

# Appunti di Logica e Algebra 2

Pietro Pizzoccheri

2024

## Indice

<b>1</b>	<b>Teoria degli anelli commutativi e dei campi</b>	<b>2</b>
1.1	Insiemi . . . . .	2
1.1.1	Operazioni tra insiemi . . . . .	2
1.2	Funzioni . . . . .	2
1.2.1	Composizione di funzioni . . . . .	3
1.2.2	Operazioni su insiemi . . . . .	3
1.3	Monoidi e Gruppi . . . . .	4
1.4	Morfismi . . . . .	5
1.5	Relazioni . . . . .	8
1.5.1	Insieme quoziente per gruppi abeliani . . . . .	9

# 1 Teoria degli anelli commutativi e dei campi

## 1.1 Insiemi

Un insieme è una collezione di oggetti, detti elementi dell'insieme.

$\mathbb{N} := \{0, 1, 2, 3, \dots\}$  insieme dei numeri naturali

$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$  insieme degli interi

$\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$  insieme dei numeri razionali

$\mathbb{R} :=$  insieme dei numeri reali

$\mathbb{C} :=$  insieme dei numeri complessi

### 1.1.1 Operazioni tra insiemi

$\subseteq$  inclusione tra insiemi

$\subsetneq$  inclusione propria tra insiemi

$X \subseteq Y$  si legge "X è sottoinsieme di Y" o "X è incluso in Y"

Se  $X$  è un insieme finito, indico con  $|X|$  il numero di elementi di  $X$ , detto anche la **cardinalità di  $X$** .

$\emptyset$  : Insieme vuoto e  $|\emptyset| = 0$

Siano  $X$  e  $Y$  due insiemi. L'insieme  $X \times Y := \{(x, y) : x \in X, y \in Y\}$  lo chiamiamo **prodotto cartesiano** di  $X$  e  $Y$ .

Sia  $A \in \mathcal{P}(X)$ , dove  $\mathcal{P}(X) := \{A : A \subseteq X\}$  è detto **Insieme delle parti di  $X$** . L'insieme  $A^c := X \setminus A$  è detto **complementare** di  $A$ .

## 1.2 Funzioni

Siano  $X$  e  $Y$  due insiemi. **Una funzione  $f$  da  $X$  a  $Y$**  è un sottoinsieme  $F \subseteq X \times Y$  tale che:

- $(x, y_1) \in F, (x, y_2) \in F \implies y_1 = y_2, \forall x \in X, y_1, y_2 \in Y$ .
- $x \in X \implies \exists y \in Y$  tale che  $(x, y) \in F$

Una funzione  $F \subseteq X \times Y$  la indichiamo con  $f : X \rightarrow Y$ . E scriviamo  $f(x) = y$  se  $(x, y) \in F$ .

**Definizione:** La funzione  $Id_x : X \rightarrow X$  tale che  $Id_x(x) = x, \forall x \in X$  la chiamiamo **funzione identità su  $X$**

**Definizione:** Una funzione  $f : X \rightarrow Y$  è **iniettiva** se  $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$

**Definizione:** Una funzione  $f : X \rightarrow Y$  è **suriettiva** se  $Im(f) = Y$ , dove  $Im(f) = \{y \in Y : \exists x \in X \text{ tale che } f(x) = y\}$  è detta **immagine di  $f$**

**Definizione:** Una funzione  $f : X \rightarrow Y$  è **biunivoca** se è sia iniettiva che suriettiva.

### 1.2.1 Composizione di funzioni

Siano  $f : X \rightarrow Y$  e  $g : Y \rightarrow Z$  due funzioni. La **composizione di  $f$  e  $g$**  è la funzione  $g \circ f : X \rightarrow Z$  tale che  $(g \circ f)(x) = g(f(x))$ ,  $\forall x \in X$ .

**Definizione:** una funzione  $f : X \rightarrow Y$  è detta **invertibile** se esiste una funzione  $g : Y \rightarrow X$  tale che

- $g \circ f = Id_X$
- $f \circ g = Id_Y$

la funzione  $g$  è detta **funzione inversa di  $f$**  e la indichiamo con  $f^{-1}$ .

Una funzione  $f : X \rightarrow Y$  è invertibile se e solo se è biunivoca.

### 1.2.2 Operazioni su insiemi

**Definizione:** Una funzione  $f : X \times X \rightarrow X$  è detta **operazione su  $X$** . Invece di  $f(x, y)$  scriveremo  $x \cdot y$ .

**Definizione:** Un'operazione  $\cdot$  su  $X$  è detta **associativa** se  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ,  $\forall x, y, z \in X$ .

**Definizione:** Un'operazione  $\cdot$  su  $X$  è detta **commutativa** se  $x \cdot y = y \cdot x$ ,  $\forall x, y \in X$ .

#### Esempio:

- $\mathcal{P}(X)$  con l'operazione di unione  $\cup$  è associativa e commutativa, così come lo è con l'intersezione  $\cap$ .
- $A \setminus B := A \cap B^C$  (**differenza insiemistica**) è un'operazione su  $\mathcal{P}(X)$ .  
non è associativa: sia  $A \neq \emptyset$ . Allora  $A \setminus (A \setminus A) = A \neq (A \setminus A) \setminus A = \emptyset$   
non è commutativa:  $A \setminus \emptyset = A \neq \emptyset \setminus A = \emptyset$ , se  $A \neq \emptyset$
- $A \Delta B := (A \setminus B) \cup (B \setminus A)$  (**differenza simmetrica**) è un'operazione su  $\mathcal{P}(X)$ .  
è commutativa e anche associativa, facilmente verificabile coi diagrammi di Venn.
- Sia  $F(X) := \{f : X \rightarrow X\}$ .  
La composizione "  $\circ$  " è un'operazione su  $F(X)$ .  
è associativa, ma non è commutativa.
- $a \circ b = \frac{a+b}{2}$  è un'operazione commutativa su  $\mathbb{Q}$ , ma non associativa.

**Definizione:** Sia  $\cdot$  un'operazione su  $X$ . Un elemento  $e \in X$  tale che  $e \cdot x = x \cdot e = x$ ,  $\forall x \in X$  è detto **elemento neutro o identità**.

L'identità è unica; se  $e, e' \in X$  sono due identità, allora  $e = e \cdot e' = e'$ .

## 1.3 Monoidi e Gruppi

**Definizione:** Un insieme  $X$  con un'operazione associativa e un'identità è detto **monoide**.

**Esempio:**

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  con l'addizione e identità 0 sono monoidi.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  con la moltiplicazione e identità 1 sono monoidi.
- $\mathcal{P}(X)$  con  $\cup$  e come identità l'insieme  $X$  è un monoide.
- $\mathcal{P}(X)$  con  $\cap$  e come identità l'insieme vuoto è un monoide.
- $F(X) := \{f : X \rightarrow X\}$  con la composizione "o" e come identità la funzione identità ( $Id_X$ ) è un monoide.

**Definizione:** Sia  $X$  un monoide. Un elemento  $x \in X$  è detto **invertibile** se esiste  $y \in X$  tale che  $x \cdot y = y \cdot x = e$ , dove  $e$  è l'identità di  $X$ . L'elemento  $y$  è detto **inverso** di  $x$ .

Se  $x \in X$  è invertibile, il suo inverso è unico e lo indichiamo con  $x^{-1}$ .  
L'identità del monoide è invertibile e il suo inverso è l'identità stessa.

**Esempio:**

- L'insieme degli elementi invertibili di  $(\mathbb{N}, +)$  è  $\{0\}$ .
- L'insieme degli elementi invertibili di  $(\mathbb{Z}, +)$  è  $\mathbb{Z}$ , di  $(\mathbb{Q}, +)$  è  $\mathbb{Q}$ , di  $(\mathbb{R}, +)$  è  $\mathbb{R}$ , di  $(\mathbb{C}, +)$  è  $\mathbb{C}$ .
- L'insieme degli elementi invertibili di  $(\mathbb{N}, \cdot)$  è  $\{1\}$ , di  $(\mathbb{Z}, \cdot)$  è  $\{1, -1\}$ , di  $(\mathbb{Q}, \cdot)$  è  $\mathbb{Q} \setminus \{0\}$ , di  $(\mathbb{R}, \cdot)$  è  $\mathbb{R} \setminus \{0\}$ , di  $(\mathbb{C}, \cdot)$  è  $\mathbb{C} \setminus \{0\}$ .
- L'insieme degli elementi invertibili di  $F(X) = \{f : X \rightarrow X\}$  è l'insieme delle funzioni invertibili.

**Definizione:** Un monoide  $X$  è detto **gruppo** se ogni suo elemento è invertibile. Se l'operazione è commutativa, il gruppo è detto **gruppo abeliano**.

**Esempio:**

- $(\mathcal{P}(x), \Delta)$  è un gruppo abeliano. L'identità è l'insieme vuoto e l'inverso di  $A \in \mathcal{P}(x)$  è  $A$  stesso. ( $A^2 = \emptyset, \forall A \subseteq X$ )
- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$  sono gruppi abeliani
- $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$  sono gruppi abeliani
- sia  $X = \{1, 2, \dots, n\}$  l'insieme delle funzioni invertibili  $f : X \rightarrow X$  è il **Gruppo delle permutazioni di  $n$  elementi (o gruppo simmetrico)**. Lo indiciamo con  $S_n$ .  $|S_n| = n!$ . Non è abeliano se  $n \geq 3$ .

**Definizione:** Sia  $X$  un monoide con identità  $e$ . Un sottoinsieme  $Y \subseteq X$  tale che  $e \in Y$  e  $Y$  è chiuso rispetto all'operazione di  $X$  è detto **sottomonide di  $X$** . Analogamente definiamo la nozione di **sottogruppo di  $X$** . il gruppo  $\{e\}$  è detto **sottogruppo banale di  $X$** .

### Esempio:

- Con l'addizione,  $\{0\}$  è un sottomonoido di  $\mathbb{N}$ .  $\{0\}$  è anche sottogruppo banale.
- Con la moltiplicazione abbiamo la catena di sottomonoidi  $\{1\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$  e di sottogruppi  $\{1\} \subseteq \mathbb{Q} \setminus \{0\} \subseteq \mathbb{R} \setminus \{0\} \subseteq \mathbb{C} \setminus \{0\}$
- con l'addizione abbiamo la catena di sottogruppi  $\{0\} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

**Definizione:** Sia  $X$  un monoide e  $S \subseteq X$  un sottoinsieme. L'insieme  $\langle S \rangle := \{x_1 \cdot x_2 \cdots x_n : n \in \mathbb{N}, x_1, x_2, \dots, x_n \in S\}$  è detto **sottomonoido generato da  $S$**  (intersezione di tutti i sottomonoidi di  $X$  che contengono  $S$ ). Se  $X$  è un gruppo,  $\langle S \rangle$  è detto **sottogruppo generato da  $S$** .

### Esempio:

- $S = \{1\} \subseteq (\mathbb{N}, +)$ . Allora  $\langle S \rangle = \{0, 1, 2, \dots\} = \mathbb{N}$
- sia  $S := \{p \in \mathbb{N} : p \text{ è primo}\} \cup \{0\} \subseteq (\mathbb{N}, \cdot)$ . allora  $\langle S \rangle = \mathbb{N}$
- $S = \{0, 1\} \subseteq (\mathbb{N}, \cdot)$ . Allora  $\langle S \rangle = \{0, 1\}$
- sia  $S = \{1\} \subseteq (\mathbb{Z}, +)$ . il sottogruppo generato da  $S$  è  $\langle S \rangle = \mathbb{Z}$
- uno spazio vettoriale  $V$  è un gruppo abeliano se consideriamo l'operazione di addizione fra vettori. Prendiamo  $V = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ . Sia  $v = (1, 1) \in \mathbb{R}^2$ . Il sottogruppo  $\langle \{v\} \rangle = \{(n, n) : n \in \mathbb{Z}\}$  è un sottogruppo proprio del sottospazio generato da  $\{v\}$ . Sia  $v_1 = (1, 0)$  ed  $v_2 = (0, 1)$ , allora il sottogruppo  $\langle \{v_1, v_2\} \rangle$  è  $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R} \times \mathbb{R}$

**Definizione:** Siano  $M_1, M_2$  con identità  $e_1, e_2$  rispettivamente. Si definisce prodotto diretto di  $M_1$  e  $M_2$  l'insieme  $M_1 \times M_2$  con l'operazione  $(m_1, m_2) \cdot (m'_1, m'_2) = (m_1 \cdot m'_1, m_2 \cdot m'_2)$  e identità  $(e_1, e_2)$ . Analogamente si definisce prodotto diretto di gruppi  $G_1, G_2$ .

L'inverso di una coppia  $(a, b) \in G_1 \times G_2$  è  $(a^{-1}, b^{-1})$ .

## 1.4 Morfismi

**Definizione:** Siano  $M_1, M_2$  monoidi con identità  $e_1, e_2$ . Una funzione  $f : M_1 \rightarrow M_2$  è un **morfismo di monoidi se**:

- $f(e_1) = e_2$
- $f(xy) = f(x)f(y)$

**Definizione:** Siano  $G_1, G_2$  gruppi con identità  $e_1, e_2$ . Una funzione  $f : G_1 \rightarrow G_2$  è un **morfismo di gruppi se**:

- $f(e_1) = e_2$
- $f(xy) = f(x)f(y)$

**Definizione:** Il **nucleo** di un morfismo di monoidi  $f : M_1 \rightarrow M_2$  è il sottomonoido di  $M_1$  definito come:  $\text{Ker}(f) := \{x \in M_1 : f(x) = e_2\}$

**Definizione:** Il nucleo di un morfismo di gruppi  $f : G_1 \rightarrow G_2$  è il sottogruppo di  $G_1$  definito come:  $\text{Ker}(f) := \{x \in G_1 : f(x) = e_2\}$ . Il nucleo è un sottogruppo di  $G_1$ . e  $\text{Im}(f)$  è un sottogruppo di  $G_2$ .

**Definizione:** Un isomorfismo di monoidi (e di gruppi) è un morfismo biunivoco, tale che la funzione inversa sia un morfismo.

**Proposizione:** Sia  $f : M_1 \rightarrow M_2$  un morfismo di monoidi. Se  $f$  è biunivoco, allora è un isomorfismo. Questo vale anche per i gruppi.

**Dimostrazione:** Dobbiamo far vedere che la funzione inversa  $f^{-1} : M_2 \rightarrow M_1$  è un morfismo di monoidi. Poiché  $f(e_1) = e_2$ , allora  $f^{-1}(e_2) = e_1$ . Siano  $x_2, y_2 \in M_2$ , allora esistono  $x_1, y_1 \in M_1$  tali che  $f(x_1) = x_2, f(y_1) = y_2$ . Quindi  $f^{-1}(f(x_1)f(y_1)) = f^{-1}(f(x_1y_1)) = x_1y_1 = f^{-1}(x_2)f^{-1}(y_2)$

**Esempio:**

- Siano  $M_1 = (\mathcal{P}(X), \cup)$  e  $M_2 = (\mathcal{P}(X), \cup)$ , dove  $X$  è un insieme. Sia  $f : M_1 \rightarrow M_2$  definita ponendo  $f(A) = A^C, \forall A \subseteq X$ . la funzione  $f$  è biunivoca. Inoltre, dalle formule di De Morgan segue che  $f(A \cap B) = (A \cap B)^C = A^C \cup B^C = f(A) \cup f(B)$ . Quindi  $f$  è un isomorfismo di monoidi, poiché  $f(X) = X^C = \emptyset$ , essendo  $X$  l'identità di  $M_1$  e  $\emptyset$  l'identità di  $M_2$ .
- Sia  $\mathbb{Z}_2 := \{0, 1\}$  con l'operazione definita come:  $0+0=0, 0+1=1+0=1, 1+1=0$ . Sia  $X := \{1, 2, \dots, n\}, n \in \mathbb{N}$ . La funzione  $f : \mathcal{P}(X) \rightarrow \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$  ( $n$  volte) definita da:  $f(A) = (a_1, a_2, \dots, a_n)$ , dove  $a_i = 1$  se  $i \in A$  e  $a_i = 0$  se  $i \notin A$ .  
è un isomorfismo del gruppo  $(\mathcal{P}(X), \Delta)$  con il gruppo  $\mathcal{P}(X) \rightarrow \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2 = (\mathbb{Z}_2)^n$

**Vediamo ora come ogni monoide finito è isomorfo a un monoide di matrici quadrate, dove l'operazione è il prodotto righe per colonne.**

Sia  $M = \{x_1, \dots, x_n\}$  un monoide,  $|M| = n \in \mathbb{N}$ , con identità  $e = x_1$ . Pero ogni  $x \in M$  definiamo una matrice  $A(x) \in \text{Mat}_{n \times n}(\mathbb{Z})$  nel seguente modo:  $A(x)_{ij} = 1$  se  $x_i \cdot x = x_j$  e  $A(x)_{ij} = 0$  altrimenti. La funzione  $F : M \rightarrow \text{Mat}_{n \times n}(\mathbb{Z})$  ( $x \mapsto A(x)$ ) è iniettiva.

Infatti, se  $A(x) = A(y)$ , allora  $A(x)_{i1} = A(y)_{i1}, \forall i \in \{1, \dots, n\}$ .

Quindi se  $A(x)_{i1} = A(y)_{i1} = 1$ , allora  $xx_1 = xe = x = yx_1 = y$ .

Risulta inoltre facile vedere che  $A(xy) = A(x)A(y)$  (prodotto righe per colonne), ossia che  $F$  è un morfismo di monoidi ( $\text{Mat}_{n \times n}(\mathbb{Z})$  è un monoide con l'operazione di prodotto righe per colonne, la cui identità è la matrice  $I_n$ ).

Quindi  $F : M \rightarrow \text{Im}(F)$  è un isomorfismo di monoidi.

**Esempio:** Sia  $M = (\mathbb{Z}_2, \cdot)$  il monoide definito da:

$\cdot$	0	1
0	0	0
1	0	1

costruiamo un sottomonoide di  $Mat_{4 \times 4}(\mathbb{Z})$  isomorfo a  $M \times M = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ .

$$(0, 0) \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, (0, 1) \mapsto \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, (1, 0) \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, (1, 1) \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$\cdot$	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 0)	(0, 1)
(1, 0)	(0, 0)	(0, 0)	(1, 0)	(1, 0)
(1, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)

Si può verificare direttamente che le matrici hanno la stessa tabella moltiplicativa. (fine esempio)

Abbiamo quindi visto che un monoide finito di cardinalità  $n$  è isomorfo a un monoide di matrici  $n \times n$  le cui colonne hanno un unico "1" e altrove sono "0".

Ognuna di queste matrici può essere vista come una funzione da  $X = \{1, \dots, n\}$  in  $X$  :

$$A_{ij} = 1 \Leftrightarrow f(j) = i$$

$$A_{ij} = 0 \Leftrightarrow f(j) \neq i$$

Il prodotto righe per colonne corrisponde alla composizione di funzioni.

Quindi un monoide finito di cardinalità  $n$  è isomorfo a un sottomonoide del monoide delle funzioni  $f$  da  $\{1, \dots, n\}$  in  $\{1, \dots, n\}$  con l'operazione di composizione.

Notiamo che un elemento  $x \in M$  di un monoide finito  $M$  è invertibile se e solo se la matrice associata è invertibile (una matrice  $A \in Mat_{n \times n}(\mathbb{Z})$  è invertibile se e solo se il suo determinante è invertibile su  $\mathbb{Z}$ , ossia se e solo se  $\det(a) \in \{-1, 1\}$ ).

Da ciò segue che un gruppo finito  $G$  di cardinalità  $|G| = n$ , è isomorfo a un gruppo di matrici le cui componenti sono "0" e "1" e che hanno un unico "1" in ogni riga e ogni colonna (matrici di permutazioni).

Il gruppo  $G$  è inoltre isomorfo a un sottogruppo del gruppo delle funzioni biunivoche da  $\{1, \dots, n\}$  in  $\{1, \dots, n\}$ , che abbiamo chiamato **gruppo simmetrico**  $S_n$ .

Gli elementi di  $S_n$  in notazione a una linea sono indicati nel modo seguente: sia  $\sigma \in S_n$  una funzione biunivoca da  $\{1, \dots, n\}$  in  $\{1, \dots, n\}$ , allora  $\sigma$  è indicata come  $\sigma(1)\sigma(2) \dots \sigma(n)$ .

**Teorema (Teorema di Cayley):** Ogni sottogruppo finito di cardinalità  $n \in \mathbb{N} \setminus \{0\}$  è isomorfo a un sottogruppo di  $S_n$

**Esempio:**

- $S_2 = \{12, 21\}$   
 $S_3 = \{123, 132, 213, 231, 312, 321\}$
- vediamo il gruppo  $(\mathbb{Z}_2, +)$  come gruppo di matrici e come gruppo di permutazioni.  
 $(\mathbb{Z}_2, +) \simeq \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \simeq \{12, 21\} = S_2$  ( $\simeq$  isomorfismodi gruppi)

## 1.5 Relazioni

**Definizione:** Sia  $X$  un insieme. Un sottoinsieme  $R \subseteq X \times X$  è detto **relazione su  $X$** .

**Definizione:** Una relazione  $R \subseteq X \times X$  è detta **relazione di equivalenza** se soddisfa le seguenti proprietà:

- **riflessità:**  $(x, x) \in R, \forall x \in X$
- **simmetria:**  $(x, y) \in R \implies (y, x) \in R, \forall x, y \in X$
- **transitività:**  $(x, y) \in R$  e  $(y, z) \in R \implies (x, z) \in R, \forall x, y, z \in X$

Se  $R$  è una relazione di equivalenza su  $X$  e  $(x, y) \in R$ , scriviamo  $x \sim y$ , che si legge "x è equivalente a y".

**Definizione:** Sia  $X$  un insieme e  $R \subseteq X \times X$  una relazione di equivalenza su  $X$ . L'insieme  $[x]_R := \{y \in X : x \sim y\}$  è detto **classe di equivalenza di  $x$  rispetto a  $R$** .

**Definizione:** L'insieme  $X/\sim := \{[x] : x \in X\}$  è detto **insieme quoziente**.

**Definizione:** La funzione  $\pi : X \rightarrow X/\sim, x \mapsto [x]$  è detta **proiezione canonica**.

**Definizione:** Siano  $x, y \in X$ . Allora se  $x \sim y$  abbiamo che  $[x] = [y]$ . Se  $x \not\sim y$  abbiamo che  $[x] \cap [y] = \emptyset$ . Quindi  $X = \bigsqcup_{[x] \in X/\sim} [x]$ , ossia  $X/\sim$  è una partizione di  $X$ .

### Esempio:

- L'uguaglianza " $=$ " è una relazione di equivalenza su ogni insieme  $X$ .
- Sia  $X = \{1, 2, \dots, n\}$ . Definiamo su  $\mathcal{P}(X)$  la seguente relazione:  $A \sim B \Leftrightarrow |A| = |B|, \forall A, B \subseteq X$ . Questa è una relazione di equivalenza e  $\mathcal{P}(X)/\sim \equiv \{0, 1, \dots, n\}$ . Se  $A \subseteq X$  è tale che  $|A| = k \leq n$  allora  $[A] = \binom{n}{k} := \frac{n!}{k!(n-k)!}$
- Sia  $G$  un gruppo e  $H \subseteq G$  un sottogruppo. La relazione  $\sim$  su  $G$  definita da  $g_1 \sim g_2 \Leftrightarrow g_1 = g_2 h$  per qualche  $h \in H$  è una relazione di equivalenza.

- $g \sim g : g \cdot e, \forall g \in G, e \in H$
- $g_1 \sim g_2 \rightarrow g_2 \sim g_1 : g_1 = g_2 h \rightarrow g_1 h^{-1} = g_2$  ( $h^{-1} \in H$ )
- $g_1 \sim g_2, g_2 \sim g_3 \rightarrow g_1 \sim g_3 : g_1 = g_2 h, g_2 = g_3 h' \rightarrow g_1 = g_3 h h' = g_3 h'', \forall g_1, g_2, g_3 \in G$

In questo caso l'insieme quoziente lo indichiamo con  $G/H$ .

**Definizione:** Il numero  $\binom{n}{k}$  è chiamato **coefficiente binomiale**, questo perché  $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}, \forall x, y \in \mathbb{C}$



### 1.5.1 Insieme quoziente per gruppi abeliani

Se  $G$  è un gruppo abeliano, possiamo definire la seguente operazione "+" su  $G/H$ :  $[g_1] + [g_2] := [g_1 + g_2]$ , vediamo che è ben definita: se  $g'_1 = g_1 + h_1$  e  $g'_2 = g_2 + h_2$ , allora  $[g'_1] = [g_1]$ ,  $[g'_2] = [g_2]$  e  $g'_1 + g'_2 = g_1 + h_1 + g_2 + h_2 = g_1 + g_2 + h$ , dove  $h = h_1 + h_2 \in H$ . Quindi  $[g'_1 + g'_2] = [g_1 + g_2]$ . L'operazione è ovviamente associativa e commutativa, perché lo è quella su  $G$ . Inoltre  $[g] + [0] = [g]$ ,  $\forall [g] \in G/H$  dove con "0" abbiamo indicato l'identità di  $G$ . Quindi la classe  $[0]$  dell'identità di  $(G/H, +)$ . Infine  $[g] + [-g] = [g - g] = [0]$ , dove con  $-g$  abbiamo indicato l'inverso di  $g$  in  $G$ . Quindi  $-[g] = [-g]$ ,  $\forall [g] \in G/H$ , ossia  $(G/H, +)$  è un gruppo abeliano.

#### Esempio:

- Se  $H = \{0\} \subseteq G$ , allora  $G/H$  è isomorfo a  $G$ . ( $\{0\}$  gruppo banale e  $G$  gruppo abeliano)
- Sia  $G = (\mathbb{Z}, +)$  e  $n \in \mathbb{N}$ . Il sottoinsieme  $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$  è un sottogruppo di  $\mathbb{Z}$ .

- $0\mathbb{Z} = \{0\}$
- $1\mathbb{Z} = \{\mathbb{Z}\}$
- $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$
- $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$

Definiamo il gruppo abeliano  $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ , per  $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} = \mathbb{Z}$ .

Sia  $n \geq 0$  e siano  $x, y \in \mathbb{Z}$ .

- Allora  $x \sim y \Leftrightarrow x = y + h \ (h \in n\mathbb{Z}) \Leftrightarrow x - y = kn \text{ (per } k \in \mathbb{Z}) \Leftrightarrow$   
il resto della divisione di  $x$  per  $n$  è uguale al resto della divisione di  $y$  per  $n$ .

I possibili resti della divisione per  $n$  sono  $0, 1, \dots, n-1$ .

Quindi  $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ . ( $\{[0], [1], \dots, [n-1]\}$  sono le classi di resto)

- $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ ,  $\overline{1} + \overline{1} = [1 + 1] = [2] = [0]$

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

- $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ ,

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

**Definizione:** Sia  $G$  un gruppo abeliano e  $H \subseteq G$  un sottogruppo. La proiezione canonica  $\pi : G \rightarrow G/H$  è un **morfismo suriettivo di gruppi**

Se  $G$  è un gruppo finito e  $H \subseteq G$  è un sottogruppo, allora  $[g] \in G/H \rightarrow |[g]| = |H|$ .  
 Infatti  $[g] = \{gh : h \in H\}$  e  $gh_1 = gh_2 \rightarrow h_1 = h_2$ .  
 Poiché le classi di equivalenza sono una partizione di  $G$ , abbiamo  $|G| = |G/H| \cdot |H|$ .  
 In particolare la cardinalità o (**ordine**) di un sottogruppo di un gruppo finito divide la cardinalità del gruppo.

**Teorema:** Sia  $f : G_1 \rightarrow G_2$  un morfismo di gruppi. Allora  $f$  è iniettivo se e solo se  $\text{Ker}(f) = \{e_1\}$ .  
 (Questo non vale per i morfismi di monoidi.)

**Dimostrazione:** Sia  $f$  iniettivo. Sia  $x \in \text{Ker}(f)$ . Allora  $f(x) = e_2$  e quindi, poiché anche  $f(e_1) = e_2$ , si ha che  $x = e_1$  per l'ipotesi di iniettività.  
 Sia  $\text{Ker}(f) = \{e_1\}$ . Siano  $x, y \in G_1$  tali che  $f(x) = f(y)$ .  
 Allora  $f(x)f(y^{-1}) = e_2 \rightarrow f(xy^{-1}) = e_2 \rightarrow xy^{-1} \in \text{Ker}(f) \rightarrow xy^{-1} = e_1 \rightarrow x = y$ .

**Esempio:**

- $G = \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ ,
  - $\langle \bar{0} \rangle = \bar{0}$  sottogruppo banale  $\simeq \mathbb{Z}_1$
  - $\langle \bar{1} \rangle = \mathbb{Z}_4$
  - $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\} \simeq \mathbb{Z}_2$  ( $2 + 2 = 0$ )
  - $\langle \bar{3} \rangle = \mathbb{Z}_4$  ( $3, 3 + 3 = 6 = 2, 3 + 2 = 5 = 1, 3 + 1 = 4 = 0$ )

I sottogruppi di  $\mathbb{Z}_4$  possono aver cardinalità 1, 2, 4. L'insieme dei sottogruppi di  $\mathbb{Z}_4$  è  $\{\{\bar{0}\}, \{\bar{0}, \bar{2}\}, \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4\}$

- $G = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ ,
  - $\langle \bar{0} \rangle = \bar{0}$  sottogruppo banale  $\simeq \mathbb{Z}_1$
  - $\langle \bar{1} \rangle = \mathbb{Z}_6$
  - $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} \simeq \mathbb{Z}_3$
  - $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\} \simeq \mathbb{Z}_2$
  - $\langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} \simeq \mathbb{Z}_3$
  - $\langle \bar{5} \rangle = \mathbb{Z}_6$

I sottogruppi di  $\mathbb{Z}_6$  possono aver cardinalità 1, 2, 3, 6. L'insieme dei sottogruppi di  $\mathbb{Z}_6$  è  $\{\{\bar{0}\}, \{\bar{0}, \bar{2}, \bar{4}\}, \{\bar{0}, \bar{3}\}, \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \mathbb{Z}_6\}$

**Caso generale:** consideriamo il gruppo  $\mathbb{Z}_n = (\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}, +)$  sia  $m \in \mathbb{N}, m < n$ .

Se  $m = 0$ ,  $\langle \bar{0} \rangle = \{\bar{0}\}$ .

Sia  $m > 0$  e  $z := \frac{\text{mcm}\{m, n\}}{m}$ . (mcm = minimo comune multiplo)

$$\bar{m} + \bar{m} + \dots = \bar{m} = \bar{z}\bar{m} = \overline{\text{mcm}\{m, n\}} = \bar{0}$$

Se  $i \leq i \leq z$ :  $im < zm = \text{mcm}\{m, n\} \rightarrow n$  non divide  $im$ .

$\bar{m} + \bar{m} + \dots = \bar{m} = \bar{im} \neq \bar{0}$  perché  $im$  è multiplo di  $m$  e  $im < \text{mcm}\{m, n\}$ , quindi  $im$  non è multiplo di  $n$ . Dunque  $|\langle \bar{m} \rangle| = z = \frac{\text{mcm}\{m, n\}}{m}$ .

In particolare,  $\langle \bar{m} \rangle = \mathbb{Z}_n \Leftrightarrow z = n \Leftrightarrow \text{MCD}\{m, n\} = 1$ . Ossia l'insieme  $\{\bar{m}\}$  genera il gruppo  $\mathbb{Z}_n$  sse  $m$  e  $n$  sono coprimi.

**Definizione:** La funzione definita da  $\varphi : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ ,  
 $\varphi(n) := |\{m \in \mathbb{N} \setminus \{0\} : m < n \text{ e } \text{MCD}\{m, n\} = 1\}|$  è detta **funzione di Eulero**.  
 Quindi ci sono  $\varphi(n)$  elementi  $\overline{m}$  tali che  $\langle \overline{m} \rangle = \mathbb{Z}_n$ .

**Proposizione:** L'insieme dei sottogruppi di  $(\mathbb{Z}, +)$  è  $\{n\mathbb{Z} : n \in \mathbb{N}\}$ .

**Dimostrazione:** Sia  $H \subseteq \mathbb{Z}$  un sottogruppo non banale.  
 Sia  $k := \min(H_{>0})$  dove  $H_{>0} := \{h \in H : h > 0\}$ .  
 Sia  $h \in H_{>0}, h \neq k$ .  
 Allora  $h > k$  e  $h = nk + r, n \in \mathbb{N}, 0 \leq r < k$ .  
 Dunque  $r = h - nk \in H \rightarrow r = 0$  per la minimalità di  $k$ .

**Definizione:** Un gruppo  $G$  è detto **ciclico** se esiste  $g \in G$  tale che  $\langle g \rangle = G$ .  
 Un gruppo ciclico è anche abeliano

**Esempio:**

- $\mathbb{Z} = \langle 1 \rangle$  è ciclico
- $\mathbb{Z}_n = \langle \overline{1} \rangle$  è ciclico
- $\mathbb{Z} \times \mathbb{Z} = \langle (1, 0), (0, 1) \rangle$  non è ciclico, infatti in  $\mathbb{Z} \times \mathbb{Z}$ , se  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ ,  $\langle (a, b) \rangle = \{(ka, kb) : k \in \mathbb{Z}\} = \{(x, y) : a \text{ divide } x, b \text{ divide } y\} \subsetneq \mathbb{Z} \times \mathbb{Z}$ .
- $\mathbb{Z}_2 \times \mathbb{Z}_2$  non è ciclico. Infatti, in  $\mathbb{Z}_2 \times \mathbb{Z}_2$  si ha:
  - $\langle (\overline{0}, \overline{0}) \rangle = \{(\overline{0}, \overline{0})\}$
  - $\langle (\overline{0}, \overline{1}) \rangle = \{\overline{0}\} \times \mathbb{Z}_2$
  - $\langle (\overline{1}, \overline{0}) \rangle = \mathbb{Z}_2 \times \{\overline{0}\}$
  - $\langle (\overline{1}, \overline{1}) \rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\}$

Quindi nessun elemento di  $\mathbb{Z}_2 \times \mathbb{Z}_2$  genera  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

**Teorema (di isomorfismo per gruppi abeliani):** Sia  $f : G_1 \rightarrow G_2$  un morfismo di gruppi abeliani. Allora esiste un morfismo iniettivo  $\varphi : G_1 / \text{Ker} f \rightarrow G_2$  tale che il seguente diagramma è commutativo:

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \pi \downarrow & \nearrow \varphi & \\ G_1 / \text{Ker}(f) & & \end{array}$$

In particolare,  $G_1 / \text{Ker}(f) \simeq \Im(f)$ .

**Dimostrazione:** L'assegnazione  $[g] \mapsto f(g), \forall g \in G$ , definisce una funzione  $\varphi : G_1 / \text{Ker}(f) \rightarrow G_2$ .

Infatti, se  $g' \sim g$ , ossia  $[g] = [g']$ , allora  $g = g' + h, h \in \text{Ker}(f)$ .

Dunque  $f(g) = f(g' + h) = f(g') + f(h) = f(g')$ . Poiché  $f$  è morfismo di gruppi, anche  $\varphi$  lo è.

Inoltre  $\text{Ker}(f) = \{[g] \in G / \text{Ker}(f) : \varphi([g]) = O_2\} = \{[g] \in G / \text{Ker}(f) : f(g) = O_2\} = [O_1]$ .  
 Quindi  $\varphi$  è iniettiva.

Infine,  $\varphi : G_1 / \text{Ker}(f) \rightarrow \text{Im}(f)$  è un morfismo di gruppi, iniettivo e suriettivo, quindi un isomorfismo.

**Teorema:** Sia  $G$  un gruppo ciclico. Allora ogni sottogruppo di  $G$  è ciclico.

**Dimostrazione:** Sia  $g \in G$  tale che  $g = \langle g \rangle$ . La funzione  $\varphi : (\mathbb{Z}, +) \rightarrow G$  definita da  $\varphi(g) = g^n, \forall n \in \mathbb{Z}$ , è un morfismo suriettivo di gruppi.

- $G$  è infinito: allora  $\text{Ker}(f) = \{0\}$  e quindi  $\varphi$  è iniettivo. Dunque  $\varphi$  è un isomorfismo di gruppi. Tutti i sottogruppi di  $\mathbb{Z}$  sono ciclici.
- $G$  è finito: sia  $H \subseteq G$  un sottogruppo. Allora  $\varphi^{-1}(H) := \{n \in \mathbb{Z} : \varphi(n) \in H\} \subseteq \mathbb{Z}$  è un sottogruppo di  $\mathbb{Z}$ , quindi esiste  $\varphi^{-1}(H) = \langle k \rangle$  con  $k \in \mathbb{N}$ .  
La restrizione  $\varphi : k\mathbb{Z} \rightarrow H$  è un morfismo suriettivo di gruppi e  $\varphi(hk) = \varphi(\underbrace{k + k + \dots + k}_{h \text{ volte}}) = \varphi(k)\varphi(k) \dots \varphi(k) = [\varphi(k)]^h, \forall h \in \mathbb{Z}$ . Quindi  $H = \langle \varphi(k) \rangle$ .

**Corollario:** L'insieme dei sottogruppi di  $\mathbb{Z}_n, n \in \mathbb{N}$  è  $\{\langle \overline{m} \rangle : \overline{m} \in \mathbb{Z}_n\}$ .

**Proposizione:** Sia  $n \in \mathbb{N}$  e sia  $d|n$  ( $d$  divide  $n$ ). Allora esiste al più un unico sottogruppo di  $\mathbb{Z}_n$  di cardinalità  $d$ .

**Dimostrazione:** Sia  $H \subseteq \mathbb{Z}_n$  sottogruppo tale che  $|H| = d$ . Si considerino le proiezioni canoniche  $\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}_n \xrightarrow{\pi_2} \mathbb{Z}_n/H$ .

Poiché  $\pi_1^{-1}(H) = \{m \in \mathbb{Z} : \pi_1(m) \in H\}$  è un sottogruppo di  $\mathbb{Z}$ , allora esiste  $k \in \mathbb{N}$  tale che  $\pi_1^{-1}(H) = k\mathbb{Z}$ . Inoltre  $\text{Ker}(\pi_1 \cdot \pi_2) = \pi_1^{-1}(H)$  e quindi, essendo  $\pi_1 \cdot \pi_2$  un morfismo suriettivo di gruppi,  $\mathbb{Z}_n/H \simeq \mathbb{Z}/\pi_1^{-1}(H) = \mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$ .

Quindi  $|\mathbb{Z}_k| = k = |\mathbb{Z}_n/H| = |\mathbb{Z}_n|/|H| = \frac{n}{d}$ , ossia  $k$  è univocamente determinato, e allora  $H = \pi_1(k\mathbb{Z})$  è univocamente determinato.

**Esempio:** I sottogruppi di  $\mathbb{Z}_{899}$  sono quattro, perché  $899 = 31 \cdot 29$ , quindi c'è un sottogruppo di cardinalità 1 (il sottogruppo banale), uno di cardinalità 31, uno di cardinalità 29 e  $\mathbb{Z}_{899}$ .

Sono:  $\{\{0\}, \langle \overline{29} \rangle, \langle \overline{31} \rangle, \mathbb{Z}_{899}\}$ .