 0$, allora $y \in \mathbb{N}^*$. Per la caratterizzazione dei naturali non nulli ($\mathbb{N}^* = \sigma(\mathbb{N})$), esiste un $z \in \mathbb{N}$ tale che $y = \sigma(z)$. Sostituendo nell'equazione:

$$0 = x + y = x + \sigma(z) = \sigma(x + z)$$

Questo implica che $0 \in \sigma(\mathbb{N})$, ovvero che lo zero è il successivo di qualcuno. Ma questo contraddice il 4° assioma di Peano. Dunque deve essere necessariamente $y = 0$. Sostituendo $y = 0$ nell'equazione originale: $x + 0 = 0 \implies x = 0$. □

Proposizione 0.33. ***Iniettività della Traslazione (Legge di Cancellazione)*** *L'applicazione traslazione $T_a(x) = a + x$ è iniettiva per ogni $a \in \mathbb{N}$.*

$$a + x = a + y \implies x = y$$

Proof. Procediamo per induzione su a. Sia $E(a)$ l'enunciato "T_a è iniettiva".

Base Induttiva ($a = 0$) Dobbiamo provare che T_0 è iniettiva. Sappiamo che $T_0(x) = 0 + x = x$. Quindi T_0 coincide con l'identità $id_{\mathbb{N}}$, che è banalmente iniettiva.

Passo Induttivo Ipotesi $E(m)$: T_m è iniettiva ($m + x = m + y \implies x = y$). Tesi $E(m + 1)$: T_{m+1} è iniettiva ($(m + 1) + x = (m + 1) + y \implies x = y$).

Siano $x, y \in \mathbb{N}$ tali che $T_{m+1}(x) = T_{m+1}(y)$.

$$(m + 1) + x = (m + 1) + y$$

Ricordando che $m + 1 = 1 + m$ (proprietà commutativa e definizione di 1), possiamo riscrivere come:

$$m + (1 + x) = m + (1 + y)$$

Riconosciamo l'azione di T_m:

$$T_m(1 + x) = T_m(1 + y)$$

Per l'ipotesi induttiva, T_m è iniettiva, quindi possiamo "cancellare" T_m:

$$1 + x = 1 + y$$

Ricordando che $1 + z = \sigma(z)$:

$$\sigma(x) = \sigma(y)$$

Per il 3° assioma di Peano, σ è iniettiva, quindi:

$$x = y$$

La tesi è dimostrata. □

Nota 12. Osserviamo una relazione interessante tra le traslazioni:

$$T_{m+1} = T_m \circ \sigma = \sigma \circ T_m$$

Verifica:

- $T_{m+1}(x) = (m + 1) + x = m + (1 + x) = m + \sigma(x) = T_m(\sigma(x))$.
- $(\sigma \circ T_m)(x) = \sigma(m + x) = (m + x) + 1 = 1 + (m + x) = (1 + m) + x = (m + 1) + x$.

Potenza in un Monoide Estendiamo il concetto di operazione ripetuta definendo la potenza ad esponente naturale in una struttura algebrica generale.

Definizione 0.32. Sia $(S, \cdot)$ un monoide con elemento neutro 1_S. Per ogni $x \in S$ e $n \in \mathbb{N}$, definiamo la potenza x^n per ricorrenza:

$$\begin{cases} x^0 = 1_S \\ x^{n+1} = x^n \cdot x \end{cases}$$

Proprietà delle Potenze La prima proprietà fondamentale è la regola della somma degli esponenti.

Proposizione 0.34. *Per ogni $x \in S$ e per ogni $r, s \in \mathbb{N}$, vale:*

$$x^r \cdot x^s = x^{r+s}$$

Proof. Fissiamo r e procediamo per induzione su s. Sia $E(s)$ l'uguaglianza da dimostrare.

Base Induttiva ($s = 0$) Dobbiamo verificare che $x^r \cdot x^0 = x^{r+0}$.

- Membro sinistro: $x^r \cdot x^0 = x^r \cdot 1_S = x^r$ (per def. di potenza e neutro).
- Membro destro: $x^{r+0} = x^r$ (per def. di somma).

L'uguaglianza regge.

Passo Induttivo Ipotesi $E(m)$: $x^r \cdot x^m = x^{r+m}$. Tesi $E(m + 1)$: $x^r \cdot x^{m+1} = x^{r+(m+1)}$.

Dimostrazione: Partiamo dal membro destro della tesi:

$$x^{r+(m+1)}$$

Per l'associatività della somma in $\mathbb{N}$, $r + (m + 1) = (r + m) + 1$.

$$= x^{(r+m)+1}$$

Per la definizione ricorsiva di potenza ($y^{k+1} = y^k \cdot x$):

$$= x^{r+m} \cdot x$$

Ora usiamo l'ipotesi induttiva per riscrivere x^{r+m}:

$$= (x^r \cdot x^m) \cdot x$$

Per l'associatività del prodotto nel monoide S:

$$= x^r \cdot (x^m \cdot x)$$

Per la definizione ricorsiva di potenza ($x^m \cdot x = x^{m+1}$):

$$= x^r \cdot x^{m+1}$$

Abbiamo ottenuto il membro sinistro. La proprietà è dimostrata. □

Potenza di un Prodotto Attenzione: la regola $(ab)^n = a^n b^n$ **non vale in generale** nei gruppi/monoidi. Vale solo se a e b commutano ($ab = ba$).

Esempio 0.28. Controesempio nel gruppo simmetrico S_3 (non commutativo). Siano $\alpha = (12)$ e $\beta = (23)$. Scegliamo $n = 2$.

- Calcoliamo separatamente le potenze: $\alpha^2 = id$ (è uno scambio). $\beta^2 = id$ (è uno scambio). Quindi $\alpha^2 \circ \beta^2 = id \circ id = id$.
- Calcoliamo la potenza del prodotto: $\alpha \circ \beta = (12)(23) = (123)$. $(\alpha \circ \beta)^2 = (123)^2 = (132)$.

Poiché $(132) \neq id$, abbiamo mostrato che $(\alpha\beta)^2 \neq \alpha^2\beta^2$.

Proprietà delle potenze di elementi permutabili Se in un monoide due elementi commutano tra loro ($ab = ba$), questo comportamento si riflette sulle loro potenze.

Lemma 0.35. *Sia $(S, \cdot)$ un monoide e siano $a, b \in S$. Se $ab = ba$, allora a commuta con qualsiasi potenza di b:*

$$ab^r = b^r a \quad \forall r \in \mathbb{N}$$

Proof. Procediamo per induzione su r.

- **Base ($r = 0$):** $a \cdot b^0 = a \cdot 1_S = a$ e $b^0 \cdot a = 1_S \cdot a = a$. Vero.
- **Passo Induttivo:** Ipotesi $ab^m = b^m a$. Tesi $ab^{m+1} = b^{m+1}a$.

$$ab^{m+1} = a(b^m b) = (ab^m)b \underset{\text{Ip.}}{=} (b^m a)b = b^m(ab) \underset{\text{Comm.}}{=} b^m(ba) = (b^m b)a = b^{m+1}a$$

La tesi è dimostrata. □

Dal lemma precedente segue immediatamente che potenze arbitrarie di elementi commutativi commutano tra loro:

$$ab = ba \implies a^s b^r = b^r a^s \quad \forall r, s \in \mathbb{N}$$

(Basta applicare il lemma scambiando i ruoli di a e b).

Proposizione 0.36. ***Potenza di un prodotto*** *Sia $(S, \cdot)$ un monoide. Se $a, b \in S$ commutano ($ab = ba$), allora:*

$$(ab)^n = a^n b^n \quad \forall n \in \mathbb{N}$$

Proof. Dimostrazione per induzione su n.

- **Base ($n = 0$):** $(ab)^0 = 1_S$ e $a^0 b^0 = 1_S \cdot 1_S = 1_S$. Vero.

- **Passo Induttivo:** Ipotesi $(ab)^m = a^m b^m$. Tesi $(ab)^{m+1} = a^{m+1}b^{m+1}$.

$$(ab)^{m+1} = (ab)^m(ab) \underset{\text{Ip.}}{=} (a^m b^m)(ab) = a^m(b^m a)b$$

Sfruttando il lemma ($b^m a = ab^m$):

$$= a^m(ab^m)b = (a^m a)(b^m b) = a^{m+1}b^{m+1}$$

La tesi è dimostrata. □

Relazione tra Successivo e Traslazione in $\mathbb{N}$ Nel monoide delle funzioni da $\mathbb{N}$ in $\mathbb{N}$, $(M(\mathbb{N}), \circ)$, esiste una relazione interessante tra la funzione successivo σ e la traslazione T_m.

Ricordiamo le definizioni:

- $\sigma(x) = x + 1$
- $T_m(x) = m + x$

Proposizione 0.37. *La traslazione T_m coincide con la potenza m-esima della funzione successivo (rispetto alla composizione):*

$$\sigma^n = T_n \quad \forall n \in \mathbb{N}$$

Proof. Dimostriamo $E(m) : \sigma^m = T_m$ per induzione su m.

Base ($m = 0$): $\sigma^0 = id_{\mathbb{N}}$ (per def. di potenza 0). $T_0(x) = 0 + x = x$, quindi $T_0 = id_{\mathbb{N}}$. L'uguaglianza è verificata.

Passo Induttivo: Ipotesi $\sigma^m = T_m$. Tesi $\sigma^{m+1} = T_{m+1}$. Valutiamo le funzioni su un generico $x \in \mathbb{N}$:

$$\sigma^{m+1}(x) = (\sigma^m \circ \sigma)(x) = \sigma^m(\sigma(x))$$

Per ipotesi induttiva $\sigma^m = T_m$:

$$= T_m(\sigma(x)) = T_m(1 + x)$$

Per definizione di T_m:

$$= m + (1 + x)$$

Per proprietà associativa e commutativa della somma:

$$= (m + 1) + x$$

Che corrisponde esattamente alla definizione di $T_{m+1}(x)$. □

Multipli in Monoidi Additivi Quando lavoriamo con un monoide in notazione additiva $(A, +)$ (con neutro 0_A), il concetto di potenza x^n viene tradotto nel concetto di **multiplo**.

La notazione esponenziale x^n diventa $n \cdot x$ (o nx).

$$\begin{cases} x^0 = 1_S & \longrightarrow \quad 0 \cdot x = 0_A \\ x^{n+1} = x^n \cdot x & \longrightarrow \quad (n+1) \cdot x = n \cdot x + x \end{cases}$$

Nota 13. Attenzione a non confondere i simboli:

- $n \in \mathbb{N}$ è il moltiplicatore (numero naturale).
- $x \in A$ è l'elemento del monoide.

Proprietà dei Multipli Le proprietà delle potenze si traducono nelle seguenti regole per i multipli:

1. Somma dei moltiplicatori:

$$r \cdot a + s \cdot a = (r + s) \cdot a$$

(Corrisponde a $x^r \cdot x^s = x^{r+s}$). Vale per ogni $a \in A$ e $r, s \in \mathbb{N}$.

2. Multiplo di una somma: Se il monoide A è commutativo ($a + b = b + a$), allora vale:

$$m \cdot (a + b) = m \cdot a + m \cdot b$$

(Corrisponde a $(xy)^n = x^n y^n$).

Applicazione ai Numeri Naturali Poiché $(\mathbb{N}, +)$ è un monoide commutativo, possiamo applicare queste definizioni ponendo $A = \mathbb{N}$. In questo caso, il prodotto scalare $m \cdot x$ coincide esattamente con la moltiplicazione tra numeri naturali.

Le proprietà sopra elencate diventano le proprietà distributive della moltiplicazione rispetto all'addizione in $\mathbb{N}$:

- $r \cdot a + s \cdot a = (r + s) \cdot a$ (Distributiva a destra)
- $m \cdot (a + b) = m \cdot a + m \cdot b$ (Distributiva a sinistra)

Proprietà della Potenza di Potenza Un'altra proprietà fondamentale delle potenze in un monoide $(S, \cdot)$ è la seguente.

Proposizione 0.38. *Per ogni $x \in S$ e per ogni $r, s \in \mathbb{N}$, vale la regola:*

$$(x^r)^s = x^{r \cdot s}$$

Proof. Procediamo per induzione su s (fissando r).

1. **Base Induttiva ($s = 0$)** Membro sinistro: $(x^r)^0 = 1_S$ (def. di potenza 0). Membro destro: $x^{r \cdot 0} = x^0 = 1_S$ (poiché $r \cdot 0 = 0$). L'uguaglianza regge.
2. **Passo Induttivo** Ipotesi $E(m)$: $(x^r)^m = x^{r \cdot m}$. Tesi $E(m+1)$: $(x^r)^{m+1} = x^{r \cdot (m+1)}$.
   Dimostrazione:
   $$(x^r)^{m+1} = (x^r)^m \cdot x^r$$
   Per ipotesi induttiva:
   $$= x^{r \cdot m} \cdot x^r$$
   Per la regola della somma degli esponenti ($a^h \cdot a^k = a^{h+k}$):
   $$= x^{r \cdot m + r}$$
   Per la proprietà distributiva in $\mathbb{N}$:
   $$= x^{r \cdot m + r \cdot 1} = x^{r(m+1)}$$
   La tesi è dimostrata.

□

Proprietà del Prodotto in $\mathbb{N}$ Nella dimostrazione precedente abbiamo usato implicitamente alcune proprietà del prodotto in $\mathbb{N}$. Vediamole formalmente.

Lemma 0.39. *Valgono le seguenti proprietà dello zero e dell'uno rispetto al prodotto:*

1. $r \cdot 0 = 0 \quad \forall r \in \mathbb{N}$
2. $r \cdot 1 = r \quad \forall r \in \mathbb{N}$

Proof. **1) Dimostrazione di $r \cdot 0 = 0$** Non possiamo usare la commutatività (non ancora dimostrata). Usiamo la proprietà distributiva e la cancellazione. Sappiamo che $0 + 0 = 0$. Moltiplichiamo a sinistra per r:

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

Aggiungiamo 0 a sinistra:

$$0 + r \cdot 0 = r \cdot 0 + r \cdot 0$$

Per la legge di cancellazione della somma, otteniamo $0 = r \cdot 0$.

2) Dimostrazione di $r \cdot 1 = r$ Per induzione su r. Base ($r = 0$): $0 \cdot 1 = 0$ (per definizione di prodotto $0 \cdot x = 0$). Passo ($m \to m + 1$):

$$(m + 1) \cdot 1 = m \cdot 1 + 1$$

Per ipotesi induttiva $m \cdot 1 = m$:

$$= m + 1$$

La tesi è dimostrata. □

Commutatività del Prodotto in $\mathbb{N}$ Siamo ora pronti per dimostrare che $(\mathbb{N}, \cdot)$ è un monoide commutativo.

Proposizione 0.40. *Il prodotto in $\mathbb{N}$ è commutativo:*

$$m \cdot n = n \cdot m \quad \forall m, n \in \mathbb{N}$$

Proof. Procediamo per induzione su m (fissando n). Sia x al posto di n per chiarezza. Enunciato $E(m) : m \cdot x = x \cdot m$.

Base Induttiva ($m = 0$) Dobbiamo provare $0 \cdot x = x \cdot 0$. $0 \cdot x = 0$ (per definizione). $x \cdot 0 = 0$ (per il Lemma L_0 dimostrato sopra). Quindi $0 = 0$, vero.

Passo Induttivo Ipotesi $E(m) : m \cdot x = x \cdot m$. Tesi $E(m+1) : (m+1) \cdot x = x \cdot (m+1)$.

Sviluppiamo il membro sinistro:

$$(m+1) \cdot x = m \cdot x + x$$

Per ipotesi induttiva:

$$= x \cdot m + x$$

Ricordando che $x = x \cdot 1$ (Lemma L_1):

$$= x \cdot m + x \cdot 1$$

Per la proprietà distributiva (a sinistra, che vale per definizione):

$$= x \cdot (m+1)$$

La tesi è dimostrata. □

Legge di Annullamento del Prodotto Un'altra proprietà cruciale è l'assenza di divisori dello zero.

Proposizione 0.41. *In $\mathbb{N}$, un prodotto è nullo se e solo se almeno uno dei fattori è nullo.*

$$x \cdot y = 0 \iff x = 0 \vee y = 0$$

Proof. ($\Longleftarrow$) Se uno è zero, il prodotto è zero (già visto).

($\Longrightarrow$) Supponiamo per assurdo che $x \cdot y = 0$ con $x \neq 0$ e $y \neq 0$. Se $y \neq 0$, allora y è un successore, diciamo $y = z + 1$. Sostituendo:

$$x \cdot (z+1) = 0$$

$$xz + x = 0$$

Per la legge di annullamento della somma, questo implica $xz = 0$ e, soprattutto, $x = 0$. Ma questo contraddice l'ipotesi $x \neq 0$. Quindi non è possibile avere entrambi i fattori non nulli. □

Invertibili in $(\mathbb{N}, \cdot)$ Chi sono gli elementi invertibili rispetto alla moltiplicazione?

Proposizione 0.42. *L'unico numero naturale invertibile rispetto al prodotto è 1.*

$$U(\mathbb{N}, \cdot) = \{1\}$$

Proof. ($\Longleftarrow$) Ovvio: $1 \cdot 1 = 1$, quindi $1 \in U(\mathbb{N}, \cdot)$.

($\Longrightarrow$) Supponiamo che x sia invertibile. Esiste quindi $y \in \mathbb{N}$ tale che $x \cdot y = 1$. Ovviamente $x \neq 0$ (altrimenti il prodotto sarebbe 0), quindi x deve essere un successore. Esiste cioè $z \in \mathbb{N}$ tale che $x = z + 1$. Sostituiamo nell'equazione:

$$1 = x \cdot y = (z+1)y = zy + y$$

A questo punto per concludere rigorosamente serve la teoria dell'ordine (che implica che se $zy + y = 1$, allora $y \leq 1$). Assumendo le proprietà dell'ordine:

- Dall'equazione segue che $y \leq 1$.
- Poiché $xy = 1$, deve essere $y \neq 0$, quindi $0 < y$, ovvero $1 \leq y$ (per il lemma sui numeri interi positivi).

Per la proprietà antisimmetrica ($y \leq 1$ e $1 \leq y$), si conclude che $y = 1$. Sostituendo all'indietro:

$$1 = x \cdot y = x \cdot 1 = x$$

Quindi $x = 1$. □

Proprietà delle Relazioni Sia $X \neq \emptyset$ un insieme. Una relazione binaria R è un sottoinsieme del prodotto cartesiano, $R \subseteq X \times X$. Scriviamo $(a, b) \in R$ oppure aRb.

Definizione 0.33. Una relazione R può godere delle seguenti proprietà:

- *Riflessiva*: $\forall a \in X,\ aRa$.
- *Transitiva*: $\forall a, b, c \in X$, se aRb e bRc, allora aRc.
- *Simmetrica*: $\forall a, b \in X$, se aRb, allora bRa.
- *Antisimmetrica*: $\forall a, b \in X$, se aRb e bRa, allora $a = b$.

Classificazione delle Relazioni Combinando queste proprietà otteniamo due tipologie fondamentali di relazioni.

Definizione 0.34.
1. **Relazione d'Ordine**: Riflessiva, Transitiva, Antisimmetrica.
2. **Relazione di Equivalenza**: Riflessiva, Transitiva, Simmetrica.

Relazione Trasposta (o Inversa)

Definizione 0.35. Data una relazione R, definiamo la sua trasposta R^t (o R^T) come:

$$(a, b) \in R^t \iff (b, a) \in R$$

Nota 14. Se R è una relazione di equivalenza, per la proprietà simmetrica abbiamo che $aRb \iff bRa$. Di conseguenza, $R = R^t$.

Cosa accade invece se R è una relazione d'ordine? La sua trasposta R^t è ancora una relazione d'ordine (detta ordine duale o inverso).

Proposizione 0.43. *Se R è una relazione d'ordine su X, allora anche R^t è una relazione d'ordine su X.*

Proof. Verifichiamo le tre proprietà per R^t:

- *Riflessiva*: Poiché R è riflessiva, aRa per ogni a. Dunque $(a, a) \in R$, che implica $(a, a) \in R^t$, ovvero aR^ta.
- *Transitiva*: Siano aR^tb e bR^tc. Per definizione, significa bRa e cRb. Poiché R è transitiva, cRa. Questo implica aR^tc.
- *Antisimmetrica*: Siano aR^tb e bR^ta. Allora bRa e aRb. Poiché R è antisimmetrica, segue necessariamente $a = b$.

□

Esempio 0.29. In $\mathbb{N}$, se R è la relazione $\leq$, allora R^t è la relazione $\geq$.

Relazione d'Ordine Stretto Una relazione d'ordine stretto (spesso indicata con $<$) soddisfa proprietà diverse rispetto all'ordine largo.

Definizione 0.36. Una relazione $R \subseteq X \times X$ è di *ordine stretto* se è:

- *Transitiva*: $aRb \wedge bRc \implies aRc$.
- *Irriflessiva*: $\forall a \in X,\ (a,a) \notin R$ (nessun elemento è in relazione con se stesso).
- *Asimmetrica*: Se aRb, allora $b \not R a$. In termini insiemistici: $R \cap R^t = \emptyset$.

Classi di Equivalenza

Definizione 0.37. Sia R una relazione di equivalenza su X. Si definisce **classe di equivalenza** di un elemento $a \in X$ l'insieme:

$$[a]_R = \{x \in X \mid xRa\}$$

Per la simmetria, vale anche $[a]_R = \{x \in X \mid aRx\}$. Grazie alla riflessività, ogni elemento appartiene alla propria classe: $a \in [a]_R$.

Proposizione 0.44. *Due classi di equivalenza o sono disgiunte o coincidono.*

$$[a]_R \cap [b]_R \neq \emptyset \implies [a]_R = [b]_R$$

Proof. Supponiamo che l'intersezione non sia vuota. Sia $c \in [a]_R \cap [b]_R$. Allora cRa e cRb. Per simmetria aRc. Per transitività (aRc e cRb), otteniamo aRb. *Dimostriamo l'uguaglianza per doppia inclusione:* 1) Sia $x \in [a]_R$. Allora xRa. Poiché abbiamo provato aRb, per transitività xRb, quindi $x \in [b]_R$. ($\implies [a]_R \subseteq [b]_R$). 2) Sia $y \in [b]_R$. Allora yRb. Poiché $aRb \implies bRa$, abbiamo yRb e bRa, quindi yRa, cioè $y \in [a]_R$. ($\implies [b]_R \subseteq [a]_R$). Conclusione: $[a]_R = [b]_R$. □

Nota 15. Abbiamo dimostrato un risultato fondamentale: $aRb \iff [a]_R = [b]_R$. Un elemento qualsiasi $x \in [a]_R$ si dice *rappresentante* della classe.

Insieme Quoziente e Partizioni

Definizione 0.38. L'insieme di tutte le classi di equivalenza prende il nome di *Insieme Quoziente*, denotato con X/R:

$$\frac{X}{R} = \{[a]_R \mid a \in X\}$$

Le classi di equivalenza formano una *partizione* di X: sono sottoinsiemi non vuoti, a due a due disgiunti, la cui unione è tutto X.

Proiezione Canonica

Definizione 0.39. È l'applicazione che associa ad ogni elemento la sua classe.

$$\pi : X \longrightarrow \frac{X}{R}, \quad a \longmapsto [a]_R$$

Nota 16. La proiezione canonica è sempre suriettiva. Vale l'equivalenza:

$$\pi(a) = \pi(b) \iff [a]_R = [b]_R \iff aRb.$$

Sistema Completo di Rappresentanti (S.C.R.)

Definizione 0.40. Un sottoinsieme $T \subseteq X$ è un S.C.R. per R se contiene esattamente un elemento per ogni classe di equivalenza:

$$\forall x \in X, \exists! t \in T : xRt$$

Relazione indotta da una funzione Ogni funzione genera naturalmente una relazione di equivalenza sul suo dominio.

Definizione 0.41. Sia $f : X \to Y$ un'applicazione. Definiamo la relazione nucleo R_f su X:

$$aR_f b \iff f(a) = f(b)$$

Proof. Verifichiamo che R_f è di equivalenza:

- *Riflessiva*: $f(a) = f(a)$ è banalmente vero.
- *Simmetrica*: Se $f(a) = f(b)$, allora $f(b) = f(a)$, quindi $bR_f a$.
- *Transitiva*: Se $f(a) = f(b)$ e $f(b) = f(c)$, per la transitività dell'uguaglianza $f(a) = f(c)$, quindi $aR_f c$.

□

Esempi Geometrici di Relazioni di Equivalenza Analizziamo come alcune funzioni $f : \mathbb{R}^2 \to \mathbb{R}$ inducano relazioni di equivalenza che corrispondono a luoghi geometrici noti nel piano cartesiano.

Esempio 0.30. Sia $X = \mathbb{R}^2$. Consideriamo la funzione che associa a ogni punto la sua distanza dall'origine:

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto \sqrt{x^2 + y^2} \end{aligned}$$

La relazione d'equivalenza indotta (nucleo) è:

$$(a, b)R(\alpha, \beta) \iff \sqrt{a^2 + b^2} = \sqrt{\alpha^2 + \beta^2}$$

Due punti sono in relazione se sono equidistanti dall'origine $O = (0, 0)$. Di conseguenza, la classe di equivalenza di un punto (a, b), indicata con $[(a, b)]_R$, corrisponde geometricamente alla *circonferenza* centrata nell'origine e passante per quel punto.

Se scegliamo come Sistema Completo di Rappresentanti (SCR) l'insieme T (semiasse positivo delle ascisse), possiamo stabilire una corrispondenza biunivoca tra l'insieme quoziente, i rappresentanti e i numeri reali.

Schematizziamo la catena di applicazioni:

$$\frac{X}{R} \longrightarrow T \longrightarrow \mathbb{R}$$

$$[(a, b)]_R \longmapsto (\sqrt{a^2 + b^2}, 0) \longmapsto \sqrt{a^2 + b^2}$$

Fascio di Rette Parallele

Esempio 0.31. Consideriamo ora la proiezione sulla prima coordinata:

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto x \end{aligned}$$

La relazione è definita da:

$$(a, b)R(\alpha, \beta) \iff a = \alpha$$

La classe di equivalenza di (a, b) è l'insieme di tutti i punti che hanno la stessa ascissa a, variando la y liberamente:

$$[(a, b)]_R = \{(a, \beta) \mid \beta \in \mathbb{R}\}$$

Geometricamente, queste classi sono rette verticali parallele all'asse y. Un possibile S.C.R. è l'asse delle ascisse (ogni retta verticale lo interseca in uno e un solo punto):

$$T = \{(a, 0) \mid a \in \mathbb{R}\}$$

L'insieme quoziente è in biiezione con $\mathbb{R}$ stesso tramite la mappa $[(a, b)] \mapsto a$.

Esempio 0.32. Sia $X = \mathbb{R}^2$ e consideriamo la funzione prodotto:

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto xy \end{aligned}$$

La relazione d'equivalenza indotta è:

$$(a, b)R(\alpha, \beta) \iff ab = \alpha\beta$$

Poniamo $c = ab$. La classe di equivalenza di (a, b) è il luogo geometrico dei punti tali che $xy = c$.

Analizziamo la geometria delle classi in base al valore di c:

1) Caso $c = 0$ (Assi Cartesiani) Se $c = 0$, l'equazione diventa $xy = 0$. Questo avviene se $x = 0$ oppure $y = 0$. Dunque la classe è l'unione dei due assi:

$$[(a, b)]_R = \{(0, y) \mid y \in \mathbb{R}\} \cup \{(x, 0) \mid x \in \mathbb{R}\}$$

2) Caso $c \neq 0$ (Iperboli) Se $c \neq 0$, la classe è un'iperbole equilatera con asintoti sugli assi.

- Se $c > 0$: Iperbole nel I e III quadrante.
- Se $c < 0$: Iperbole nel II e IV quadrante.

Ricerca del Sistema Completo di Rappresentanti (SCR) Vogliamo selezionare un unico punto rappresentativo per ogni classe. Una scelta geometricamente elegante è prendere il *vertice* dell'iperbole che ha ordinata positiva (o l'origine per il caso degenere). Questo corrisponde a intersecare le curve con il grafico della funzione valore assoluto:

$$y = |x|$$

Calcoliamo le intersezioni:

Se $c > 0$ (I quadrante, $y = x$):

$$\begin{cases} xy = c \\ y = x \end{cases} \implies x^2 = c \implies x = \sqrt{c} \quad \text{(poiché } x > 0 \text{ nel I quad.)}$$

Il punto è $(\sqrt{c}, \sqrt{c}) = (\sqrt{ab}, \sqrt{ab})$.

Se $c < 0$ (II quadrante, $y = -x$):

$$\begin{cases} xy = c \\ y = -x \end{cases} \implies -x^2 = c \implies x^2 = -c \implies x = -\sqrt{-c} \quad \text{(poiché } x < 0 \text{ nel II quad.)}$$

Il punto è $(-\sqrt{-c}, \sqrt{-c}) = (-\sqrt{-ab}, \sqrt{-ab})$.

Se $c = 0$: L'unica intersezione tra gli assi ($xy = 0$) e $y = |x|$ è l'origine $(0, 0)$.

Concludendo, l'SCR è:

$$S.C.R. = \{(x, |x|) \mid x \in \mathbb{R}\}$$

Possiamo riassumere la mappa che associa ad ogni classe il suo rappresentante (vertice):

$$[(a, b)]_R \longmapsto \begin{cases} (\sqrt{ab}, \sqrt{ab}) & \text{se } ab > 0 \\ (0, 0) & \text{se } ab = 0 \\ (-\sqrt{-ab}, \sqrt{-ab}) & \text{se } ab < 0 \end{cases}$$

Operazioni Indotte su Insiemi Prodotto Dati due insiemi dotati di operazioni, possiamo definire una nuova struttura sul loro prodotto cartesiano.

Definizione 0.42. Siano (A, ω_A) e (B, ω_B) due strutture algebriche. Si definisce l'operazione prodotto $\omega_{A\times B}$ su $A \times B$ componente per componente:

$$(a, b)\ \omega_{A\times B}\ (\alpha, \beta) = (a\ \omega_A\ \alpha,\ b\ \omega_B\ \beta)$$

Struttura su $\mathbb{N}\times\mathbb{N}$ Applicando questa definizione a $(\mathbb{N}, +)$, otteniamo che $(\mathbb{N}\times\mathbb{N}, +)$ è un monoide commutativo con operazione:

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

L'elemento neutro è la coppia $(0, 0)$.

Una nuova operazione di prodotto (*) Introduciamo ora una seconda operazione su $\mathbb{N}\times\mathbb{N}$, denotata con $*$, che non è quella componente per componente, ma è definita come:

$$(a, b) * (c, d) = (ac + bd, ad + bc)$$

Nota 17. Questa definizione è cruciale per la costruzione dei numeri interi $\mathbb{Z}$. Se interpretiamo la coppia (a, b) come la differenza $a-b$, allora il prodotto $(a-b)(c-d)$ sviluppato è proprio $(ac+bd)-(ad+bc)$, che corrisponde alla coppia definita sopra.

Anche $(\mathbb{N}\times\mathbb{N}, *)$ risulta essere un monoide commutativo. L'elemento neutro rispetto a $*$ è $(1, 0)$. Infatti:

$$(a, b) * (1, 0) = (a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b)$$

Proprietà Distributiva Consideriamo la struttura con entrambe le operazioni $(\mathbb{N}\times\mathbb{N}, +, *)$. Vogliamo verificare che il prodotto $*$ sia distributivo rispetto alla somma $+$. Dobbiamo provare che:

$$(a, b) * [(c, d) + (e, f)] = (a, b) * (c, d) + (a, b) * (e, f)$$

Poiché entrambe le operazioni sono commutative, basta verificarlo da un lato.

Proof. Membro Sinistro: Calcoliamo prima la somma dentro la parentesi quadra:

$$(c, d) + (e, f) = (c + e, d + f)$$

Ora applichiamo il prodotto con (a, b):

$$(a, b) * (c + e, d + f) = (a(c + e) + b(d + f),\ a(d + f) + b(c + e))$$

Sviluppando i prodotti in $\mathbb{N}$:

$$= (ac + ae + bd + bf,\ ad + af + bc + be)$$

Membro Destro: Calcoliamo i due prodotti separatamente:

$$(a, b) * (c, d) = (ac + bd,\ ad + bc)$$

$$(a, b) * (e, f) = (ae + bf,\ af + be)$$

Sommiamo i risultati componente per componente:

$$= ((ac + bd) + (ae + bf),\ (ad + bc) + (af + be))$$

Riordinando i termini (grazie alla commutatività e associatività di $+$ in $\mathbb{N}$):

$$= (ac + ae + bd + bf,\ ad + af + bc + be)$$

Le due espressioni coincidono. La proprietà distributiva è verificata. □

Gli Anelli Introduciamo una struttura algebrica dotata di due operazioni binarie, che generalizza l'aritmetica dei numeri interi.

Definizione 0.43. Un insieme non vuoto A dotato di due operazioni, che indicheremo con $+$ (addizione) e $\cdot$ (moltiplicazione), si dice *Anello* $(A, +, \cdot)$ se soddisfa le seguenti condizioni:

1. $(A, +)$ è un gruppo abeliano (commutativo).
2. $(A, \cdot)$ è un semigruppo.
3. Valgono le leggi distributive della moltiplicazione rispetto all'addizione:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in A$$

Analizziamo cosa implicano queste richieste:

- Per la **I condizione** (Gruppo Abeliano su $+$): L'operazione è associativa, commutativa, esiste l'elemento neutro (che chiameremo 0_A) ed esiste l'opposto per ogni elemento $(-a)$.
- Per la **II condizione** (Semigruppo su $\cdot$): L'operazione è associativa.

Tipologie di Anelli Le varianti degli anelli si ottengono aggiungendo proprietà alla seconda operazione $(\cdot)$, dato che la prima è già "satura" di proprietà.

- *Anello Commutativo*: Se l'operazione di moltiplicazione è commutativa ($ab = ba \ \forall a, b$).
- *Anello Unitario*: Se $(A, \cdot)$ è un monoide, ovvero possiede un elemento neutro 1_A (diverso da 0_A).

Definiamo ora due strutture fondamentali che sono specificazioni degli anelli.

Definizione 0.44. Campo: È un anello commutativo unitario in cui ogni elemento diverso da zero è invertibile rispetto alla moltiplicazione.

$$\forall a \in A \setminus \{0_A\}, \ \exists a^{-1} \in A : a \cdot a^{-1} = 1_A$$

Definizione 0.45. Dominio d'Integrità: È un anello commutativo unitario privo di divisori dello zero. Ovvero, l'insieme degli elementi non nulli A^* è stabile rispetto al prodotto:

$$a \neq 0_A \wedge b \neq 0_A \implies a \cdot b \neq 0_A$$

Il prototipo fondamentale è l'anello dei numeri interi $(\mathbb{Z}, +, \cdot)$.

Relazioni Compatibili Per costruire nuove strutture algebriche (come $\mathbb{Z}$ a partire da $\mathbb{N}$), dobbiamo introdurre il concetto di compatibilità tra una relazione e un'operazione.

Definizione 0.46. Sia $(S, *)$ una struttura con operazione binaria e sia R una relazione di equivalenza su S. Diciamo che R è *compatibile* con l'operazione $*$ se:

$$aR\alpha \wedge bR\beta \implies (a * b)R(\alpha * \beta)$$

In parole povere: se sostituisco gli operandi con elementi equivalenti, il risultato rimane equivalente.

Costruzione degli Interi $\mathbb{Z}$ Consideriamo il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ dotato dell'operazione somma componente per componente:

$$(a, b) + (c, d) = (a + c, b + d)$$

Definiamo la relazione R su $\mathbb{N} \times \mathbb{N}$ che formalizza l'idea che la coppia (a, b) rappresenti la differenza $a - b$:

$$(a, b)R(\alpha, \beta) \iff a + \beta = b + \alpha$$

Proposizione 0.45. *R è una relazione di equivalenza.*

Proof. Verifichiamo le tre proprietà:

1. *Riflessiva*: $(a,b)R(a,b)$ poiché $a+b=b+a$ (vero per commutatività di $\mathbb{N}$).
2. *Simmetrica*: Se $(a,b)R(c,d)$ allora $a+d=b+c$. Leggendo l'uguaglianza al contrario $c+b=d+a$, che significa $(c,d)R(a,b)$.
3. *Transitiva*: Siano $(a,b)R(c,d)$ e $(c,d)R(e,f)$.

$$\begin{cases} a+d=b+c \\ c+f=d+e \end{cases}$$

Sommando membro a membro:

$$a+d+c+f=b+c+d+e$$

Cancellando c e d (legge di cancellazione in $\mathbb{N}$):

$$a+f=b+e$$

Che implica $(a,b)R(e,f)$.

□

Proposizione 0.46. *La relazione R è compatibile con l'addizione su $\mathbb{N}\times\mathbb{N}$.*

Proof. Siano $(a,b)R(\alpha,\beta)$ e $(c,d)R(\gamma,\delta)$. Per ipotesi:

$$a+\beta=b+\alpha \quad \text{e} \quad c+\delta=d+\gamma$$

Sommando le due equazioni:

$$(a+c)+(\beta+\delta)=(b+d)+(\alpha+\gamma)$$

Questa uguaglianza ci dice esattamente che la somma delle prime coppie è in relazione con la somma delle seconde:

$$(a+c,b+d)R(\alpha+\gamma,\beta+\delta)$$

Quindi R è compatibile. □

Definizione dell'Insieme $\mathbb{Z}$ Possiamo ora definire l'insieme dei numeri interi come l'insieme quoziente:

$$\mathbb{Z}=\frac{\mathbb{N}\times\mathbb{N}}{R}=\{[(a,b)]_R \mid (a,b)\in\mathbb{N}\times\mathbb{N}\}$$

Grazie alla compatibilità dimostrata sopra, possiamo definire l'operazione di somma su $\mathbb{Z}$ "indotta" da quella su $\mathbb{N}\times\mathbb{N}$:

$$[(a,b)]_R+[(c,d)]_R:=[(a+c,b+d)]_R$$

Nota 18. La compatibilità è fondamentale: essa garantisce che questa definizione sia *ben posta*. Significa che il risultato della somma di due numeri interi non cambia se scegliamo rappresentanti diversi per le classi (es. sommare $[(5,2)]$ o sommare $[(8,5)]$ è la stessa cosa, perché rappresentano lo stesso intero $+3$).

Compatibilità: Esempi e Controesempi Analizziamo come le relazioni di equivalenza interagiscono con le operazioni dei gruppi, usando il gruppo simmetrico S_3 come banco di prova.

Esempio 0.33. *Compatibilità in S_3 (Sottogruppo Normale)* Consideriamo $(S_3, \circ)$ e la relazione R le cui classi sono:

$$A = \{id, (123), (132)\} \quad \text{e} \quad B = \{(12), (13), (23)\}$$

Verifichiamo che R è compatibile: dobbiamo controllare che se $aR\alpha$ e $bR\beta$, allora $(a \circ b)R(\alpha \circ \beta)$.

Primo controllo: Siano $a = (123), \alpha = (132)$ (quindi $aR\alpha$) e $b = (12), \beta = (23)$ (quindi $bR\beta$).

$$\left.\begin{aligned} a \circ b &= (123) \circ (12) = (13) \\ \alpha \circ \beta &= (132) \circ (23) = (13) \end{aligned}\right\} \text{ I risultati sono identici, quindi in relazione.}$$

Secondo controllo (cambiando β): Manteniamo a, α come sopra, ma scegliamo $\beta = (13)$.

$$\left.\begin{aligned} \alpha \circ \beta &= (132) \circ (13) = (12) \\ a \circ b &= (13) \end{aligned}\right\} (12) \text{ e } (13) \text{ sono entrambi in } B, \text{ quindi in relazione.}$$

La relazione è compatibile.

Esempio 0.34. *Non-Compatibilità in S_3 (Sottogruppo non Normale)* Consideriamo ora la relazione R le cui classi sono i laterali destri di $H = \{id, (12)\}$:

$$C_1 = \{id, (12)\}, \quad C_2 = \{(123), (23)\}, \quad C_3 = \{(132), (13)\}$$

Verifichiamo se è compatibile. Siano:

- $a = (123)$ e $\alpha = (23)$ (quindi $aR\alpha$ perché stanno in C_2).
- $b = (132)$ e $\beta = (13)$ (quindi $bR\beta$ perché stanno in C_3).

Calcoliamo i prodotti:

$$a \circ b = (123) \circ (132) = id$$
$$\alpha \circ \beta = (23) \circ (13) = (123)$$

Affinché fosse compatibile, dovremmo avere $idR(123)$. Ma $id \in C_1$ e $(123) \in C_2$. Poiché le classi sono diverse, la relazione *non* è compatibile.

L'Anello Quoziente $\mathbb{Z}_2$ Un esempio fondamentale di compatibilità si ha con la parità dei numeri naturali. Consideriamo $(\mathbb{N}, +, \cdot)$ e la relazione R con classi:

$$P = \{2n \mid n \in \mathbb{N}\} \quad \text{(Pari)}, \qquad D = \{2n+1 \mid n \in \mathbb{N}\} \quad \text{(Dispari)}$$

La relazione è compatibile sia con la somma che con il prodotto. Possiamo costruire le tabelle delle operazioni per l'insieme quoziente $\mathbb{N}/R = \{P, D\}$:

$+$	P	D
P	P	D
D	D	P

$(\mathbb{N}/R, +)$ è un *gruppo* (ogni elemento ha opposto, $D + D = P$).

$\cdot$	P	D
P	P	P
D	P	D

$(\mathbb{N}/R, \cdot)$ è un *monoide* con neutro D (poiché $D \cdot x = x$).

Conclusione: La struttura $(\frac{\mathbb{N}}{R}, +, \cdot)$ è un *Anello Unitario* (con due elementi, isomorfo a $\mathbb{Z}_2$). Notiamo che siamo partiti da $\mathbb{N}$ (che non è un gruppo) e abbiamo ottenuto un gruppo additivo nel quoziente.

Proprietà Ereditarie nei Quozienti Quando una relazione è compatibile, molte proprietà della struttura originale si trasferiscono al quoziente.

Proposizione 0.47. *Sia $(S, *)$ una struttura e S/R il suo quoziente tramite una relazione compatibile.*

- *Commutatività: Se $*$ è commutativa in S, lo è anche in S/R.*
- *Associatività: Se $*$ è associativa in S, lo è anche in S/R.*
- *Elemento Neutro: Se 1_S è neutro in S, allora $[1_S]_R$ è neutro in S/R.*

Proof. Commutatività: Infatti:

$$[x]_R * [y]_R = [x * y]_R$$

Poiché per ipotesi $x * y = y * x$, il rappresentante della classe è lo stesso, dunque:

$$= [y * x]_R = [y]_R * [x]_R$$

Associatività: Infatti:

$$[a]_R * ([b]_R * [c]_R) = [a]_R * [b * c]_R = [a * (b * c)]_R$$

Grazie all'associatività interna a S, sappiamo che $a * (b * c) = (a * b) * c$. Sostituendo il rappresentante:

$$= [(a * b) * c]_R = [a * b]_R * [c]_R = ([a]_R * [b]_R) * [c]_R$$

Neutro: Infatti:

$$[1_S]_R * [x]_R = [1_S * x]_R$$

Essendo $1_S * x = x$, otteniamo immediatamente:

$$= [x]_R$$

Dunque $[1_S]_R = 1_{\frac{S}{R}}$. □

La Struttura degli Interi $\mathbb{Z}$ Torniamo alla costruzione di $\mathbb{Z}$ come quoziente di $\mathbb{N} \times \mathbb{N}$ tramite la relazione $a + \beta = b + \alpha$. Abbiamo già stabilito che $(\mathbb{Z}, +)$ è un monoide commutativo con neutro $0_{\mathbb{Z}} = [(0, 0)]_R$.

Proposizione 0.48. *$(\mathbb{Z}, +)$ è un Gruppo. Dobbiamo provare che ogni elemento possiede un inverso additivo (opposto).*

Proof. Sia $x = [(a, b)]_R$. Il candidato opposto è la classe "rovesciata" $[(b, a)]_R$.

$$[(a, b)] + [(b, a)] = [(a + b, b + a)]$$

Poiché $a + b = b + a$, la coppia $(a + b, b + a)$ è in relazione con $(0, 0)$ (infatti $x + 0 = x + 0$). Quindi la somma è $[(0, 0)]_R = 0_{\mathbb{Z}}$. □

La Moltiplicazione in $\mathbb{Z}$ Definiamo il prodotto in $\mathbb{N} \times \mathbb{N}$ come:

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc)$$

Questo forma un monoide commutativo con neutro $(1, 0)$. Dobbiamo dimostrare che la relazione R è *compatibile* con questa operazione per poterla indurre su $\mathbb{Z}$.

Compatibilità della Moltiplicazione Vogliamo definire il prodotto in $\mathbb{Z}$ tramite l'operazione su $\mathbb{N} \times \mathbb{N}$:

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc)$$

Dobbiamo dimostrare che la relazione R (definita da $a + \beta = b + \alpha$) è compatibile con questa moltiplicazione.

Tesi Generale: Se $(a, b)R(\alpha, \beta)$ e $(c, d)R(\gamma, \delta)$, allora:

$$[(a, b) \cdot (c, d)] \; R \; [(\alpha, \beta) \cdot (\gamma, \delta)]$$

Dimostrazione La dimostrazione si divide in due step logici per semplificare i calcoli.

Step 1: Lemma preliminare Proviamo che la relazione regge se moltiplichiamo entrambi i membri per una *stessa* coppia (x, y).

$$(r, s)R(u, v) \implies (r, s) \cdot (x, y)\ R\ (u, v) \cdot (x, y)$$

Dimostrazione Step 1: L'ipotesi è $(r, s)R(u, v)$, il che significa che $r + v = s + u$. Calcoliamo i due prodotti:

$$P_1 = (r, s) \cdot (x, y) = (rx + sy,\ ry + sx)$$

$$P_2 = (u, v) \cdot (x, y) = (ux + vy,\ uy + vx)$$

Dobbiamo verificare che $P_1 R P_2$. Applicando la definizione di R (somma degli estremi = somma dei medi):

$$(rx + sy) + (uy + vx) \stackrel{?}{=} (ry + sx) + (ux + vy)$$

Per verificare se è vera, riordiniamo i termini raccogliendo la x e la y:

$$x(r + v) + y(s + u) \stackrel{?}{=} y(r + v) + x(s + u)$$

Ora usiamo l'ipotesi: sappiamo che $r + v$ è uguale a $s + u$. Chiamiamo questa quantità K. Sostituendo K nell'equazione:

$$xK + yK \stackrel{?}{=} yK + xK$$

Questa uguaglianza è banalmente vera per la proprietà commutativa di $\mathbb{N}$. Quindi il Lemma è dimostrato.

Step 2: Dimostrazione Generale (uso della transitività) Ora torniamo alla tesi completa con quattro coppie diverse. Vogliamo passare da $(a, b) \cdot (c, d)$ a $(\alpha, \beta) \cdot (\gamma, \delta)$. Possiamo farlo in due passaggi, cambiando una coppia alla volta:

1. Consideriamo il passaggio dalla prima alla seconda coppia: Essendo $(a, b)R(\alpha, \beta)$, per il Lemma appena dimostrato (moltiplicando entrambi per (c, d)) si ha:

$$(a, b) \cdot (c, d)\ R\ (\alpha, \beta) \cdot (c, d)$$

2. Consideriamo ora il passaggio sul secondo fattore: Essendo $(c, d)R(\gamma, \delta)$, sempre per il Lemma (moltiplicando entrambi per (α, β)) si ha:

$$(\alpha, \beta) \cdot (c, d)\ R\ (\alpha, \beta) \cdot (\gamma, \delta)$$

Conclusione: Abbiamo ottenuto una catena di relazioni:

$$[(a, b)(c, d)]\ R\ [(\alpha, \beta)(c, d)]\ R\ [(\alpha, \beta)(\gamma, \delta)]$$

Poiché R è una relazione di equivalenza, vale la proprietà transitiva. Dunque il primo elemento è in relazione con l'ultimo:

$$(a, b) \cdot (c, d)\ R\ (\alpha, \beta) \cdot (\gamma, \delta)$$

Conclusione sulla Struttura di $\mathbb{Z}$ Definendo il prodotto nel quoziente come $[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$: 1. $(\mathbb{Z}, +)$ è un Gruppo Abeliano. 2. $(\mathbb{Z}, \cdot)$ è un Monoide Commutativo (neutro $1_{\mathbb{Z}} = [(1, 0)]$). 3. Valgono le proprietà distributive (ereditate).

Dunque $(\mathbb{Z}, +, \cdot)$ è un *Anello Commutativo Unitario.*

L'Ordine in $\mathbb{N}$ è Totale Concludiamo con una proprietà fondamentale dell'ordine naturale, necessaria per la buona definizione di molte strutture successive.

Proposizione 0.49. *L'ordine naturale $\leq$ su $\mathbb{N}$ è totale:*

$$\forall x, y \in \mathbb{N}, \quad x \leq y \vee y \leq x$$

Proof. Definiamo i segmenti iniziali e finali: $[0, n] = \{x \mid x \leq n\}$ e $[n, +\infty[= \{x \mid x \geq n\}$. Proviamo per induzione che $A = \{n \in \mathbb{N} \mid [0, n] \cup [n, +\infty[= \mathbb{N}\}$ coincide con $\mathbb{N}$.

Base ($n = 0$): $[0, 0] \cup [0, +\infty[= \{0\} \cup \mathbb{N} = \mathbb{N}$. (Vero).

Passo Induttivo ($m \to m+1$): Supponiamo che ogni numero sia confrontabile con m. Prendiamo un generico x.

- Se $x \in [0, m]$, allora $x \leq m < m + 1$, quindi $x \in [0, m + 1]$.
- Se $x \in [m, +\infty[$, allora $x \geq m$. Se $x = m$, $x < m + 1$. Se $x \neq m$, allora $x \geq m + 1$.

In ogni caso x cade nell'unione $[0, m + 1] \cup [m + 1, +\infty[$. Poiché l'unione copre tutto $\mathbb{N}$, ogni numero x è confrontabile con n. □

L'Immersione di $\mathbb{N}$ in $\mathbb{Z}$ Abbiamo costruito $\mathbb{Z}$ come insieme di classi di equivalenza. Vogliamo ora identificare formalmente i "vecchi" numeri naturali all'interno di questa nuova struttura.

Definizione 0.47. Definiamo l'applicazione immersione $j : \mathbb{N} \to \mathbb{Z}$ come:

$$j(x) = [(x, 0)]_R$$

Questa funzione associa a ogni naturale x la classe che rappresenta l'intero positivo $+x$.

Proposizione 0.50. *La funzione j è un monomorfismo che rispetta le operazioni (è un omomorfismo iniettivo):*

1. $j(x + y) = j(x) + j(y)$
2. $j(x \cdot y) = j(x) \cdot j(y)$
3. *j è iniettiva.*

Proof. **1. Additività:**

$$j(x) + j(y) = [(x, 0)] + [(y, 0)] = [(x + y, 0)] = j(x + y)$$

2. Moltiplicatività:

$$j(x) \cdot j(y) = [(x, 0)] \cdot [(y, 0)] = [(x \cdot y + 0 \cdot 0, x \cdot 0 + 0 \cdot y)] = [(xy, 0)] = j(xy)$$

3. Iniettività: Sia $j(x) = j(y)$. Allora $[(x, 0)] = [(y, 0)]$. Per definizione di relazione R, significa $(x, 0)R(y, 0)$, ovvero $x + 0 = 0 + y$, che implica $x = y$. □

Nota 19. Poiché j conserva la struttura, l'insieme immagine $j(\mathbb{N}) \subseteq \mathbb{Z}$ è una "copia" esatta di $\mathbb{N}$ dentro $\mathbb{Z}$. D'ora in poi identificheremo $x \in \mathbb{N}$ con la sua immagine $j(x)$, scrivendo semplicemente x al posto di $[(x, 0)]$.

Struttura degli Interi (Positivi e Negativi) Dimostriamo che ogni numero intero è o un numero naturale (positivo) o l'opposto di un numero naturale.

Proposizione 0.51. *Per ogni $z \in \mathbb{Z}$, vale una delle seguenti:*

$$z \in \mathbb{N} \quad (\textit{cioè } z \in j(\mathbb{N})) \quad \textit{oppure} \quad -z \in \mathbb{N}$$

Proof. Sia $z = [(a, b)]_R \in \mathbb{Z}$. Poiché l'ordinamento in $\mathbb{N}$ è totale, i numeri naturali a e b sono sempre confrontabili. Si presentano due casi:

- *Caso 1 ($a \leq b$)*: Per definizione dell'ordine naturale, esiste un unico $x \in \mathbb{N}$ tale che $b = a + x$. Sostituiamo b nella rappresentazione della classe:

  $$z = [(a, a + x)]_R$$

  Sfruttando la definizione di somma in $\mathbb{Z}$:

  $$z = [(a, a) + (0, x)]_R = [(a, a)]_R + [(0, x)]_R$$

  Poiché $[(a, a)]_R$ è l'elemento neutro $0_{\mathbb{Z}}$ (equivalente a $[(0, 0)]_R$), otteniamo:

  $$z = 0_{\mathbb{Z}} + [(0, x)]_R = [(0, x)]_R$$

Consideriamo ora l'opposto di z. Ricordando che l'opposto si ottiene scambiando gli elementi della coppia:

$$-z = -[(0,x)]_R = [(x,0)]_R$$

Per definizione della funzione immersione j, si ha $[(x,0)]_R = j(x)$. Pertanto $-z \in j(\mathbb{N})$, che identifichiamo con $\mathbb{N}$.

- *Caso 2 ($b \leq a$)*: Esiste un unico $y \in \mathbb{N}$ tale che $a = b + y$. Analogamente al caso precedente:

$$z = [(b+y,b)]_R = [(y,0)+(b,b)]_R = [(y,0)]_R + [(b,b)]_R$$

Essendo $[(b,b)]_R = 0_{\mathbb{Z}}$, si ha:

$$z = [(y,0)]_R + 0_{\mathbb{Z}} = [(y,0)]_R$$

Riconosciamo immediatamente l'immagine tramite l'immersione:

$$z = j(y)$$

Pertanto $z \in j(\mathbb{N})$, che identifichiamo con $\mathbb{N}$.

□

Corollario 2. *L'insieme degli interi è l'unione dei naturali e dei loro opposti:*

$$\mathbb{Z} = \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\}$$

L'intersezione di questi due insiemi è solo lo zero: $x = -x \iff x = 0$.

Proof. $\forall z \in \mathbb{Z}$, vale che $z \in \mathbb{N}$ oppure $-z \in \mathbb{N}$. In questo secondo caso $\exists x \in \mathbb{N}$ tale che $-z = x$, da cui $-(-z) = -x$, cioè $z = -x$. Infine se $z = -z$ (supponendo z associato a x, cioè $z = [(x,0)]_R$), allora:

$$[(x,0)]_R = -[(x,0)]_R = [(0,x)]_R$$

Questo implica $(x,0)R(0,x)$, cioè $x + x = 0 + 0$ in $\mathbb{N}$. Ovvero $x + x = 0$, che implica $x = 0$ (per la legge di cancellazione in $\mathbb{N}$). □

L'Ordine in $\mathbb{Z}$ Estendiamo la nozione di disuguaglianza dai naturali agli interi.

Definizione 0.48. Siano $z_1, z_2 \in \mathbb{Z}$. Definiamo la relazione d'ordine $\leq$ come:

$$z_1 \leq z_2 \iff z_2 - z_1 \in \mathbb{N}$$

(Ovvero, la differenza è un intero non negativo).

Proposizione 0.52. *La relazione $\leq$ è un ordine (riflessivo, transitivo, antisimmetrico) su $\mathbb{Z}$ ed estende l'ordine di $\mathbb{N}$.*

Proof.

- **Riflessiva:** $z \leq z$ perché $z - z = 0 \in \mathbb{N}$.
- **Transitiva:** Se $z_1 \leq z_2$ e $z_2 \leq z_3$, allora le differenze $z_2 - z_1 = j(x)$ e $z_3 - z_2 = j(y)$ sono in $\mathbb{N}$. Sommando le differenze:

$$(z_3 - z_2) + (z_2 - z_1) = z_3 - z_1 = j(y) + j(x) = j(x+y) \in \mathbb{N}$$

Quindi $z_1 \leq z_3$.

- **Antisimmetrica:** Se $z_1 \leq z_2$ e $z_2 \leq z_1$, allora $z = z_2 - z_1 \in \mathbb{N}$ e anche il suo opposto $-(z_2 - z_1) = z_1 - z_2 \in \mathbb{N}$. L'unico numero che sta in $\mathbb{N}$ insieme al suo opposto è lo zero. Quindi $z = 0 \implies z_1 = z_2$.

□

Coerenza con l'Ordine Naturale Verifichiamo che questo nuovo ordine coincida con il precedente quando ristretto ai naturali.

Proposizione 0.53. *Per ogni* $x, y \in \mathbb{N}$*:*

$$j(x) \leq j(y) \text{ in } \mathbb{Z} \iff x \leq y \text{ in } \mathbb{N}$$

Proof. Vogliamo provare che $j(x) \leq j(y)$ in $\mathbb{Z} \iff x \leq y$ in $\mathbb{N}$.

$\implies$ Siano $x, y \in \mathbb{N}$ tali che $x \leq y$. Per definizione di ordine in $\mathbb{N}$, esiste $t \in \mathbb{N}$ tale che $y = x + t$. Sostituiamo nelle immagini tramite j:

$$j(y) = [(y, 0)]_R = [(x + t, 0)]_R$$

Calcoliamo la differenza $j(y) - j(x)$ in $\mathbb{Z}$:

$$\begin{aligned} j(y) - j(x) &= [(x + t, 0)]_R + (-[(x, 0)]_R) \\ &= [(x + t, 0)]_R + [(0, x)]_R \\ &= [(x + t, x)]_R \end{aligned}$$

Osserviamo che la classe $[(x + t, x)]_R$ è equivalente alla classe $[(t, 0)]_R$. Infatti la relazione $(x + t, x)R(t, 0)$ è verificata poiché $(x + t) + 0 = x + t$. Quindi:

$$= [(t, 0)]_R = j(t)$$

Poiché $j(t) \in j(\mathbb{N})$, la definizione di ordine in $\mathbb{Z}$ è soddisfatta: $j(x) \leq j(y)$.

$\impliedby$ Siano $x, y \in \mathbb{N}$ tali che $j(x) \leq j(y)$ in $\mathbb{Z}$. Per definizione di ordine su $\mathbb{Z}$, la differenza deve essere un "intero naturale":

$$j(y) - j(x) \in j(\mathbb{N})$$

Ciò significa che esiste un $t \in \mathbb{N}$ tale che:

$$j(y) - j(x) = j(t)$$

Portando $j(x)$ a destra e usando la proprietà di omomorfismo (additività) di j:

$$j(y) = j(x) + j(t) \implies j(y) = j(x + t)$$

Poiché l'immersione j è **iniettiva**, possiamo togliere la j:

$$y = x + t$$

Questa è esattamente la definizione di $x \leq y$ in $\mathbb{N}$.

□

Rappresentazione Canonica degli Interi Concludiamo identificando un Sistema Completo di Rappresentanti (SCR) per $\mathbb{Z}$ che formalizza la classica notazione con il segno.

Ogni intero $z = [(a, b)]$ si riduce a una forma canonica semplice:

$$z = \begin{cases} [(x, 0)] & \text{se } a \geq b \quad (\text{dove } x = a - b \in \mathbb{N}) \\ [(0, y)] & \text{se } a < b \quad (\text{dove } y = b - a \in \mathbb{N}^*) \end{cases}$$

L'insieme dei rappresentanti canonici è quindi:

$$T = \{(x, 0) \mid x \in \mathbb{N}^*\} \cup \{(0, 0)\} \cup \{(0, y) \mid y \in \mathbb{N}^*\}$$

Che corrisponde all'insieme $\{1, 2, \dots\} \cup \{0\} \cup \{-1, -2, \dots\}$.

Il Dominio di Integrità $\mathbb{Z}$ L'insieme $\mathbb{Z}$ è un dominio di integrità. Questo significa che è un anello commutativo unitario privo di divisori dello zero. Formalmente, $(\mathbb{Z}^*, \cdot)$ è un monoide commutativo unitario, dove $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

La stabilità di $\mathbb{Z}^*$ rispetto alla moltiplicazione (ovvero: il prodotto di due numeri non nulli è non nullo) è evidenziata dalla seguente tavola dei segni:

$\cdot$	$+$	0	$-$
$+$	$+$	0	$-$
0	0	0	0
$-$	$-$	0	$+$

Possiamo espandere questa tabella considerando le classi di equivalenza che definiscono $\mathbb{Z}$ (dove $x, y \in \mathbb{N}^*$):

$\cdot$	$[(x_2, 0)]$	$[(0,0)]$	$[(0, y_2)]$
$[(x_1, 0)]$	$[(x_1x_2, 0)]$	$[(0,0)]$	$[(0, x_1y_2)]$
$[(0,0)]$	$[(0,0)]$	$[(0,0)]$	$[(0,0)]$
$[(0, y_1)]$	$[(0, y_1x_2)]$	$[(0,0)]$	$[(y_1y_2, 0)]$

Questa tavola dimostra che se i fattori sono in $\mathbb{Z}^*$ (quindi non sono la classe $[(0,0)]$), anche il prodotto è in $\mathbb{Z}^*$.

Il Gruppo delle Matrici Triangolari Superiori (Heisenberg) Consideriamo l'insieme G delle matrici triangolari superiori unitarie a coefficienti interi:

$$G = \left\{ X = \begin{pmatrix} 1 & d & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}) \middle| d, b, c \in \mathbb{Z} \right\}$$

Invertibilità Il determinante di una matrice triangolare è il prodotto degli elementi sulla diagonale:

$$\det(X) = 1 \cdot 1 \cdot 1 = 1 \neq 0$$

Poiché il determinante è non nullo (e in particolare è un'unità in $\mathbb{Z}$), la matrice X è invertibile.

Calcolo dell'Inversa Cerchiamo la matrice inversa X^{-1}. Ipotizziamo che sia dello stesso tipo di X, ovvero:

$$X^{-1} = Y = \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}$$

Imponiamo la condizione di inversa destra: $X \cdot Y = I_3$.

$$\begin{pmatrix} 1 & d & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Svolgiamo il prodotto righe per colonne nel membro sinistro:

$$\begin{pmatrix} 1 & \alpha + d & \gamma + d\beta + c \\ 0 & 1 & \beta + b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Uguagliando i termini corrispondenti, otteniamo il sistema:

$$\begin{cases} \alpha + d = 0 \\ \beta + b = 0 \\ \gamma + d\beta + c = 0 \end{cases} \implies \begin{cases} \alpha = -d \\ \beta = -b \\ \gamma - db + c = 0 \end{cases} \implies \begin{cases} \alpha = -d \\ \beta = -b \\ \gamma = db - c \end{cases}$$

Sostituendo i valori trovati in Y, otteniamo la matrice candidata inversa:

$$Y = \begin{pmatrix} 1 & -d & db - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

Verifica dell'Inversa Sinistra Bisogna ancora verificare che $Y \cdot X = I_3$.

$$\begin{pmatrix} 1 & -d & db-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

Calcoliamo i termini non banali:

- Posizione (1,2): $1(d) + (-d)(1) + (db-c)(0) = d - d = 0$
- Posizione (1,3): $1(c) + (-d)(b) + (db-c)(1) = c - db + db - c = 0$
- Posizione (2,3): $0(c) + 1(b) + (-b)(1) = b - b = 0$

Il risultato è:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$$

Dunque Y è effettivamente l'inversa di X.

Struttura di Gruppo L'insieme G, dotato dell'operazione di moltiplicazione righe per colonne, è un gruppo.

$$\begin{pmatrix} 1 & d & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+d & \gamma+d\beta+c \\ 0 & 1 & \beta+b \\ 0 & 0 & 1 \end{pmatrix}$$

Verifichiamo le proprietà:

- **Associatività:** Vale perché il prodotto di matrici è associativo.
- **Elemento Neutro:** Esiste $1_G = I_3$ (caso $d = b = c = 0$).
- **Elemento Inverso:** Per ogni $X \in G$, esiste $Y \in G$ (calcolato sopra) tale che $XY = YX = I_3$.

Analisi dei Sottogruppi A, B, C Analizziamo tre sottoinsiemi notevoli di G.

1. Sottogruppo A

$$A = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\} \subseteq G$$

Verifichiamo che $A \leq G$:

- *Stabilità:* Siano $X, Y \in A$.

$$X \cdot Y = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  Il risultato appartiene ancora ad A (la somma $\alpha + a \in \mathbb{Z}$).

- *Inverso:* Sia $X \in A$. L'inversa (usando la formula generale con $b = 0, c = 0$) è:

$$X^{-1} = \begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  Che appartiene chiaramente ad A.

$\implies A \leq G$.

2. Sottogruppo B

$$B = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Z} \right\} \subseteq G$$

Verifichiamo che $B \leq G$:

- *Stabilità:* Siano $X, Y \in B$.

$$X \cdot Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b+\beta \\ 0 & 0 & 1 \end{pmatrix}$$

  Il risultato appartiene a B.

- *Inverso:* Sia $X \in B$. L'inversa (formula generale con $d = 0, c = 0$) è:

$$X^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

  Che appartiene a B.

$\implies B \leq G$.

3. Sottogruppo C

$$C = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| c \in \mathbb{Z} \right\} \subseteq G$$

Verifichiamo che $C \leq G$:

- *Stabilità:* Siano $X, Y \in C$.

$$X \cdot Y = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & c+\gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  Il risultato appartiene a C.

- *Inverso:* Sia $X \in C$. L'inversa (formula generale con $d = 0, b = 0$) è:

$$X^{-1} = \begin{pmatrix} 1 & 0 & -c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  Che appartiene a C.

$\implies C \leq G$.

I sottogruppi A, B, C precedentemente definiti sono tra di loro isomorfi e, a loro volta, isomorfi al gruppo additivo degli interi $(\mathbb{Z}, +)$. Possiamo definire esplicitamente gli isomorfismi:

$$\begin{aligned} f_A : \mathbb{Z} &\longrightarrow A \\ x &\longmapsto \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned} \qquad \begin{aligned} f_B : \mathbb{Z} &\longrightarrow B \\ x &\longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \end{aligned} \qquad \begin{aligned} f_C : \mathbb{Z} &\longrightarrow C \\ x &\longmapsto \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

In tutti e tre i casi, l'applicazione f è biunivoca e rispetta le operazioni (manda la somma di interi nel prodotto di matrici).

Il Prodotto di Sottogruppi $A \cdot B$ in G Definiamo l'insieme prodotto:

$$A \cdot B = \{X \cdot Y \mid X \in A, Y \in B\} \subseteq G$$

Calcoliamo il prodotto di un generico elemento di A per uno di B:

$$X \cdot Y = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & ab \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

Dunque l'insieme è:

$$A \cdot B = \left\{ \begin{pmatrix} 1 & a & ab \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$$

Notiamo che l'elemento in posizione $(1,3)$ è vincolato: deve essere esattamente il prodotto $a \cdot b$.

Verifica: $A \cdot B$ è un sottogruppo? Per essere un sottogruppo, $A \cdot B$ deve essere stabile rispetto alla moltiplicazione. Prendiamo due elementi generici di $A \cdot B$ e moltiplichiamoli:

$$\mathcal{M}_1 = \begin{pmatrix} 1 & a & ab \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{M}_2 = \begin{pmatrix} 1 & \alpha & \alpha\beta \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}$$

Il loro prodotto è:

$$\mathcal{M}_1 \cdot \mathcal{M}_2 = \begin{pmatrix} 1 & \alpha + a & (\alpha\beta + a\beta + ab) \\ 0 & 1 & \beta + b \\ 0 & 0 & 1 \end{pmatrix}$$

Affinché questa matrice risultante appartenga all'insieme $A \cdot B$, il suo termine in posizione $(1,3)$ deve essere il prodotto dei termini $(1,2)$ e $(2,3)$. Dobbiamo quindi verificare se:

$$\underbrace{(\alpha + a)(\beta + b)}_{\text{Richiesto dalla struttura}} \stackrel{?}{=} \underbrace{\alpha\beta + a\beta + ab}_{\text{Ottenuto dal calcolo}}$$

Sviluppando il membro sinistro:

$$\alpha\beta + \alpha b + a\beta + ab \stackrel{?}{=} \alpha\beta + a\beta + ab$$

Cancellando i termini comuni, l'uguaglianza vale se e solo se:

$$\alpha b = 0$$

Poiché questo non è vero per ogni $a, b, \alpha, \beta \in \mathbb{Z}$ (ad esempio $\alpha = 1, b = 1$), l'insieme non è stabile. **Conclusione:** $A \cdot B$ non è un sottogruppo di G.

Il Caso Abeliano Se $(G, \cdot)$ fosse un gruppo **Abeliano** (commutativo), allora il prodotto di due sottogruppi sarebbe sempre un sottogruppo.

Proof. Siano $A, B \leq G$. Definiamo $A \cdot B = \{ab \mid a \in A, b \in B\}$.

1. *Stabilità:* Siano $x_1, x_2 \in A \cdot B$. Allora esistono $a_1, a_2 \in A$ e $b_1, b_2 \in B$ tali che $x_1 = a_1 b_1$ e $x_2 = a_2 b_2$.

   $$x_1 \cdot x_2 = (a_1 b_1) \cdot (a_2 b_2)$$

   Grazie alla commutatività di G, possiamo scambiare b_1 e a_2:

   $$= a_1 \cdot (a_2 \cdot b_1) \cdot b_2 = (a_1 a_2) \cdot (b_1 b_2)$$

   Poiché A e B sono sottogruppi stabili, $(a_1 a_2) \in A$ e $(b_1 b_2) \in B$. Quindi il prodotto appartiene ad $A \cdot B$.

2. *Inverso:* Sia $x = ab \in A \cdot B$.

   $$x^{-1} = (ab)^{-1} = b^{-1} a^{-1}$$

   Per la commutatività:

   $$= a^{-1} b^{-1}$$

   Poiché A, B sono sottogruppi, $a^{-1} \in A$ e $b^{-1} \in B$. Quindi $x^{-1} \in A \cdot B$.

Dunque $A \cdot B \leq G$.

□

Relazione tra A, B e l'unione Possiamo chiederci se i sottogruppi originali sono contenuti nel prodotto.

- Poiché $1_G \in B$, ogni $a \in A$ si scrive come $a \cdot 1_G$, quindi $A \subseteq A \cdot B$.
- Poiché $1_G \in A$, ogni $b \in B$ si scrive come $1_G \cdot b$, quindi $B \subseteq A \cdot B$.

Tornando al nostro gruppo G (Heisenberg), abbiamo visto che $A \cdot B$ fallisce perché G non è abeliano. Infatti:

$$X \cdot Y = \begin{pmatrix} 1 & a & ab \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad \neq \quad Y \cdot X = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

La condizione di non commutatività è $ab \neq 0$.

Il Sottogruppo C (Il Centro) Il sottogruppo C ha una proprietà speciale: i suoi elementi commutano con tutti. Verifichiamo la commutatività con A e B.

Sia $Z = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in C$.

Commutatività con A: Sia $X \in A$.

$$Z \cdot X = \begin{pmatrix} 1 & a & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad X \cdot Z = \begin{pmatrix} 1 & a & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies \text{UGUALI}$$

Commutatività con B: Sia $Y \in B$.

$$Y \cdot Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

$$Z \cdot Y = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \implies \text{UGUALI}$$

Poiché C commuta con gli altri sottogruppi, i prodotti $A \cdot C$ e $B \cdot C$ sono stabili e sono sottogruppi di G. Ad esempio:

$$A \cdot C = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| a, c \in \mathbb{Z} \right\} \leq G$$

Riepilogo: Costruzione di $\mathbb{Z}$ Torniamo alla definizione formale di $\mathbb{Z}$ come insieme quoziente $\frac{\mathbb{N}\times\mathbb{N}}{R}$. Dato un intero $z = [(a,b)]_R$, usiamo la proprietà di tricotomia per classificarlo:

$$z = [(a,b)]_R \implies \begin{cases} a < b \implies \exists d \in \mathbb{N}^* : b = a + d & \implies z = [(0,d)]_R \quad \text{(Interi Negativi)} \\ a = b & \implies z = [(0,0)]_R \quad \text{(Zero)} \\ b < a \implies \exists c \in \mathbb{N}^* : a = b + c & \implies z = [(c,0)]_R \quad \text{(Interi Positivi)} \end{cases}$$

Il Sistema Completo di Rappresentanti (SCR) per questa relazione è l'unione di tre insiemi disgiunti:

$$S.C.R. = \{(0,d) \mid d \in \mathbb{N}^*\} \cup \{(0,0)\} \cup \{(c,0) \mid c \in \mathbb{N}^*\}$$

L'Immersione Canonica

Definizione 0.49. Definiamo l'applicazione che identifica i numeri naturali all'interno degli interi:

$$\begin{aligned} j : \mathbb{N} &\longrightarrow \mathbb{Z} \\ x &\longmapsto [(x,0)]_R \end{aligned}$$

Proposizione 0.54. *Questa funzione gode di proprietà fondamentali:*

1. *È iniettiva.*
2. *È un omomorfismo rispetto alla somma:* $j(x+y) = j(x) + j(y)$.
3. *È un omomorfismo rispetto al prodotto:* $j(xy) = j(x) \cdot j(y)$

L'Ordine in $\mathbb{Z}$

Proposizione 0.55. *Definiamo la relazione d'ordine sui numeri interi ponendo:*

$$z_1 \leq z_2 \iff \exists x \in \mathbb{N} : z_2 = z_1 + j(x)$$

In pratica, z_1 è minore o uguale a z_2 se la differenza $z_2 - z_1$ è un intero non negativo (cioè appartiene all'immagine di $\mathbb{N}$). Verifichiamo che $\leq$ sia una relazione d'ordine:

Proof. **1. Riflessiva** Dobbiamo provare che $z_1 \leq z_1$. Basta scegliere $x = 0_{\mathbb{N}}$.

$$z_1 + j(0) = z_1 + 0_{\mathbb{Z}} = z_1$$

La condizione è soddisfatta.

2. Transitiva Ipotesi: $z_1 \leq z_2$ e $z_2 \leq z_3$. Dalle ipotesi sappiamo che esistono $x, y \in \mathbb{N}$ tali che:

$$z_2 = z_1 + j(x) \quad \text{e} \quad z_3 = z_2 + j(y)$$

Sostituendo z_2 nella seconda equazione:

$$z_3 = (z_1 + j(x)) + j(y) = z_1 + (j(x) + j(y)) = z_1 + j(x+y)$$

Poiché $x + y \in \mathbb{N}$, la condizione è soddisfatta: $z_1 \leq z_3$.

3. Antisimmetrica Ipotesi: $z_1 \leq z_2$ e $z_2 \leq z_1$. Esistono $x, y \in \mathbb{N}$ tali che:

$$z_2 = z_1 + j(x) \quad \text{e} \quad z_1 = z_2 + j(y)$$

Sostituendo:

$$z_1 = z_1 + j(x) + j(y) = z_1 + j(x+y)$$

Sottraendo z_1 (sfruttando la struttura di gruppo di $\mathbb{Z}$):

$$0_{\mathbb{Z}} = j(x+y)$$

Poiché j è iniettiva e $j(0_{\mathbb{N}}) = 0_{\mathbb{Z}}$, deve essere:

$$x + y = 0_{\mathbb{N}}$$

In $\mathbb{N}$, la somma di due numeri è zero se e solo se entrambi sono zero:

$$x = 0_{\mathbb{N}} \quad \text{e} \quad y = 0_{\mathbb{N}}$$

Quindi $j(x) = 0_{\mathbb{Z}}$. Tornando alla prima equazione:

$$z_2 = z_1 + 0_{\mathbb{Z}} = z_1$$

□

Compatibilità tra Ordine di $\mathbb{N}$ e $\mathbb{Z}$ L'ordine definito su $\mathbb{Z}$ estende fedelmente quello di $\mathbb{N}$.

Proposizione 0.56. *$\forall a, b \in \mathbb{N}$, si ha:*

$$a \leq b \text{ in } \mathbb{N} \iff j(a) \leq j(b) \text{ in } \mathbb{Z}$$

Proof. ($\implies$) Se $a \leq b$ in $\mathbb{N}$, allora $\exists x \in \mathbb{N}$ tale che $b = a + x$. Applicando j:

$$j(b) = j(a + x) = j(a) + j(x)$$

Questa è esattamente la definizione di $j(a) \leq j(b)$ in $\mathbb{Z}$.

($\impliedby$) Se $j(a) \leq j(b)$ in $\mathbb{Z}$, allora $\exists x \in \mathbb{N}$ tale che $j(b) = j(a) + j(x)$. Per l'omomorfismo: $j(b) = j(a + x)$. Per l'iniettività di j: $b = a + x$. Quindi $a \leq b$ in $\mathbb{N}$.

□

Caratterizzazione dei Positivi

Proposizione 0.57. *Possiamo identificare l'immagine di* $\mathbb{N}$ *come l'insieme degli interi non negativi:*

$$j(\mathbb{N}) = \{z \in \mathbb{Z} \mid 0_{\mathbb{Z}} \leq z\}$$

Proof. Se $0 \leq z$, allora $\exists x \in \mathbb{N}$ tale che $z = 0 + j(x) = j(x)$, quindi $z \in j(\mathbb{N})$. Viceversa, se $z \in j(\mathbb{N})$, allora $z = j(x) = 0 + j(x)$, quindi $0 \leq z$. □

Lemma dell'Inversione dell'Ordine

Lemma 0.58. *Passando agli opposti, il verso della disuguaglianza si inverte.*

$$z_1 \leq z_2 \implies -z_2 \leq -z_1$$

Proof. Per ipotesi $\exists x \in \mathbb{N}$ tale che $z_2 = z_1 + j(x)$. Prendiamo l'opposto di entrambi i membri:

$$-z_2 = -(z_1 + j(x)) = -z_1 - j(x)$$

Aggiungiamo $j(x)$ ad entrambi i lati (o portiamo $-j(x)$ a sinistra):

$$-z_2 + j(x) = -z_1$$

Questa uguaglianza ci dice esattamente che $-z_2 \leq -z_1$ (poiché $-z_1$ si ottiene aggiungendo un naturale a $-z_2$). □

Il Valore Assoluto

Definizione 0.50. Definiamo la funzione valore assoluto $|\cdot| : \mathbb{Z} \to \mathbb{Z}$ come:

$$|z| = \begin{cases} z & \text{se } 0 \leq z \\ -z & \text{se } z < 0 \end{cases}$$

Questa definizione copre interamente l'insieme $\mathbb{Z}$, sfruttando la sua decomposizione in parti disgiunte:

$$\mathbb{Z} = j(\mathbb{N}) \cup \{-j(x) \mid x \in \mathbb{N}^*\}$$

Esplicitando le classi di equivalenza, i due casi della definizione corrispondono a:

- **Casi non negativi ($0 \leq z$):** Sono le classi del tipo $z = [(x, 0)]_R$ (incluso lo zero $[(0, 0)]_R$). In questo caso $|z| = z$.
- **Casi negativi ($z < 0$):** Sono le classi del tipo $z = [(0, y)]_R$ con $y \in \mathbb{N}^*$. In questo caso $|z| = -z = [(y, 0)]_R$, che è un elemento positivo.

Proposizione 0.59. *$|z| \geq 0$ per ogni $z \in \mathbb{Z}$.*

Proof. Dobbiamo provare che il valore assoluto è sempre non negativo. Distinguiamo i due casi:

Caso $z < 0$: Applicando il Lemma (che inverte il verso della disuguaglianza passando agli opposti) alla relazione $z < 0$, otteniamo:

$$-0 < -z$$

Sapendo che $-0 = 0$ e che per definizione $|z| = -z$, si ha:

$$0 < |z|$$

Quindi in particolare $|z| \geq 0$.

- **Caso $0 \leq z$:** Per definizione $|z| = z$. Quindi la disuguaglianza $|z| \geq 0$ diventa $z \geq 0$, che è vera per ipotesi.

□

Proprietà del Valore Assoluto

Proposizione 0.60.
- ***Moltiplicatività:*** $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$
- ***Disuguaglianza Triangolare:*** $|z_1 + z_2| \leq |z_1| + |z_2|$

Identificazione Canonica Da questo momento in poi, identifichiamo ufficialmente l'insieme dei numeri naturali $\mathbb{N}$ con la sua immagine in $\mathbb{Z}$:

$$\mathbb{N} \equiv j(\mathbb{N}) = \{z \in \mathbb{Z} \mid 0 \leq z\}$$

Scriveremo quindi direttamente n al posto di $j(n)$ o delle classi $[(n, 0)]_R$.

Il Principio del Minimo (Buon Ordinamento) Questo principio è una conseguenza diretta degli assiomi di Peano e caratterizza l'insieme dei numeri naturali.

Teorema 0.61. *Sia $S \subseteq \mathbb{N}$ un sottoinsieme non vuoto ($S \neq \emptyset$). Allora esiste un elemento $m \in S$ tale che $m \leq x$ per ogni $x \in S$. Tale m si dice **minimo** di S.*

Proof. Dimostriamo la tesi per assurdo (o meglio, dimostriamo la contronominale): proviamo che se $S \subseteq \mathbb{N}$ è privo di minimo, allora S è vuoto.

Costruiamo l'insieme ausiliario A contenente i numeri naturali n il cui intervallo iniziale $[0, n]_{\mathbb{N}}$ è disgiunto da S:

$$A = \{n \in \mathbb{N} \mid [0, n]_{\mathbb{N}} \cap S = \emptyset\}$$

Il nostro obiettivo è dimostrare che $A = \mathbb{N}$ (usando l'induzione), il che implicherà che nessun naturale sta in S, dunque $S = \emptyset$.

1. Base ($0 \in A$) Se per assurdo $0 \notin A$, allora l'intersezione $[0, 0]_{\mathbb{N}} \cap S$ non sarebbe vuota. Poiché l'intervallo contiene solo lo zero, avremmo $0 \in S$. Essendo 0 il minimo assoluto di $\mathbb{N}$ ($0 \leq x, \forall x$), sarebbe automaticamente anche il minimo di S. Questo contraddice l'ipotesi che S non abbia minimo. Dunque necessariamente $0 \in A$.

2. Passo Induttivo ($z \in A \implies z + 1 \in A$) Sia $z \in A$. Per definizione, questo significa che non ci sono elementi di S nell'intervallo $[0, z]_{\mathbb{N}}$. Vogliamo provare che anche $z + 1 \in A$. Ragioniamo per assurdo: se $z + 1 \notin A$, allora l'intervallo $[0, z + 1]_{\mathbb{N}}$ tocca S. Dato che fino a z non c'era nulla, deve essere per forza che $z + 1 \in S$.

Ora, prendiamo un qualsiasi $x \in S$. Poiché $z \in A$, sappiamo che x non può essere minore o uguale a z, quindi deve essere strettamente maggiore: $x > z$. Nei numeri naturali, se $x > z$ allora $x \geq z + 1$. Abbiamo quindi dimostrato che $z + 1 \in S$ e che per ogni $x \in S$, $z + 1 \leq x$. Questo farebbe di $z + 1$ il minimo di S, il che è impossibile per ipotesi.

L'assurdo deriva dall'aver supposto $z + 1 \notin A$. Quindi $z + 1 \in A$.

Conclusione Per il principio di induzione, $A = \mathbb{N}$. Poiché per ogni $n \in \mathbb{N}$ l'intervallo $[0, n]$ non interseca S, nessun numero naturale appartiene a S. Dunque $S = \emptyset$. □

Lemma di Divisione Euclidea in $\mathbb{Z}$

Lemma 0.62. *Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Allora esistono e sono unici due interi q (quoziente) ed r (resto) tali che:*

$$a = bq + r \quad con \quad 0 \leq r < |b|$$

Esistenza

Proof. Distinguiamo due casi per il dividendo a. **I Caso:** $0 \leq a$ Consideriamo l'insieme:

$$S = \{a - bx \mid x \in \mathbb{Z},\ 0 \leq a - bx\}$$

Osserviamo che:

- $S \subseteq \mathbb{Z}$ e tutti gli elementi sono positivi o nulli, quindi $S \subseteq \mathbb{N}$.
- $S \neq \emptyset$ perché $a \in S$ (scegliendo $x = 0$, si ha $a - b(0) = a \geq 0$).

Per il principio del buon ordinamento, esiste il minimo di S:

$$\exists m = \min S$$

Poiché $m \in S$, esiste un $\bar{x} \in \mathbb{Z}$ tale che $m = a - b\bar{x}$. Quindi possiamo scrivere $a = b\bar{x} + m$ con $m \geq 0$.

Dobbiamo provare che $m < |b|$. Supponiamo per assurdo che $m \geq |b|$. Allora $m - |b| \geq 0$. Analizziamo il valore $m - |b|$ in base al segno di b:

$$\begin{cases} b > 0 \implies m - b = (a - b\bar{x}) - b = a - b(\bar{x} + 1) \\ b < 0 \implies m - (-b) = m + b = (a - b\bar{x}) + b = a - b(\bar{x} - 1) \end{cases}$$

In entrambi i casi, l'espressione è della forma $a - b(\text{intero})$ ed è ≥ 0. Quindi $m - |b| \in S$. Tuttavia, essendo $b \neq 0$, si ha $|b| > 0$, quindi:

$$m - |b| < m$$

Questo contraddice il fatto che m sia il minimo di S. Dunque deve essere $m < |b|$. Ponendo $q = \bar{x}$ e $r = m$, l'esistenza è dimostrata per $a \geq 0$.

II Caso: $a < 0$ Se $a < 0$, allora $-a > 0$. Applicando il risultato del I Caso a $-a$, sappiamo che esistono $s, t \in \mathbb{Z}$ tali che:

$$-a = bs + t \quad \text{con} \quad 0 \leq t < |b|$$

Ora distinguiamo due sottocasi per t:

- *Sottocaso (i):* $t = 0$. Allora $-a = bs \implies a = b(-s)$. Scegliamo $q = -s$ e $r = 0$. Si ha $a = bq + r$ con $0 \leq r < |b|$.
- *Sottocaso (ii):* $t \neq 0$. Allora $0 < t < |b|$, il che implica $0 < |b| - t < |b|$. Partiamo da $-a = bs + t$:

  $$a = -(bs + t) = b(-s) - t$$

  Aggiungiamo e sottraiamo $|b|$ per ottenere un resto positivo:

  $$a = b(-s) - |b| + (|b| - t)$$

  Distinguiamo in base al segno di b:

  $$\begin{cases} b > 0 \implies b(-s) - b + (|b| - t) = b(-s - 1) + (|b| - t) & \to q = -s - 1 \\ b < 0 \implies b(-s) + b + (|b| - t) = b(-s + 1) + (|b| - t) & \to q = -s + 1 \end{cases}$$

  In entrambi i casi poniamo $r = |b| - t$. Abbiamo ottenuto $a = bq + r$ con $0 < r < |b|$.

□

Esempi Pratici

Caso $t = 0$

Esempio 0.35. $a = -18,\ b = 3$. Consideriamo $-a = 18$.

$$18 = 3 \cdot 6 + 0 \implies s = 6,\ t = 0$$

$$-18 = 3 \cdot (-6) + 0 \implies q = -6,\ r = 0$$

Caso $t \neq 0$

Esempio 0.36. $a = -20,\ b = 3$. Consideriamo $-a = 20$.

$$20 = 3 \cdot 6 + 2 \implies s = 6,\ t = 2$$

La formula prevede $r = |b| - t = 3 - 2 = 1$. Passaggi algebrici:

$$-20 = -(3 \cdot 6 + 2) = 3(-6) - 2 = 3(-6) \underbrace{-3 + 3}_{0} - 2$$

$$= 3(-6) - 3 + (3 - 2) = 3(-6 - 1) + 1 = 3(-7) + 1$$

Quindi $q = -7,\ r = 1$.

Unicità

Proof. Siano q_1, r_1 e q_2, r_2 due coppie di soluzioni:

$$\begin{cases} a = bq_1 + r_1 & 0 \leq r_1 < |b| \\ a = bq_2 + r_2 & 0 \leq r_2 < |b| \end{cases}$$

Supponiamo per assurdo che $r_1 \neq r_2$. Senza perdita di generalità, sia $r_2 > r_1$. Sottraendo le due equazioni ($a - a = 0$):

$$0 = bq_1 + r_1 - (bq_2 + r_2) \implies r_2 - r_1 = b(q_1 - q_2)$$

Poiché $r_2 > r_1$, si ha $r_2 - r_1 > 0$. Passando ai valori assoluti:

$$|r_2 - r_1| = |b| \cdot |q_1 - q_2|$$

Sappiamo che $r_2 - r_1 \leq r_2 < |b|$ (poiché $r_1 \geq 0$). Quindi:

$$|b| \cdot |q_1 - q_2| < |b|$$

Poiché $|b| > 0$, dividiamo per $|b|$:

$$|q_1 - q_2| < 1$$

Essendo q_1, q_2 interi, la differenza $|q_1 - q_2|$ è un intero non negativo minore di 1, quindi deve essere 0.

$$|q_1 - q_2| = 0 \implies q_1 = q_2$$

Sostituendo nell'equazione della differenza:

$$r_2 - r_1 = b(0) = 0 \implies r_2 = r_1$$

Questo contraddice l'ipotesi $r_2 > r_1$. Dunque l'unica possibilità è $r_1 = r_2$ e $q_1 = q_2$. □

Divisibilità in $\mathbb{Z}$

Definizione 0.51. Siano $a, b \in \mathbb{Z}$. Diciamo che a **divide** b se:

$$\exists x \in \mathbb{Z} : b = ax$$

Si scrive $a|b$. In tal caso a è un **divisore** di b e b è un **multiplo** di a.

Proprietà della divisibilità

Proposizione 0.63.
- ***Riflessiva:*** $a|a \quad \forall a \in \mathbb{Z}$;
- ***Transitiva:*** $a|b \wedge b|c \implies a|c$;
- ***Divisore Universale:*** $1|a \quad \forall a \in \mathbb{Z}$;
- ***Divisori dell'Unità:*** $a|1 \iff a = 1 \vee a = -1$;
- ***Antisimmetria (a meno del segno):*** $a|b \wedge b|a \iff a = b \vee a = -b$.

Proof.
- **Riflessiva:** Infatti $a = a \cdot 1$.
- **Transitiva:** $b = ax,\ c = by \implies c = (ax)y = a(xy)$. Poiché $xy \in \mathbb{Z}$, $a|c$..
- **Divisore Universale:** Infatti $a = 1 \cdot a$.
- **Divisori dell'Unità:**

  $\implies$ Se $ax = 1$, passando ai valori assoluti in $\mathbb{N}$: $|a| \cdot |x| = |1| = 1$. In $\mathbb{N}$, il prodotto di due numeri è 1 solo se entrambi sono 1. Quindi $|a| = 1 \implies a = \pm 1$.

  $\impliedby$ $1 = 1 \cdot 1$ e $1 = (-1)(-1)$.
- **Antisimmetria (a meno del segno):**

  $\implies$ Ovvio.

  $\impliedby$ Se $b = ax$ e $a = by$, allora $a = (by)x = a(yx)$.

  $$a(1 - yx) = 0.$$

  Due casi:
  - Se $a = 0$, allora $b = 0 \cdot x = 0$, quindi $a = b$.
  - Se $a \neq 0$, allora $1 - yx = 0 \implies yx = 1$. Poiché sono interi, o $x = y = 1$ (quindi $a = b$) o $x = y = -1$ (quindi $a = -b$).

□

Divisori Banali e Numeri Primi

Definizione 0.52. Un numero a e il suo opposto $-a$ condividono gli stessi divisori. I **divisori banali** di un intero a sono $\{1, -1, a, -a\}$. Un numero $p \in \mathbb{Z}$ si dice **primo** se:

1. $p \notin \{1, -1, 0\}$
2. Gli unici divisori di p sono quelli banali.

$$\{\text{Divisori di } p\} = \{1, -1, p, -p\}.$$

Aritmetica Modulare Richiamiamo la struttura $(\mathbb{Z}, +, \cdot)$ e la funzione valore assoluto:

$$z \longmapsto |z| = \begin{cases} z & z \geq 0 \\ -z & z < 0 \end{cases}$$

Divisione Euclidea

Lemma 0.64.

$$\forall a, b \in \mathbb{Z}, b \neq 0, \exists! q, r \in \mathbb{Z} : a = bq + r \ \ e \ 0 \leq r < |b|$$

Divisibilità

Definizione 0.53. Diciamo che a **divide** b (scritto $a|b$) in $\mathbb{Z}$ se:

$$a|b \iff \exists x \in \mathbb{Z} : b = ax$$

Relazione di Congruenza

Definizione 0.54. Sia $n \in \mathbb{Z}, n > 1$. Siano $a, b \in \mathbb{Z}$. Diciamo che a è congruo a b modulo n se la loro differenza è un multiplo di n. Si scrive:

$$a \equiv b \pmod{n} \quad \text{oppure} \quad a \equiv_n b \iff n|(a-b)$$

Proprietà della Congruenza

Proposizione 0.65. *La congruenza è una relazione di equivalenza in $\mathbb{Z}$, compatibile con le operazioni di somma e prodotto.*

Relazione di Equivalenza

Proof.

- **Riflessiva:** $\forall a \in \mathbb{Z},\ a \equiv_n a$. Infatti $a - a = 0$ e $n|0$ (poiché $0 = n \cdot 0$).
- **Transitiva:** $\forall a, b, c \in \mathbb{Z}$, se $a \equiv_n b$ e $b \equiv_n c$, allora $a \equiv_n c$. Ipotesi: $n|(a-b)$ e $n|(b-c)$. Cioè $\exists x, y \in \mathbb{Z}$ tali che $a - b = nx$ e $b - c = ny$. Sommando le uguaglianze:

  $$a - c = (a - b) + (b - c) = nx + ny = n(x + y)$$

  Quindi $n|(a-c)$, ovvero $a \equiv_n c$.
- **Simmetrica:** $\forall a, b \in \mathbb{Z}$, se $a \equiv_n b$ allora $b \equiv_n a$. Ipotesi: $n|(a-b)$, cioè $\exists x \in \mathbb{Z} : a - b = nx$. Moltiplicando per -1:

  $$b - a = -(a - b) = -(nx) = n(-x)$$

  Quindi $n|(b-a)$, ovvero $b \equiv_n a$.

□

Compatibilità con le operazioni

Proof. Siano $a \equiv_n \alpha$ e $b \equiv_n \beta$. Ciò significa che $\exists x, y \in \mathbb{Z}$ tali che:

$$a - \alpha = nx \implies a = \alpha + nx$$

$$b - \beta = ny \implies b = \beta + ny$$

1. **Somma** Calcoliamo $a + b$:

   $$a + b = (\alpha + nx) + (\beta + ny) = (\alpha + \beta) + n(x + y)$$

   Portando i termini a sinistra:

   $$(a + b) - (\alpha + \beta) = n(x + y)$$

   Dunque n divide la differenza, quindi $(a + b) \equiv_n (\alpha + \beta)$.

2. **Prodotto** Calcoliamo ab:

$$ab = (\alpha + nx) \cdot (\beta + ny) = \alpha\beta + \alpha ny + nx\beta + nxny$$

Raccogliamo n dai termini che lo contengono:

$$ab = \alpha\beta + n\underbrace{(\alpha y + x\beta + xny)}_{Z \in \mathbb{Z}}$$

$$ab - \alpha\beta = n \cdot Z$$

Dunque $n|(ab - \alpha\beta)$, quindi $ab \equiv_n \alpha\beta$.

□

L'Insieme Quoziente $\mathbb{Z}_n$ La classe di equivalenza di a si indica con $[a]_{\equiv_n}$ o semplicemente $[a]_n$.

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv_n a\}$$

L'insieme quoziente è definito come:

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv_n} = \{[a]_n \mid a \in \mathbb{Z}\}$$

Grazie alla compatibilità dimostrata sopra, le operazioni su $\mathbb{Z}_n$ sono ben definite (non dipendono dal rappresentante scelto):

- $[a]_n + [b]_n = [a + b]_n$
- $[a]_n \cdot [b]_n = [ab]_n$

Struttura Algebrica di $\mathbb{Z}_n$ La terna $(\mathbb{Z}_n, +, \cdot)$ è un **Anello Commutativo Unitario**.

1. $(\mathbb{Z}_n, +)$ è un gruppo abeliano. L'elemento neutro è $0_{\mathbb{Z}_n} = [0]_n$. L'opposto è $-[a]_n = [-a]_n$.
2. $(\mathbb{Z}_n, \cdot)$ è un monoide commutativo. L'elemento neutro è $1_{\mathbb{Z}_n} = [1]_n$. Nota: $[1]_n \neq [0]_n$ poiché $n > 1$ (se fossero uguali, n dividerebbe 1, assurdo).
3. Vale la proprietà distributiva:

$$[a]_n \cdot ([b]_n + [c]_n) = [a]_n[b + c]_n = [a(b + c)]_n = [ab + ac]_n = [ab]_n + [ac]_n = [a]_n[b]_n + [a]_n[c]_n$$

Cardinalità e Rappresentanti Quanti elementi ha $\mathbb{Z}_n$?

Lemma 0.66. *Sia $T_n = \{0, 1, \ldots, n-1\} = [0, n-1]_{\mathbb{N}}$. Allora T_n è un Sistema Completo di Rappresentanti per la congruenza modulo n. Cioè: $\forall y \in \mathbb{Z}, \exists! t \in T_n : y \equiv_n t$.*

Proof.
- **Esistenza:** Per il lemma di divisione euclidea, dato $y \in \mathbb{Z}$, esistono unici q, r tali che $y = nq + r$ con $0 \leq r < n$. Quindi $y - r = nq \implies y \equiv_n r$. Poiché $0 \leq r \leq n - 1$, $r \in T_n$.
- **Unicità:** Supponiamo esistano $t_1, t_2 \in T_n$ tali che $y \equiv_n t_1$ e $y \equiv_n t_2$. Allora $y = nq_1 + t_1$ e $y = nq_2 + t_2$, con $0 \leq t_1, t_2 < n$. Sia t_1 che t_2 soddisfano le condizioni per essere il resto della divisione euclidea di y per n. Per l'unicità del resto, $t_1 = t_2$.

□

Corollario 3. *La cardinalità di $\mathbb{Z}_n$ è n.*

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

Esempi

Caso $n = 2$

Esempio 0.37. $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$.

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

L'unico elemento non nullo $[1]_2$ è invertibile ($1 \cdot 1 = 1$). $\implies U(\mathbb{Z}_2) = \{[1]_2\} = \mathbb{Z}_2^*$. $(\mathbb{Z}_2, +, \cdot)$ è un **Campo**.

Caso $n = 3$

Esempio 0.38. $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

x	x^{-1}
$[1]$	$[1]$
$[2]$	$[2]$

Tutti gli elementi non nulli sono invertibili. $U(\mathbb{Z}_3) = \mathbb{Z}_3^*$. $(\mathbb{Z}_3, +, \cdot)$ è un **Campo**.

Caso $n = 4$

Esempio 0.39. $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[\mathbf{0}]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

x	x^{-1}
$[0]$	NO
$[1]$	$[1]$
$[2]$	NO (divisore dello zero)
$[3]$	$[3]$

Si nota che $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$. $U(\mathbb{Z}_4) = \{[1]_4, [3]_4\} \neq \mathbb{Z}_4^*$. $(\mathbb{Z}_4, +, \cdot)$ non è un campo e non è nemmeno un dominio di integrità.

Caso $n = 8$ **(Notazione** $\bar{a}$**)**

Esempio 0.40. $\mathbb{Z}_8 = \{\bar{0}, \ldots, \bar{7}\}$. Tavola della moltiplicazione:

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Analisi degli inversi:

x	x^{-1}
$\bar{1}$	$\bar{1}$
$\bar{3}$	$\bar{3}$
$\bar{5}$	$\bar{5}$
$\bar{7}$	$\bar{7}$
Pari	Non invertibili

$U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \neq \mathbb{Z}_8^*$. $(\mathbb{Z}_8, +, \cdot)$ non è un campo né un dominio di integrità.