APPUNTI DELLE LEZIONI DI MATEMATICA DISCRETA

DONATELLA IACONO

Queste note sono state scritte come ulteriore supporto a favore della preparazione dello studente.

Sono note integrative alle lezione, contengono solo alcuni argomenti del corso, e questi sono esposti sinteticamente. **NON** intendono sostituirsi ai libri di testo consigliati, ma al più affiancarsi a questi.

Pertanto, **NON** possono essere usati come unico riferimento nella preparazione dell'esame[1].

Nonostante l'impegno, errori, sviste e imprecisioni sono sparsi ovunque all'interno delle note (pertanto lo studente deve stare attento!!), la loro segnalazione è molto apprezzata.

Inoltre, **NON** sono autorizzate diffusioni e ripubblicazione di tale materiale (esempio: diffusione e ripubblicazione del pdf degli appunti o di una parte).

LIBRI CONSIGLIATI

G.M. PIACENTINI CATTANEO: **MATEMATICA DISCRETA**, ed. ZANICHELLI

M.G. BIANCHI, A. GILLIO: **INTRODUZIONE ALLA MATEMATICA DISCRETA**, ed. McGRAW-HILL

K. H. ROSEN, **Discrete Mathematics and Its Applications**, McGraw-Hill Editore, (in Inglese).

A. FACCHINI: **ALGEBRA E MATEMATICA DISCRETA**, ed. ZANICHELLI

No exploitation, distribution, sale, transfer, publication, public indexing, training of artificial intelligence systems or external transfer is authorised. ALL RIGHTS RESERVED.

Date: November 13, 2026.

[1]Esempio: Risolvo un esercizio (sia teorico che computazionale) esattamente come è svolto nlle note. Prendo sicuramente il massimo punteggio? No, perché in queste note potrebbe essere stato svolto con qualche errore o in maniera sintetica non esauriente.

Contents

1. Insiemi 4
1.1. Inclusione, Uguaglianza, Unione e Intersezione di Insiemi 5
1.2. Complementare, Differenza, Insieme delle parti, Prodotto cartesiano 8
2. Logica 10
2.1. Negazione, Congiunzione, Disgiunzione, Implicazione 10
2.2. Tecniche di dimostrazione 14
3. Funzioni 16
3.1. Funzioni Iniettive 19
3.2. Funzioni Suriettive 20
3.3. Funzioni Biettive 21
3.4. Composizione di Funzioni 22
3.5. Inversa di Funzioni 24
4. Contare gli elementi di un insieme 26
5. Principio di Induzione 28
5.1. Principio di Induzione (prima forma) 28
5.2. Principio di Induzione (seconda forma) 28
5.3. Principio di Induzione Generalizzato (prima forma) 30
5.4. Principio di Induzione Generalizzato (seconda forma) 30
6. Successioni 32
6.1. I numeri di Fibonacci 35
6.2. Le Torri di Hanoi 36
6.3. Simbolo di Sommatoria 37
7. Combinatoria 39
7.1. Regola della Somma 39
7.2. Principio di inclusione-esclusione 39
7.3. Regola del Prodotto 41
8. Combinazioni e disposizioni 42
8.1. Caso 1) scegliere k elementi distinti 42
8.2. Formula di Newton 44
8.3. Caso 2) Scegliere k elementi con ripetizione in un insieme con n elementi 45
9. Relazioni 49
9.1. Relazioni d'ordine 49
9.2. Relazioni di equivalenza 51
9.3. Classi di equivalenza e Insieme quoziente 52
10. I Numeri Interi 56
10.1. Divisione 56
10.2. Massimo Comun Divisore 58
10.3. Algoritmo di Euclide 59
10.4. Minimo Comune Multiplo 61
11. Equazioni diofantee 62
11.1. I numeri primi 65
11.2. Crivello di Eratostene 67
11.3. Metodi di Fattorizzazione 67
12. Congruenze modulo n 68
12.1. Criteri di Divisibilità 71
12.2. Congruenze lineari 72
12.3. Sistemi di congruenze lineari 74
13. Strutture Algebriche 77
13.1. Esempio: Monoide delle parole 78
14. Gruppi 82
14.1. Operazioni compatibili con relazioni di equivalenza 82

14.2. Sottogruppi e Gruppi Ciclici (Versione ridotta valida per A.A. 2023-2024, 2024-2025, 2025-2026) 85
14.3. Sottogruppi e gruppi ciclici (versione standard non ridotta con dettagli ed esempi per anni accademici precedenti) 86
15. Gruppo Simmetrico 91
16. Anelli e Campi (valido fino al 2024/2025) 97
17. Anelli e Campi (valido dal 2025/2026) 100
18. Campo dei numeri complessi (A.A 2025/2026) 102
19. Matrici 106
20. Grafi 114
Index 122

1. Insiemi

L'Italia è una Repubblica democratica, fondata sul lavoro.
La sovranità appartiene al popolo, che la esercita nelle forme
e nei limiti della Costituzione.

In questa sezione ci concentriamo sul concetto di insieme[2], impareremo a descrivere gli insieme. Introdurremo molti esempi, descriveremo alcune proprietà e costruiremo insiemi a partire da altri insiemi.

Quello di insieme è un concetto primitivo: questo vuol dire che non si può dare la definizione di insieme ricorrendo ad altre definizioni. La stessa cosa vale, per esempio, in geometria per il concetto di punto. Si può pensare ad un insieme come ad una *famiglia di oggetti*, che vengono chiamati elementi dell'insieme. Quindi, un insieme A è una *collezione di oggetti*, detti *elementi dell'insieme*, e per poter dire di aver assegnato l'insieme A, bisogna aver stabilito dei criteri secondo i quali si possa essere in grado di stabilire se un elemento appartenga o meno ad A.

Esempio 1. Per esempio hanno senso matematicamente:

- A=l'insieme delle lettere che costituiscono la parola: casa.
- B=l'insieme dei cittadini italiani nati nel 2010.
- $\mathbb{N}$ = insieme dei numeri naturali.
- $\mathbb{Z}$ = insiemi dei numeri interi.
- $\mathbb{Q}$ = insieme dei numeri razionali.
- $\mathbb{R}$ = insiemi dei numeri reali.
- C=l'insieme dei numeri interi positivi.
- D=l'insieme dei numeri interi pari e dispari.

NOTAZIONE/CONVENZIONE. In generale, gli insiemi si indicano con la lettere Maiuscola. Gli elementi dell'insieme si denotano con la lettera minuscola.

Se un elemento appartiene ad un insieme, si usa il simbolo di appartenenza

$$\in$$

ad esempio $a \in A$, si legge: a "appartiene"ad A oppure a "è elemento di"A. Se un elemento a non appartiene ad un insieme A, allora scriveremo

$$a \notin A.$$

Esempio 2. Nell'Esempio 1. Possiamo scrivere

$$5 \in C, 10 \in C, -2 \notin C, \frac{2}{3} \notin C.$$

Definizione 1. (INSIEME VUOTO) L'*insieme vuoto*, si indica con $\emptyset$, ed è l'unico insieme che non contiene elementi.

Esempio 3. Non ci sono numeri interi che siano contemporaneamente pari e dispari, per cui l'insieme D, sebbene sia ben definito, è privo di elementi: D non è altro che l'*insieme vuoto*, $D = \emptyset$.

Si osservi che frasi del tipo:"la strada è l'insieme dell'asfalto che contiene"oppure "un litro è l'insieme di 10 decilitri", non definiscono insiemi.

Possiamo descrivere un insieme in diversi modi:

[2]Se vogliamo essere matematicamente corretti, fissiamo un universo che contiene tutti gli insiemi che tratteremo.

1) Elencare i suoi elementi

Esempio 4. Alcuni esempi

- $\mathbb{N}$ = insieme dei numeri naturali=$\{0, 1, 2, 3, \ldots\}$
- $\mathbb{Z}$ = insiemi dei numeri interi=$\{0, 1, -1, 2, -2, 3, -3, \ldots\}$
- $X = \{a, b, 3, *, -1, 0\}$
- $Y = \{a, b, c, \ldots, u, v, z\}$= lettere alfabeto italiano.

$0 \in \mathbb{N}$ e $0 \in \mathbb{Z}$. $c \in Y$ e $c \notin X$.

Nota Bene 1. Per indicare un insieme si usano le parentesi graffe: $A = \{\ldots\}$.

Nota Bene 2. Non importa l'ordine in cui elenchiamo gli elementi ed ogni elemento viene scritto una sola volta. Ad esempio $X = \{a, b, 3, *, -1, 0\} = \{3, *, b, -1, a, 0\}$.

Questa descrizione è comoda soprattutto per gli insiemi finiti.

2) Specificare una proprietà caratteristica, ovvero una proprietà verificata da tutti e soli gli elementi di A.

In generale, per assegnare un insieme tramite una proprietà caratteristica si scriverà:

$$A = \{x \mid x \text{ soddisfa } P\} \text{ oppure } A = \{x : x \text{ soddisfa } P\}.$$

I due punti : o | si leggono "tale che ", ovvero A è l'insieme di tutti gli x che soddisfano la proprietà P.

Esempio 5. $\mathbb{Q}$ = insiemi dei numeri razionali=$\{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ e } q \neq 0\}$

Esempio 6. Sia A insieme dei numeri interi compresi tra -3 e 7, estremi esclusi, allora

$$A = \{a \in \mathbb{Z} \mid -3 < a < 7\} = \{-2, \ldots, 6\}.$$

Notiamo anche che

$$\{a \in \mathbb{Z} \mid -3 < a < 7\} = \{x \in \mathbb{Z} \mid -3 < x < 7\} = \{x \in \mathbb{Z} \mid -2 \leq x \leq 6\}.$$

3) Diagrammi di Venn[3].

Esempio 7. Aggiungere Disegno

1.1. Inclusione, Uguaglianza, Unione e Intersezione di Insiemi.

Definizione 2. (INCLUSIONE) Siano A e B insiemi. Si dice che A è *incluso* in B, oppure A è *contenuto* in B o anche che A è *sottoinsieme* di B e si scrive

$$A \subseteq B$$

se ogni elemento di A è anche elemento di B.

Se A non è sottoinsieme di B, scriveremo $A \not\subseteq B$.

Osservazione 1. Non confondere il simbolo di appartenenza "$\in$" di un elemento ad un insieme con il simbolo di inclusione "$\subseteq$" di un insieme in un altro. Sono corrette le scritture:

$$3 \in \mathbb{N}; \quad \{-5\} \subseteq \mathbb{Z}; \quad \{4, 0, 2\} \subseteq \mathbb{Q}.$$

Sono invece errate:

$$1 \subseteq \mathbb{N}, \quad \{-5\} \in \mathbb{Z}.$$

Esempio 8. Si ha che $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Esempio 9. Siano

$$A = \{n \in \mathbb{Z} \mid -1 < n \leq 5\} \qquad B = \{n \in \mathbb{N} \mid n < 5\} \qquad C = \{p \in \mathbb{R} \mid -1 < p < 5\}$$

dove $\mathbb{R}$ denota l'insieme dei numeri reali.

Allora $A \not\subseteq B$ e $B \subseteq A$, $A \not\subseteq C$, $C \not\subseteq A$, $B \subseteq C$, $C \not\subseteq B$

[3] John Venn, matematico inglese che ha introdotto l'uso dei diagrammi nel 1881.

Esercizio 1. Convincersi delle inclusioni degli Esempi 9 e 8.

Osservazione 2. Si osservi che per ogni insieme A l'insieme vuoto ed A stesso risultano essere sottoinsiemi di A:

$$\emptyset \subseteq A \qquad A \subseteq A.$$

Osservazione 3. Si osservi che se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$.

Definizione 3. (INCLUSIONE PROPRIA) Se A è sottinsieme di B ed esiste un elemento di B che non appartiene ad A, diremo che l'*inclusione è propria* e scriveremo

$$A \subset B \ \text{ o } \ A \subsetneq B.$$

Si dice anche che A *è incluso strettamente* in B oppure *è contenuto propriamente o strettamente* in B o anche che A *è sottoinsieme proprio* di B.

Esempio 10. Si ha che $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. Nell'Esempio 9, $B \subsetneq A$ e $B \subsetneq C$.

Definizione 4. (UGUAGLIANZA) Siano A e B insiemi. Si dice che A e B sono *uguali*, e si scrive $A = B$, se $A \subseteq B$ e $B \subseteq A$. In tal caso, gli insiemi A e B hanno gli stessi elementi.

Esempio 11. Ad esempio, gli insiemi

$$A = \{n \in \mathbb{Z} \mid n \leq 0\} \qquad \text{e} \qquad B = \{-n \mid n \in \mathbb{N}\}$$

sono uguali, oppure sono uguali

$$C = \{a, b, 3, -1, *, 0\} \qquad \text{e} \qquad D = \{3, *, 0, b, a, -1\}.$$

Esempio 12. Siano

$A =$ insieme dei residenti a Bari nati nel 2000,

e

$B =$ insieme dei residenti a Bari nati nel 2000 che praticano attività sportiva.

Sicuramente sarà $B \subseteq A$, ma non si può scrivere $B \subset A$ se non si è sicuri che almeno un ragazzo tra i residenti a Bari nati nel 2000 non pratichi attività sportiva.

Introduciamo due simboli di fondamentale importanza in Matematica il quantificatore Universale ed Esistenziale:

$$\textit{quantificatore universale} \ : \qquad \forall$$
$$\textit{quantificatore esistenziale} \ : \qquad \exists$$

il simbolo $\forall$ si legge per ogni, il simbolo $\exists$ si legge esiste.

Si usa anche il simbolo

$$\exists!$$

che si legge esiste ed è unico.

Inoltre, introduciamo il simbolo di "se e solo se "

$$\text{se e solo se } :\Longleftrightarrow$$

Esempio 13. Ad esempio

$$\forall A \text{ insieme} \quad \text{si ha che } \emptyset \subseteq A \text{ e } A \subseteq A.$$

Esempio 14. Ad esempio

$$A \subseteq B \Longleftrightarrow \forall a \in A \text{ si ha che } a \in B,$$

$$A \subsetneq B \Longleftrightarrow A \subseteq B \text{ e } A \neq B,$$

oppure

$$A \subsetneq B \Longleftrightarrow \forall a \in A \text{ si ha che } a \in B \text{ ed } \exists\, b \in B \text{ tale che } b \notin A.$$

Esempio 15. (Esempio su come vengono usati i quantificatori) Consideriamo $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. La somma $+$ su $\mathbb{N}$ soddisfa le seguenti proprietà:

(1) $\forall a, b \in \mathbb{N}$ si ha che $a + b \in \mathbb{N}$;

(2) (proprietà commutativa di $+$) $\forall a, b \in \mathbb{N}, \quad a + b = b + a$;

(3) (proprietà associativa di $+$) $\forall a, b, c \in \mathbb{N}, \quad (a + b) + c = a + (b + c)$;

(4) (esistenza elemento neutro di $+$[4]) $\exists 0 \in \mathbb{N}$ tale che $\forall a \in \mathbb{N}$ si ha $a+0 = 0+a = a$;

Queste proprietà valgono anche per la somma in $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$.
La moltiplicazione $\cdot$ su $\mathbb{N}$ soddisfa le seguenti proprietà:

(1) $\forall a, b \in \mathbb{N}$ si ha che $a \cdot b \in \mathbb{N}$;

(2) (proprietà commutativa di $\cdot$) $\forall a, b \in \mathbb{N}, \quad a \cdot b = b \cdot a$;

(3) (proprietà associativa di $\cdot$) $\forall a, b, c \in \mathbb{N}, \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(4) (esistenza elemento neutro di $\cdot$[5]) $\exists 1 \in \mathbb{N}$ tale che $\forall a \in \mathbb{N}$ si ha $a \cdot 1 = 1 \cdot a = a$.

Definizione 5. (INTERSEZIONE) Siano A e B insiemi. Si definisce *intersezione* di A e B e si indica con $A \cap B$, l'insieme costituito dagli elementi che appartengono sia ad A che a B, ovvero l'insieme

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

Esempio 16. Siano $A = \{a, b, 1, 2, 3, +, *, \circ\}$, $B = \{1, -1, 2, -2, *, \sqrt{5}\}$. Allora

$$A \cap B = \{1, 2, *\}.$$

Esempio 17.

$$A = \{-1, -2, -3, 1, 2\} \qquad B = \{0, 5, -3, 2\}$$
$$C = \{-1, 2, 1\} \qquad D = \{p \in \mathbb{Z} : -1 < p \leq 5\}.$$

Allora

$$A \cap B = \{-3, 2\}, \qquad A \cap D = \{1, 2\}.$$

Esercizio 2. Calcolare $A \cap C, B \cap C, B \cap D, D \cap C$ dell'Esempioo 17.

Definizione 6. (INSIEMI DISGIUNTI) Due insiemi A e B sono *disgiunti* se la loro intersezione è vuota, ovvero $A \cap B = \emptyset$.

Esempio 18. Sono disgiunti, per esempio, gli insiemi $\mathbf{P} = \{n \in \mathbb{Z} \mid n \text{ è pari}\}$ e $\mathbf{D} = \{n \in \mathbb{Z} \mid n \text{ è dispari}\}$. Notiamo, che si può anche scrivere

$$P = \{n \in \mathbb{Z} \mid \exists t \in \mathbb{Z} \text{ tale che } n = 2t\} = \{n \in \mathbb{Z} \mid n = 2t \text{ con } t \in \mathbb{Z}\} = \{2t \mid t \in \mathbb{Z}\}$$

e

$$D = \{n \in \mathbb{Z} \mid \exists t \in \mathbb{Z} \text{ tale che } n = 2t+1\} = \{n \in \mathbb{Z} \mid n = 2t+1 \text{ con } t \in \mathbb{Z}\} = \{2t+1 \mid t \in \mathbb{Z}\}.$$

Definizione 7. (UNIONE) Siano A e B insiemi. Si definisce *unione* di A e B e si indica con $A \cup B$, l'insieme costituito dagli elementi che appartengono ad A oppure a B, ovvero l'insieme

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

[4]Dimostreremo che esiste ed è unico

[5]Dimostreremo che esiste ed è unico

Esempio 19. Siano $A = \{a, b, 1, 2, 3, +, *, \circ\}$, $B = \{1, -1, 2, -2, *, \sqrt{5}\}$. Allora

$$A \cup B = \{a, b, 1, -1, 2, -2, 3, +, *, \circ, \sqrt{5}\}.$$

Esercizio 3. Calcolare le unioni a due a due degli insiemi dell'Esempio 17.

Osservazione 4. Descrivere l'intersezione e l'unione con i diagrammi di Venn.

Proposizione 1. *Siano A, B, C insiemi. Si ha allora:*

(1) $A \cup \emptyset = A$;
(2) $A \cap \emptyset = \emptyset$;
(3) $A \cup A = A$ *e* $A \cap A = A$;
(4) $A \subseteq B \iff A \cup B = B \iff A \cap B = A$;
(5) $A \subseteq A \cup B$ *e* $B \subseteq A \cup B$;
(6) $A \cap B \subseteq A$ *e* $A \cap B \subseteq B$;
(7) $(A \cup B) \cup C = A \cup (B \cup C)$ *(proprietà associativa dell'unione);*
(8) $(A \cap B) \cap C = A \cap (B \cap C)$ *(proprietà associativa dell'intersezione);*
(9) $A \cup B = B \cup A$ *(proprietà commutativa dell'unione);*
(10) $A \cap B = B \cap A$ *(proprietà commutativa dell'intersezione);*
(11) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, *(proprietà distributive dell'intersezione rispetto all'unione);*
(12) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(proprietà distributive dell'unione rispetto all'intersezione).*

Dimostrazione. La dimostrazione di queste proprietà è lasciata come esercizio al lettore volenteroso.

Osservazione 5. Si osservi che le Proprietà (1) e (2) della proposizione precedente sono un caso particolare della Proprietà (4), ma si è preferito, in ogni modo, evidenziarle. Anche nelle Proprietà (11) (e (12)) la seconda segue dalla prima per la Proprietà commutativa.

1.2. **Complementare, Differenza, Insieme delle parti, Prodotto cartesiano.**

Definizione 8. (COMPLEMENTARE) Siano A insieme e $B \subseteq A$. Si definisce il *complementare di B rispetto ad A* l'insieme di tutti gli elementi di A che non appartengono a B, ovvero l'insieme:

$$\complement_A(B) = \{x \in A \mid x \notin B\}.$$

Esempio 20. Sia

$$A = \{n \in \mathbb{Z} \mid n \geq -4\} \qquad B = \mathbb{N}$$

Allora $B = \mathbb{N} \subseteq A$ e $\complement_A(B) = \{-4, -3, -2, -1\}$.

Proposizione 2. *Siano A un insieme e B e C sottoinsiemi di A. Risulta allora:*

(1) $\complement_A(A) = \emptyset$
(2) $\complement_A(\emptyset) = A$
(3) $B \cup \complement_A(B) = A$
(4) $B \cap \complement_A(B) = \emptyset$
(5) $\complement_A(B \cup C) = \complement_A(B) \cap \complement_A(C)$
(6) $\complement_A(B \cap C) = \complement_A(B) \cup \complement_A(C)$.

Le proprietà (5) e (6) vanno sotto il nome di Leggi di De Morgan[6].

Dimostrazione. La dimostrazione è lasciata come utile esercizio per il lettore.

Esercizio 4. Dimostrare le leggi di De Morgan.

[6]Augustus De Morgan, 1806-1871, matematico britannico, nato in India

Definizione 9. (INSIEME DIFFERENZA) Siano A, B insiemi. L'*insieme differenza* tra l'insieme A e l'insieme B è l'insieme costituito da tutti gli elementi di A, tranne gli elementi di B, ovvero

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

L'insieme differenza tra A e B può anche essere denotato con $A - B$.

Osservazione 6. Questa definizione generalizza la definizione di insieme complementare che si può dare solo nel caso di sottoinsiemi.

Osservazione 7. Si prova che $A \setminus B = \complement_A(A \cap B)$. Inoltre, se $B \subseteq A$, allora $\complement_A(B) = A \setminus B$.

Esempio 21. Ad esempio $\mathbb{N} \setminus \{3\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{Q} \setminus \{\frac{1}{2}\}$, $\mathbb{R} \setminus \{\sqrt{4}\}$.

Osservazione 8. Useremo spesso le notazioni: $\mathbb{N}^* = \mathbb{N}\setminus\{0\}$, $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$, $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Esempio 22. In riferimento all'Esempio 19: $A = \{a, b, 1, 2, 3, +, *, \circ\}$, $B = \{1, -1, 2, -2, *, \sqrt{5}\}$, risulta:

$$A \smallsetminus B = \{a, b, 3, +, \circ\}, \quad B \smallsetminus A = \{-1, -2, \sqrt{5}\},$$
$$\complement_{(A\cup B)}(A \cap B) = \{a, b, -1, -2, 3, +, \circ, \sqrt{5}\}.$$

Osservazione 9. Descrivere il complementare e la differenza con i diagrammi di Venn.

Definizione 10. (INSIEME delle PARTI) Sia A un insieme. L'*insieme delle parti di* A si indica con $\mathscr{P}(A)$ ed è l'insieme formato da tutti i sottoinsiemi di A. In simboli:

$$\mathscr{P}(A) = \{X \mid X \subseteq A\} = \{\emptyset, A, \ldots\}$$

Osservazione 10. Notiamo che se $a \in A$ allora $\{a\} \subseteq A$ e $\{a\} \in \mathscr{P}(A)$.

Osservazione 11. Sia A un insieme. Allora: $A \in \mathscr{P}(A)$ e $\emptyset \in \mathscr{P}(A)$.

Esempio 23. Ad esempio abbiamo

1. Se $A = \emptyset$, allora $\mathscr{P}(\emptyset) = \{\emptyset\}$.
2. Se $A = \{1\}$, allora $\mathscr{P}(A) = \{\emptyset, \{1\}\} = \{\emptyset, A\}$.
3. Se $A = \{a, b\}$, allora $\mathscr{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
4. Se $A = \{1, 2, *\}$, allora $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{*\}, \{1, 2\}, \{1, *\}, \{2, *\}, A\}$.

Esercizio 5. Determinare $\mathscr{P}(A)$ nei seguenti casi:

$$A = \{3, 6, 9\} \qquad e \qquad A = \{x, y, z, w\}.$$

Definizione 11. (PRODOTTO CARTESIANO) Siano A e B due insiemi. Il *prodotto cartesiano* di A e B, si indica con $A \times B$ ed è l'insieme di tutte le coppie ordinate (a, b) con $a \in A$ e $b \in B$, ovvero in simboli

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

Esempio 24. Siano

$$A = \{3, 6, 9\} \qquad e \qquad B = \{x, y, *\}$$

Allora

$$A \times B = \{(3, x), (3, y), (3, *), (6, x), (6, y), (6, *), (9, x), (9, y), (9, *), \}.$$

Inoltre, ad esempio $(2, a) \notin A \times B$ e $(y, 3) \notin A \times B$.

Esercizio 6. Consideriamo gli insiemi

$$A = \{-1, -2, -3, 1, 2\}, \qquad B = \{0, 5, -3, 2\},$$
$$C = \{-1, 2, 1\} \qquad \text{e} \qquad D = \{p \in \mathbb{Z} : -1 < p \leq 5\}.$$

Determinare $A \times B$, $C \times B$, $D \times C$.

Check list. In questo capitolo sono stati introdotti vari simboli:

$$\in,\ \notin, \forall, \exists, \cap,\ \cup,\ |, \cap,\ \cup,\ =,\ \neq,\ \subsetneq,\ \subseteq,\ A \times B,\ \mathscr{P}(A),\ \complement_A(B),\ A \setminus B.$$

2. Logica

La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo,
sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalit à ,
e richiede l'adempimento dei doveri inderogabili
di solidariet à politica, economica e sociale.

Alla base della logica (matematica) ci sono le così dette *proposizioni* (*dichiarative*), ovvero le proposizioni (nel senso della logica classica) delle quali (tramite giudizio) si possa affermare con certezza (stabilire senza ambiguità) se sono vere o false. Se una proposizione è vera, ad essa si attribuisce valore di verità V (o 1 o anche T), se è falsa si attribuisce ad essa valore di verità F (o 0). Pertanto una proposizione non può essere contemporaneamente vera e falsa.

Esempio 25. Consideriamo
P: 8 è un numero dispari.
Q: Il cane è un mammifero.
Certamente la proposizione P è falsa, la proposizione Q è vera. Quindi il valore di verità di P è F, il valore di verità di Q è V.

Esempio 26. Consideriamo:
R: le cicorie sono buone;
S: x è un numero positivo.
Queste non possono essere classificate come proposizioni: R perchè presenta un predicato che non è di carattere oggettivo, per cui ciascuno può attribuire valore di verità V o F secondo i propri gusti; S presenta una variabile e quindi non si può stabilire se è vera o falsa. Ad esempio se $x = 4$ allora S è vera, se $x = -1$ oppure $x = penna$ allora S è falsa.

Esempio 27. Se si usano i quantificatori, si ha:
$\forall x \in \mathbb{Z}$ allora x è positivo. Questa è una proposizione che ha valore di verità F.
$\exists x \in \mathbb{Z}$ tale che x è positivo. Questa è una proposizione che ha valore di verità V, ad esempio esiste il numero intero $x = 2$ che è positivo.

Esempio 28. Ad esempio
P: Parigi è una città in Puglia. F

Esempio 29. Ad esempio
P: z+2=5. Questa non è una proposizione visto che non si può dire se è vera o falsa. Se $z = 3$ allora è vera, se $z = 4$ allora è falsa.

2.1. Negazione, Congiunzione, Disgiunzione, Implicazione.

Le proposizioni possono essere combinate tramite i connettivi logici per costruire altre proposizioni. [7]

Data una proposizione, con la negazione costruiamo una nuova proposizione.

Definizione 12. (NEGAZIONE) Data una proposizione P, la *negazione* della proposizione P si indica con

$$\bar{P} \text{ oppure } \neg P.$$

Se P è vera allora $\bar{P}$ è falsa. Se P è falsa allora $\bar{P}$ è vera.

Esempio 30. P: Roma è una citta del Lazio. V
$\bar{P}$: Roma non è una citta del Lazio. F

[7] Inotrodotto dal matematico Inglese George Boole, The Laws of Tought, 1854.

Esempio 31. P: Parigi è una citta in Puglia. F
$\bar{P}$: Parigi non è una citta in Puglia. V

Dalla definizione si deduce subito la tavola di verità della negazione

P	$\bar{\mathbf{P}}$
V	F
F	V.

Esempio 32. Scrivere la negazione della seguente proposizione.
P: Ogni giorno Marco va a Roma ($\forall$).
Allora si ha:
$\bar{P}$: Non è vero che ogni giorno Marco va a Roma = Esiste un giorno in cui Marco non va a Roma ($\exists$).

Esempio 33. Scrivere la negazione della seguente proposizione.
P: Esiste un numero pari ($\exists$).
Allora si ha:
$\bar{P}$: Non esiste un numero pari = Ogni numero non è pari ($\forall$) = Ogni numero è dispari ($\forall$).

La negazione di una proposizione è una nuova proposizione. Ora introduciamo i connettivi logici, che da due proposizione, costruiscono altre proposizioni.

Definizione 13. (CONGIUNZIONE, $\wedge$) Siano P e Q due proposizioni. La proposizione "P *e* Q "(*congiunzione di* P *e* Q) si denota con

$$P \wedge Q.$$

È vera quando P e Q sono entrambe vere ed è falsa altrimenti (ovvero è falsa quando una delle due è falsa).

La tavola di verità della congiunzione è:

P	**Q**	**P** $\wedge$ **Q**
V	V	V
V	F	F
F	V	F
F	F	F.

Esempio 34. Scrivere la congiunzione delle seguenti proposizioni.
P: Il cellulare è rosso.
Q: Il cellulare è a led.
Allora si ha:
$P \wedge Q$: Il cellulare è rosso ed è a led.

Esercizio 7. Scrivere la congiunzione delle seguenti proposizioni.
P: La mosca è un insetto.
Q: 4 è un numero dispari.
Allora si ha:
$P \wedge Q$: La mosca è un insetto e 4 è un numero dispari.
Certamente $P \wedge Q$ ha valore di verità F perchè P ha valore di verità V ma Q ha valore di verità F.

Definizione 14. (DISGIUNZIONE, $\vee$) Siano P e Q due proposizioni. La proposizione "P *o* Q "(*disgiunzione di* P *e* Q) si denota con

$$P \vee Q.$$

È falsa quando P e Q sono entrambe false ed è vera altrimenti (ovvero vera quando almeno una delle due è vera).

Si deduce la tavola di verità della disgiunzione:

P	**Q**	**P ∨ Q**
V	V	V
V	F	V
F	V	V
F	F	F.

Esempio 35. Scrivere la disgiunzione delle seguenti proposizioni.
P: Il cellulare è un Iphone.
Q: Il cellulare è un Samsung.
Allora si ha:
$P \vee Q$: Il cellulare è un Iphone o un Samsung.

Esempio 36. Scrivere la tabella di verità di $P \wedge \bar{P}$.

P	$\bar{\mathbf{P}}$	**P ∧ $\bar{\mathbf{P}}$**
V	F	F
F	V	F

La proposizione $P \wedge \bar{P}$ è sempre falsa.

Definizione 15. Una proposizione sempre falsa si dice *contraddizione*.

Esempio 37. Scrivere la tabella di verità di $P \vee \bar{P}$.

P	$\bar{\mathbf{P}}$	**P ∨ $\bar{\mathbf{P}}$**
V	F	V
F	V	V

La proposizione $P \vee \bar{P}$ è sempre vera.

Definizione 16. Una proposizione sempre vera si dice *tautologia*.

Definizione 17. (IMPLICAZIONE, $\longrightarrow$) Siano P e Q due proposizioni. La proposizione implicazione "P *implica* Q "si denota con $P \longrightarrow Q$ ed è falsa quando P è vera e Q è falsa ed è vera altrimenti, (ovvero se P è vera allora Q deve essere vera).

Possiamo costruire la tavola di verità della implicazione.

P	**Q**	**P ⟶ Q**
V	V	V
V	F	F
F	V	V
F	F	V

Se P è falsa tutto può succedere.

Esempio 38. (Differenza con i linguaggi di programmazione)
P: 2+4=6
Q: x:=x+1
$P \longrightarrow Q$: if 2+4=6 then x:=x+1
Se assegnamo alla $x = 0$, allora ci restituisce $x = 1$.
Intanto non sono proposizioni, P è una proposizione mentre Q è un programma da eseguire. Il computer esegue solo se la prima è vera altrimenti non fa nulla.

Definizione 18. (DOPPIA IMPLICAZIONE $\longleftrightarrow$) La *doppia implicazione* di P e Q è una proposizione che è vera solo se P e Q sono entrambe vere o entrambe false. Si denota con

$$P \longleftrightarrow Q,$$

e si legge P se e solo se Q.

La tavola di verità della doppia implicazione è:

P	**Q**	**P $\longleftrightarrow$ Q**
V	V	V
V	F	F
F	V	F
F	F	V

Quindi la doppia implicazione è vera quando sono vere entrambe le implicazioni $P \longrightarrow Q$ e $Q \longrightarrow P$

Definizione 19. (EQUIVALENZA $\Longleftrightarrow$) Due proposizioni P e Q si dicono *equivalenti* e si scrive

$$P \Longleftrightarrow Q,$$

se P è vera se e soltanto se Q è vera, ovvero se P e Q hanno le stesse tavole di verità. In tal caso diremo P è equivalente a Q. Notiamo che $P \Longleftrightarrow Q$ se e solo se la proposizione $P \longleftrightarrow Q$ è una tautologia.

Osservazione 12. Qui potrebbe nascere un pò di confusione sulla differenza tra $P \longleftrightarrow Q$ e $P \Longleftrightarrow Q$. La prima è una proposizione con i suoi valori di verità riassunti nella tavola. La seconda $P \Longleftrightarrow Q$ non è una proposizione ma il simbolo $\Longleftrightarrow$ rappresenta la circostanza che le due proposizioni sono equivalenti. Le due proposizioni sono equivalenti quando la loro doppia implicazione è una tautologia.

Esercizio 8. Siano P e Q due proposizioni. Dimostrare che le seguenti proposizioni sono equivalenze:

$$\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q} \qquad \text{e} \qquad \overline{P \vee Q} \Longleftrightarrow \overline{P} \wedge \overline{Q}$$

Suggerimento: fare tavole di verità.

Esempio 39. Consideriamo le proposizioni:
P: Il computer ha Linux (come sistema operativo).
Q: Il computer ha 500GB (di hard disk).
Le proposizioni negazione di P e di Q sono:
$\overline{P}$: Non è vero che il computer ha Linux = il computer non ha Linux.
$\overline{Q}$: Non è vero che il computer ha 500GB= il computer non ha 500GB.
Allora abbiamo:
$P \vee Q$: Il computer ha Linux o 500GB.
$\overline{P \vee Q}$: Non è vero che il computer ha Linux o 500GB = il computer non ha Linux e non ha 500GB= $\overline{P} \wedge \overline{Q}$.
$P \wedge Q$: Il computer ha Linux e 500GB.
$\overline{P \wedge Q}$: Non è vero che il computer ha Linux e 500GB = il computer non ha Linux o non ha 500GB= $\overline{P} \vee \overline{Q}$.

Esempio 40. Consideriamo le Proposizioni P e Q:
P: Ogni giorno vado a Roma.
Q: Ogni giorno uso il cellulare.
Determinare $P \wedge Q$ e la sua negazione $\overline{P \wedge Q}$. Allora abbiamo che:
$P \wedge Q$: Ogni giorno vado a Roma e ogni giorno uso il cellulare.
Quindi la sua negazione è la proposizione:

$\overline{P \wedge Q}$: Non è vero che ogni giorno vado a Roma e ogni giorno uso il cellulare = Esiste almeno un giorno in cui non vado a Roma o esiste almeno un giorno in cui non uso il cellulare.

Le proposizioni negazione di P e di Q sono:

$\overline{P}$: Non è vero che ogni giorno vado a Roma = Esiste almeno un giorno in cui non vado a Roma.

$\overline{Q}$: Non è vero che giorno uso il cellulare = Esiste almeno un giorno in cui non uso il cellulare.

La proposizione $\overline{P} \vee \overline{Q}$ risulta essere

$\overline{P} \vee \overline{Q}$: Esiste almeno un giorno in cui non vado a Roma o esiste almeno un giorno in cui non uso il cellulare = $\overline{P \wedge Q}$.

Determinare $P \vee Q$ e $\overline{P \vee Q}$. Allora si ha

$P \vee Q$: Ogni giorno vado a Roma o ogni giorno uso il cellulare.

La proposizione $\overline{P \vee Q}$ risulta essere

$\overline{P \vee Q}$: Non è vero che ogni giorno vado a Roma o ogni giorno uso il cellulare = Esiste almeno un giorno in cui non vado a Roma ed esiste almeno un giorno in cui non uso il cellulare = $\overline{P} \wedge \overline{Q}$.

Esercizio 9. Siano P e Q due proposizioni. Dimostrare che $P \longrightarrow Q$ equivale a $\overline{Q} \longrightarrow \overline{P}$.

P	**Q**	$\overline{\mathbf{P}}$	$\overline{\mathbf{Q}}$	$\mathbf{P} \longrightarrow \mathbf{Q}$	$\overline{\mathbf{Q}} \longrightarrow \overline{\mathbf{P}}$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

2.2. **Tecniche di dimostrazione.** Cosa Significa provare un teorema?

Un teorema è una affermazione che vogliamo dimostrare essere vera. Generalmente è della forma

Se P allora Q, ovvero vogliamo dimostrare che la proposizione $P \longrightarrow Q$ è vera.

La proposizione P è detta *ipotesi* del teorema e la proposizione Q è la *tesi*.

Quindi vogliamo dimostrare l'implicazione. Poiché la proposizione implicazione $P \longrightarrow Q$ è falsa solo nel caso in cui P è vera e Q è falsa, per dimostrare che è vera basta dimostrare che se P è vera allora anche Q è vera.

Per questo si dice, nel teorema c'è l'ipotesi vera e vogliamo dimostrare vera anche la tesi. In generale in un teorema useremo la notazione $P \Longrightarrow Q$, Q è conseguenza logica di P, rappresenta la circostanza in cui la proposizione $P \longrightarrow Q$ è vera.

Dimostrazione diretta: è appunto assumere P vera e usando, definizioni, cose già note o dimostrate, assiomi e connettivi logici, provare che anche Q è vera.

Dimostrazione indiretta:

Poichè la proposizione $P \longrightarrow Q$ equivale a $\overline{Q} \longrightarrow \overline{P}$, allora per dimostrarla basta dimostrare che $\overline{Q} \longrightarrow \overline{P}$ è vera. Quindi si assume vera $\overline{Q}$ e si dimostra vera $\overline{P}$. Quindi si assume che la tesi Q non è vera (quindi $\overline{Q}$ è vera) e si cerca di dimostrare che l'ipotesi P è falsa (ovvero che $\overline{P}$ è vera).

Per Saperne di più. A cosa serve la logica? La logica è alla base del ragionamento matematico e non solo. È alla base della programmazione, dell'intelligenza artificiale, dei linguaggi di programmazione, etc..

Per capire la matematica, dobbiamo capire cosa è un ragionamento corretto, ovvero una dimostrazione. Una volta che con un ragionamento logico abbiamo provato che una affermazione è vera, allora l'affermazione la chiamiamo teorema e il nostro ragionamento logico la sua dimostrazione.

Le dimostrazioni, non sono solo un artificio (o tortura) che piace ai matematici, le dimostrazioni sono fondamentali nella computer science. Ad esempio, le dimostrazioni sono usate nel linguaggio di programmazione per verificare che l'output è corretto per

tutti i possibili input. Sono usate per verificare che gli algoritmi usati danno i risultati corretti (e voluti) e ovviamente sono alla base dell'intelligenza artificiale.

Inoltre, conoscendo una dimostrazione di un teorema, spesso ci suggerisce l'idea di come poterla estendere e modificare per applicarla a nuovi casi. Analizzando varie tecniche dimostrative, implementiamo il nostro bagaglio di strategie da utilizzare per affrontare e superare problemi tecnici nell'ambito dell'Informatica.

Vedremo vari metodi di dimostrazioni, e li useremo per prendere pratica con queste tecniche. Uno degli obiettivi principali del corso è capire cosa sia un ragionamento corretto e soprattutto come costruirlo, in modo da poter utilizzare queste tecniche nei campi dell'Informatica.

Check list. In questo capitolo abbiamo introdotto tutti i simboli logici che useremo: $\vee$, $\wedge$, $\bar{P}$, $\longrightarrow$, $\Longrightarrow$, $\longleftrightarrow$, $\Longleftrightarrow$.

3. Funzioni

Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge,
senza distinzione di sesso, di razza, di lingua, di religione,
di opinioni politiche, di condizioni personali e sociali. (I parte)

Definizione 20. (FUNZIONE) Dati due insieme A e B diversi dall'insieme vuoto, una *funzione* (o *applicazione*) f dall'insieme A all'insieme B è una legge che ad ogni elemento di A associa un unico elemento dell'insieme B. Notazione

$$f : A \longrightarrow B.$$

A è l'*insieme di partenza* ed è anche detto *dominio* di f.

B è l'*insieme di arrivo* di f.

Formalmente,

$$\forall a \in A \qquad \exists! b \in B \text{ tale che } f(a) = b.$$

Se $f(a) = b$, allora b è il valore della funzione in a, b è detto *immagine* di a; per definizione b è unico. Per indicare $f(a) = b$ si usa anche la notazione $a \mapsto b$.

Fare graficamente con i diagramma di Venn.

Esempio 41. Siano $A = \{a, b, c\}$ e $B = \{2, 4, 6\}$ e $f : A \to B$ la legge che associa ad $a \mapsto 4, b \mapsto 4, c \mapsto 2$. Tale f è una funzione da A a B.

Esempio 42. Consideriamo

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall\, n \in \mathbb{N} \qquad f(n) = n + 3,$$

ovvero $f(n) = n + 3$ è una funzione. Ad esempio $f(1) = 4$, $f(10) = 13$ e $f(0) = 3$.

Esempio 43. Consideriamo

$$f : \mathbb{Z} \to \mathbb{N} \qquad \forall\, n \in \mathbb{Z} \qquad n \mapsto n + 3,$$

ovvero $f(n) = n + 3$ Non è una funzione perché $f(-10) = -10 + 3 = -7$ che non appartiene ad $\mathbb{N}$.

La legge f si può chiamare anche g, h, etc.. Così come anche l'elemento dell'insieme.

Esempio 44. Consideriamo

$$g : \mathbb{Q} \to \mathbb{R} \qquad \forall\, x \in \mathbb{Q} \qquad g(x) = \frac{4}{x - 2}.$$

Allora g NON è una funzione, perché $g(2)$ non è definito.

Esempio 45. Consideriamo

$$g : \mathbb{Q} \setminus \{2\} \to \mathbb{R} \qquad \forall\, y \in \mathbb{Q} \setminus \{2\} \qquad g(y) = \frac{4}{y - 2}.$$

Allora g è una funzione.

Esempio 46. Siano $A =$ { città d'Italia } e $B =$ { regioni d'Italia } e f la legge che associa ad ogni città la regione di appartenza, $f : A \to B$ è una funzione ben definita.

La legge g che associa ad ogni città una regione a cui non appartiene non è ben definita, perché ad una città non corrisponde una unica regione.

Definizione 21. (FUNZIONI che COINCIDONO) Due funzioni f e g *coincidono* (si dice anche che sono *uguali*) se e solo se hanno lo stesso insieme di partenza A, lo stesso insime di arrivo B, e $f(a) = g(a)$ $\forall a \in A$.

Esempio 47. Le funzioni

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall\, n \in \mathbb{N} \qquad f(n) = 6n + 3,$$

ovvero $f(n) = 6n + 3$, e

$$g : \mathbb{N} \to \mathbb{N} \qquad \forall\, n \in \mathbb{N} \qquad g(n) = (1 + 2n)3$$

coincidono. Infatti $\forall n \in \mathbb{N}$ si ha $6n + 3 = (1 + 2n)3$.

Nota Bene 3. Ad esempio

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall\, n \in \mathbb{N} \qquad f(n) = 6n + 3$$

e

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall\, t \in \mathbb{N} \qquad f(t) = 6t + 3$$

sono la stessa funzione.

Definizione 22. (IMMAGINE) L'*immagine* (o immagine diretta) di una funzione $f : A \to B$ si indica con $Im(f)$ oppure $f(A)$ ed è il sottoinsieme di B i cui elementi sono le immagini di tutti gli elementi di A, ovvero

$$f(A) \subseteq B \qquad f(A) = \{b \in B \mid \exists a \in A \text{ con } f(a) = b\} = \{f(a) \mid a \in A\}.$$

In generale, dato un sottoinsieme $A' \subseteq A$. L'immagine di A' è il sottoinsieme $f(A') \subseteq B$ con

$$f(A') \subseteq B \qquad f(A') = \{b \in B \mid \exists a \in A' \text{ con } f(a) = b\} = \{f(a) \mid a \in A'\}.$$

Fare il diagramma di Venn.

Esempio 48. Sia assegnata la seguente funzione

$$g : \mathbb{Z} \to \mathbb{Z} \qquad \forall\, a \in \mathbb{Z} \qquad g(a) = 4a.$$

Calcolare l'immagine $g(\mathbb{Z})$ e di $A' = \{1, -1, -3, -4, 0\}$.

Allora,

$$g(\mathbb{Z}) = \{b \in \mathbb{Z} \mid \exists a \in \mathbb{Z} \text{ con } g(a) = b\} =$$

$$= \{b \in \mathbb{Z} \mid \exists a \in \mathbb{Z} \text{ con } b = 4a\} = \text{ multipli di 4 .}$$

Inoltre,

$$g(A') = \{b \in \mathbb{Z} \mid \exists a \in A' \text{ con } g(a) = b\ \};$$

dato che $g(1) = 4, g(-1) = -4, g(-3) = -12, g(-4) = -16, g(0) = 0$, allora

$$g(A') = \{-4, 4, 0, -16, -12\}$$

Esempio 49. Se consideriamo

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall\, n \in \mathbb{N} \qquad f(n) = n + 3,$$

allora $Im(f) = f(\mathbb{N}) = \mathbb{N} \setminus \{0, 1, 2\}$.

Definizione 23. (CONTROIMMAGINE) Sia data una funzione $f : A \to B$ e sia $Y \subseteq B$. La *controimmagine* di Y (o immagine inversa o immagine reciproca di Y) è il sottoinsieme di A, e si indica $f^{-1}(Y)$, costituito da tutti gli elementi di A la cui immagine appartiene a Y, ovvero

$$f^{-1}(Y) \subseteq A \qquad f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

In particolare,

$$f^{-1}(B) = \{a \in A \mid f(a) \in B\} = A.$$

Esempio 50. Sia assegnata la seguente funzione

$$g : \mathbb{Z} \to \mathbb{Z} \qquad \forall\ a \in \mathbb{Z} \qquad g(a) = 4a$$

Calcolare la controimmagine di $Y = \{5, 7\}$, $D = \{16\}$ e di $C = \{2, -4, 0\}$.

Allora,

$$g^{-1}(Y) = \{x \in \mathbb{Z} \mid\ g(x) \in Y = \{5, 7\}\} = \{x \in \mathbb{Z} \mid\ g(x) = 5\ o\ g(x) = 7\}$$
$$= \{x \in \mathbb{Z} \mid\ 4x = 5\ o\ 4x = 7\} = \emptyset.$$

Inoltre,

$$g^{-1}(D) = \{4\} \qquad \text{e} \qquad g^{-1}(C) = \{-1, 0\}.$$

Osservazione 13. Data la funzione $f : A \to B$, si usa spesso la notazione $f^{-1}(\{b\}) = f^{-1}(b)$ con $b \in B$. In generale, non è detto che $f^{-1}(b)$ sia un insieme con un unico elemento.

Esercizio 10. Consideriamo la funzione

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall\ x \in \mathbb{R} \qquad f(x) = x^2.$$

Calcolare $f^{-1}(1)$ e $f^{-1}(-4)$.

Esempio 51. (Funzione COSTANTE) Siano A e B due insieme e sia $b_0 \in B$ un elemento fissato. Allora possiamo definire la funzione *costante*

$$f : A \to B \qquad \forall a \in A \qquad f(a) = b_0.$$

Ogni elemento di A è mandato in b_0.

Inoltre, $f^{-1}(b_0) = A$, $f^{-1}(c) = \emptyset$ per ogni $c \neq b_0$ $f(A') = \{b_0\}$ per ogni sottoinsieme A' non vuoto di A.

Fare il diagramma di Venn.

Esempio 52. La funzione

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = 3$$

manda tutto in 3.

Esempio 53. (Funzione IDENTITÀ) Sia A un insieme. Allora possiamo definire la *funzione identità* (o funzione identica)

$$f = Id_A : A \to A \qquad \forall a \in A \qquad f(a) = a.$$

Ogni elemento mandato in se stesso. Si usa anche la notazione id_A.

Esempio 54. Consideriamo

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall\ x \in \mathbb{R} \qquad f(x) = x.$$

Allora f manda ogni elemento in se stesso, ovvero f è la funzione identità.

Proprietà Sia $f : A \to B$ una funzione, e siano $X, X' \subseteq A$ e $Y, Y' \subseteq B$. Allora:

(1) $f(X \cap X') \subseteq f(X) \cap f(X')$

(2) $f(X \cup X') = f(X) \cup f(X')$

(3) $f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$

(4) $f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$

Esercizio 11. Dimostrare le Proprietà enunciate.

Esempio 55. Consideriamo

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = x^2.$$

Sia $X = \{-2, 0\}$ e $X' = \{0, 2\}$ allora $f(X) = \{0, 4\}, f(X') = \{0, 4\}$ e quindi $f(X) \cap f(X') = \{0, 4\}$. Invece, $X \cap X' = \{0\}$ e $f(X \cap X') = \{f(0)\} = \{0\}$.

Utile introdurre grafico di una funzione.

Definizione 24. (GRAFICO) Il *grafico di una funzione* $f : A \to B$ è un sottoinsieme del prodotto cartesiano $A \times B$, costituito dalle coppie ordinate $(a, f(a))$, al variare di $a \in A$. Ovvero

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

Esempio 56. Consideriamo

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = x^2.$$

Allora il grafico di f:

$$\Gamma(f) = \{(x, f(x)) \in \mathbb{R} \times \mathbb{R} \mid x \in \mathbb{R}\} = \{(x, x^2) \in \mathbb{R} \times \mathbb{R} \mid x \in \mathbb{R}\}.$$

Osservazione 14. Nel corso di Analisi studierete in maniera approfondita il concetto di grafico.

3.1. **Funzioni Iniettive.**

Definizione 25. (INIETTIVA) Sia $f : A \to B$ una funzione. La funzione f è detta *iniettiva* se elementi distinti di A hanno immagini distinte in B. Ovvero,

$$\forall a, a' \in A \quad a \neq a' \Longrightarrow f(a) \neq f(a').$$

Equivalentemente

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

(L'equivalenza è dovuta al fatto che $P \longrightarrow Q$ equivale a $\overline{Q} \longrightarrow \overline{P}$, Esercizio 9.)

Fare il diagramma di Venn.

Osservazione 15. Una funzione $f : A \to B$ non è iniettiva se $\exists a, a' \in A$ con $a \neq a'$ e $f(a) = f(a')$.

Esempio 57. Consideriamo

$$f : \mathbb{Z} \to \mathbb{Z} \qquad \forall a \in \mathbb{Z} \qquad f(a) = 3a - 4.$$

Allora la funzione f è iniettiva. Infatti, $\forall a, a' \in \mathbb{Z}$, se $f(a) = f(a')$ allora $3a - 4 = 3a' - 4$ che implica $a = a'$.

Esempio 58. La funzione

$$f : \mathbb{Z} \to \mathbb{N} \qquad \forall n \in \mathbb{Z} \qquad f(n) = n^2$$

non è iniettiva. Infatti, $f(-2) = 4 = f(2)$.

Esempio 59. Consideriamo la funzione modulo

$$f : \mathbb{Z} \to \mathbb{N} \qquad \forall x \in \mathbb{Z} \qquad f(x) =\mid x \mid$$

definita nel seguente modo:

$$|x| = \begin{cases} x & \text{se } x \geq 0, \\ -x & \text{se } x < 0. \end{cases}$$

Allora f non è iniettiva, infatti: $f(4) = 4 = f(-4)$.

Esempio 60. Consideriamo

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall x \in \mathbb{N} \qquad f(x) = 2x.$$

Allora f è iniettiva.

Esempio 61. La funzione costante è iniettiva? Siano A e B due insieme e sia $b_0 \in B$ un elemento fissato. Allora possiamo definire la funzione costante

$$f : A \to B \qquad \forall a \in A \qquad f(a) = b_0.$$

Tutto mandato in b_0. Quindi la funzione costante è iniettiva se e solo se A contiene un solo elemento.

Esempio 62. In generale, siano $c, d \in \mathbb{R}$. Consideriamo la funzione

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = cx + d.$$

La funzione f è iniettiva?

Se $c = 0$ no perché otteniamo la funzione costante. Altrimenti, se $c \neq 0$, allora $f(x) = f(x')$ se e solo se $cx + d = cx' + d$ se e solo se $x = x'$. Quindi f è iniettiva.

Nota Bene 4. Se $f : A \to B$ è una funzione iniettiva, allora per ogni $b \in B$ l'insieme controimmagine $f^{-1}(b)$ ha al più un elemento.

3.2. **Funzioni Suriettive.**

Definizione 26. (SURIETTIVA) Sia $f : A \to B$ una funzione. La funzione f è detta *suriettiva* se $Im(f) = f(A) = B$, ovvero se $\forall y \in B \qquad \exists a \in A$ con $f(a) = b$.

Fare il diagramma di Venn.

Esempio 63. Consideriamo

$$f : \mathbb{Z} \to \mathbb{Z} \qquad \forall n \in \mathbb{Z} \qquad f(n) = 3n - 4.$$

Allora f non è suriettiva. Infatti, ci chiediamo, è vero che $\forall b \in \mathbb{Z}$, esiste $a \in \mathbb{Z}$ tale che $f(a) = b$? Dire che $3a - 4 = b$ equivale ad affermare $3a = b + 4$ da cui segue che $a = \frac{b+4}{3}$. Tale elemento a appartiene a $\mathbb{Z}$ per ogni scelta di b in $\mathbb{Z}$? Non sempre! Se $b = 0$ tale elemento $a = \frac{0+4}{3} = \frac{4}{3}$ non appartiene a $\mathbb{Z}$. Quindi non è suriettiva.

Esempio 64. Consideriamo

$$f : \mathbb{Q} \to \mathbb{Q} \qquad \forall n \in \mathbb{Q} \qquad f(n) = 3n - 4.$$

Allora f è suriettiva.

Esempio 65. La funzione costante è suriettiva? Siano A e B due insieme e sia $b_0 \in B$ un elemento fissato. La funzione costante

$$f : A \to B \qquad a \mapsto b_0 \qquad \forall a \in A.$$

è suriettiva se e solo se B è un elemento, cioè $B = \{b_0\}$.

Esempio 66. In generale, siano $c, d \in \mathbb{R}$. Consideriamo la funzione

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = cx + d.$$

La funzione f è suriettiva?

Se $c = 0$, no perché otteniamo la funzione costante. Altrimenti, se $c \neq 0$, si ha che f è suriettiva se e solo se $\forall y \in \mathbb{R}$ esiste $x \in \mathbb{R}$ con $f(x) = y$. Questo equivale a $cx + d = y$ ovvero $x = \frac{y-d}{c} \in \mathbb{R}$. Quindi è suriettiva per ogni $c \neq 0$.

Esempio 67. La funzione

$$f : \mathbb{Z} \to \mathbb{N} \qquad \forall x \in \mathbb{Z} \qquad f(x) = x^2$$

non è suriettiva. La funzione

$$f : \mathbb{Q} \to \mathbb{Q} \qquad \forall x \in \mathbb{Z} \qquad f(x) = x^4$$

non è suriettiva.

Esempio 68. La funzione

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = x^5$$

è suriettiva.

Esercizio 12. Capire l'Esempio 67 e l'Esempio 68.

Nota Bene 5. Come abbiamo visto la nozione di funzione iniettiva e suriettiva, dipende anche dall'insieme di partenza e dall'insieme di arrivo e non solo dalla legge.

Nota Bene 6. La funzione $f : A \to B$ è suriettiva, se e solo se $f^{-1}(b) \neq \emptyset$, per ogni $b \in B$.

3.3. **Funzioni Biettive.**

Definizione 27. (BIETTIVA) Una funzione $f : A \to B$ è detta funzione *biettiva* se è sia iniettiva che suriettiva. Ovvero

$$\forall b \in B,\ \exists!\, a \in A \text{ con } f(a) = b$$

Infatti

$$(f \text{ è suriettiva}) \qquad \forall b \in B,\ \exists\, a \in A \text{ con } f(a) = b$$

e

$$(f \text{ è intiettiva}) \qquad \forall a, a' \in A \quad a \neq a' \Longrightarrow f(a) \neq f(a').$$

Allora, per ogni $b \in B$ l'insieme controimmagine $f^{-1}(b)$ è costituito esattamente da un unico elemento.

Osservazione 16. Terminolgia: Una funzione biettiva spesso è chiamata anche *corrispondenza biunivoca.*

Esempio 69. Sia A un insieme non vuoto, allora la funzione identità è biettiva.

Esempio 70. Si consideri

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = x^5 - 4.$$

La funzione f è biettiva? Come si dimostra?

Esempio 71. La funzione

$$f : \mathbb{Z} \to \mathbb{N} \qquad \forall x \in \mathbb{Z} \qquad f(x) = x^2$$

non è biettiva, poiché non è ne suriettiva ne iniettiva. La funzione

$$f : \mathbb{Q} \to \mathbb{Q} \qquad \forall x \in \mathbb{Z} \qquad f(x) = x^4$$

non è suriettiva e non è iniettiva, quindi non è biettiva.

Esempio 72. In generale, siano $c, d \in \mathbb{R}$. Consideriamo la funzione

$$f : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad f(x) = cx + d.$$

Se $c \neq 0$ allora, applicando l'Esempio 62 e l'Esempio 66, si ha che f è biettiva.

3.4. **Composizione di Funzioni.**

Definizione 28. (COMPOSIZIONE) Date due funzioni $f : A \to B$ e $g : B \to C$, la funzione composizione g composto f, si indica con $g \circ f$ (si legge anche g dopo f, oppure g cerchietto f) ed è la funzione

$$g \circ f : A \to C \text{ tale che} \qquad \forall\, a \in A \qquad (g \circ f)(a) = g(f(a)),$$

quindi

$$A \xrightarrow{f} B \xrightarrow{g} C \qquad\qquad a \mapsto f(a) \mapsto g(f(a)),$$

ovvero prima facciamo f e poi facciamo g. L'insieme di partenza della funzione composta $g \circ f$ è uguale all'insieme di partenza di f, l'insieme di arrivo di $g \circ f$ è quello di g.

Nota Bene 7. In generale si ha $g \circ f \neq f \circ g$, a volte non sono definite entrambe.

Esempio 73. Consideriamo

$$f : \mathbb{N} \to \mathbb{N} \qquad \forall x \in \mathbb{N} \qquad f(x) = x^2,$$

$$g : \mathbb{N} \to \mathbb{N} \qquad \forall t \in \mathbb{N} \qquad g(t) = t + 2.$$

Calcolare se esistono $g \circ f$ e $f \circ g$.

Esiste $g \circ f$? Si insieme arrivo di f =insieme partenza g allora

$$g \circ f : \mathbb{N} \to \mathbb{N} : \forall a \in \mathbb{N} \qquad a \mapsto a^2 \mapsto a^2 + 2.$$

Esiste $f \circ g$? Si insieme arrivo di g = insieme partenza f allora

$$f \circ g : \mathbb{N} \to \mathbb{N} : \forall b \in \mathbb{N} \qquad b \mapsto b + 2 \mapsto (b + 2)^2.$$

Le funzioni composte sono diverse! Infatti, $(g \circ f)(1) = 3$ ed $(f \circ g)(1) = 9$.

Esempio 74. Consideriamo

$$h : \mathbb{N} \to \mathbb{Q}^* \qquad \forall x \in \mathbb{N} \qquad h(x) = \frac{x}{3} + 1$$

$$f : \mathbb{Q}^* \to \mathbb{Q} \qquad \forall y \in \mathbb{Q}^* \qquad g(y) = \frac{1}{y}$$

Calcolare se esistono $h \circ f$ e $f \circ h$.

Esiste $h \circ f$? No insieme arrivo di f è diverso dall'insieme partenza di g.

Esiste $f \circ h$? Si insieme arrivo di h = insieme partenza f allora

$$f \circ h : \mathbb{N} \to \mathbb{Q} : \qquad \forall x \in \mathbb{N} \qquad x \mapsto \frac{x}{3} + 1 \mapsto \frac{1}{\frac{x}{3} + 1} = \frac{3}{x + 3}.$$

PROPRIETÀ della composizione di funzioni.

(1) (ASSOCIATIVA) Siano $f : A \to B$, $g : B \to C$ e $h : C \to D$, tre funzioni allora $h \circ (g \circ f) = (h \circ g) \circ f$.

(2) Siano $f : A \to B$ una funzione e $Id_A : A \to A$ e $Id_B : B \to B$ le funzioni identità di A e B, rispettivamente. Allora si ha

$$f \circ Id_A = Id_B \circ f = f.$$

(3) Se $f : A \to B$ e $g : B \to C$ sono funzioni invettive, allora $g \circ f$ è iniettiva, ma non è vero il viceversa.

(4) Se $f : A \to B$ e $g : B \to C$ sono funzioni suriettive, allora $g \circ f$ è suriettiva, ma non è vero il viceversa.

(5) Se $f : A \to B$ e $g : B \to C$ sono funzioni biettive, allora $g \circ f$ è biettiva, ma non è vero il viceversa.

Esercizio 13. Dimostrare la Proprietà (3) e (4).

Dall'Esercizio 13 segue la Proprietà (5) : se $f : A \to B$ e $g : B \to C$ sono funzioni biettive, allora $g \circ f$ è biettiva. Il viceversa non è vero.

Esempio 75. (CONTROESEMPIO: SURIETTIVITÀ) Esempio di $g \circ f$ è suriettiva, ma f non è suriettiva.

Consideriamo $f : A \to B$ e $g : B \to C$ con $A = \{1\}$, $B = \{a, b, c\}$ e $C = \{t\}$. La funzione f manda tutto in a, la funzione g tutto in t. La composizione è una funzione suriettiva ma f non è suriettiva.

Esempio 76. (CONTROESEMPIO: INIETTIVITÀ) Esempio di $g \circ f$ è iniettiva, ma g non è iniettiva.

Consideriamo $f : A \to B$ e $g : B \to C$ con $A = \{1\}$, $B = \{a, b, c\}$ e $C = \{t\}$. La funzione f manda tutto in a, la funzione g tutto in t. La composizione è una funzione iniettiva, ma g non lo è.

3.5. **Inversa di Funzioni.**

Definizione 29. (INVERSA) Sia $f : A \to B$ una funzione. La funzione f si dice *invertibile* se esiste $g : B \to A$ tale che $g \circ f = Id_A$ e $f \circ g = Id_B$.

La funzione g se esiste è unica e si chiama funzione *inversa* di f e si denota con f^{-1}.

Quindi

$$f^{-1} \circ f = Id_A \qquad f \circ f^{-1} = Id_B$$

Dimostriamo l'unicità dell'inversa:

Supponiamo che esistano $g : B \to A$ e $g' : B \to A$ tale che $g \circ f = Id_A$ e $f \circ g = Id_B$ e $g' \circ f = Id_A$ e $f \circ g' = Id_B$.

Allora abbiamo che

$$g = g \circ Id_B = g \circ (f \circ g') = (g \circ f) \circ g' = Id_A \circ g' = g'.$$

Quindi, $g = g'$ e questo conclude la dimostrazione.

Come determiniamo se una funzione è invertibile?

Teorema 1. *Sia $f : A \to B$ una funzione. La funzione f è invertibile se e solo se f è biettiva.*

Osservazione 17. Come facciamo a determinare l'inversa di una funzione biettiva?

Sia $f : A \to B$ una funzione biettiva, quindi $\forall b \in B, \exists! a \in A$ con $f(a) = b$ Allora $f^{-1} : B \to A$ è tale che $f^{-1}(b) = a$, dove a è l'unico elemento tale che $b = f(a)$.

Esempio 77. La funzione $h : \mathbb{N} \to \mathbb{Q}^* \qquad \forall x \in \mathbb{N} \qquad h(x) = \frac{x}{3} + 1$ non è suriettiva quindi non è biettiva.

Esempio 78. La funzione $f : \mathbb{Q}^* \to \mathbb{Q} \qquad \forall y \in \mathbb{Q}^* \qquad f(y) = \frac{1}{y}$ non è suriettiva (0 non appartiene ad immagine), quindi non è biettiva.

Esempio 79. Consideriamo $h : \mathbb{Q} \to \mathbb{Q} \qquad \forall x \in \mathbb{Q} \qquad h(x) = \frac{x}{3} + 1$. È una funzione biettiva? Quindi dobbiamo capire se h è una funzione iniettiva e suriettiva. È iniettiva? È vero che $\forall a, a' \in A$ se $h(a) = h(a') \Longrightarrow a = a'$?

Allora $h(a) = h(a')$ implica che $\frac{a}{3} + 1 = \frac{a'}{3} + 1$ che implica $\frac{a}{3} = \frac{a'}{3}$, che implica $a = a'$. Quindi h è iniettiva.

È suriettiva? È vero che $\forall b \in \mathbb{Q}$, esiste $a \in \mathbb{Q}$ tale che $h(a) = b$? Quindi $h(a) = b$ implica $b = \frac{a}{3} + 1$, ovvero $b - 1 = \frac{a}{3}$, quindi $a = 3(b-1) \in \mathbb{Q}$, per ogni scelta di $b \in \mathbb{Q}$. Allora h è suriettiva. Ne segue che h è biettiva e pertanto esiste inversa. La funzione inversa è :

$$h^{-1} : \mathbb{Q} \to \mathbb{Q} \qquad \forall b \in \mathbb{Q} \qquad h^{-1}(b) = 3(b-1).$$

Esempio 80. Consideriamo $h : \mathbb{Q} \setminus \{1\} \to \mathbb{Q}^* \qquad \forall x \in \mathbb{Q} \setminus \{1\} \qquad h(x) = \frac{1}{x-1}$. È iniettiva? Si (dimostrare). È suriettiva? Sia $y \in \mathbb{Q}^*$, esiste $x \in \mathbb{Q} \setminus \{1\}$ tale che $h(x) = y$? Quindi $y = \frac{1}{x-1}$. Dato che $x \neq 1$, possiamo moltiplicare e ottenere $y(x-1) = 1$. Ora sfruttiamo $y \neq 0$ e otteniamo $x - 1 = \frac{1}{y}$ che è vero se e solo se $x = \frac{1}{y} + 1$. Per ogni $y \in \mathbb{Q}^*$ si ha che $x = \frac{1}{y} + 1 \in \mathbb{Q} \setminus \{1\}$, e quindi h è suriettiva. Ne segue che è biettiva e pertanto esiste inversa. La funzione inversa è :

$$h^{-1} : \mathbb{Q}^* \to \mathbb{Q} - \{1\} \qquad \forall y \in \mathbb{Q}^* \qquad h^{-1}(y) = \frac{1}{y} + 1.$$

Esempio 81. Consideriamo $h : \mathbb{R} \to \mathbb{R} \qquad \forall x \in \mathbb{R} \qquad h(x) = x^5$. È iniettiva e suriettiva? Si (da dimostrare). Allora h è biettiva e pertanto esiste inversa. La funzione inversa è :

$$h^{-1} : \mathbb{R} \to \mathbb{R} \qquad \forall y \in \mathbb{R} \qquad h^{-1}(y) = \sqrt[5]{y}.$$

PROPRIETÀ

(1) Siano $f : A \to B$ e $g : B \to C$ funzioni biettive. Allora si ha che $g \circ f : C \to A$ è biettiva (visto prima: è la Proprietà (5) della composizioni di funzioni) e quindi è invertibile. Inoltre
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} : C \to A$$

(2) Se $Id_A : A \to A$ è la funzione identica, allora $(Id_A)^{-1} = Id_A$.

(3) Sia $f : A \to B$ una funzione biettiva. Allora $(f^{-1})^{-1} = f$.

Nella prossima sezione vediamo come applicare la definizione di funzioni biettive per contare gli elementi di un insieme.

Per Saperne di più. In Informatica le funzioni sono molto importanti e vengono usate tantissimo. Un esempio è quando si vuole dare un'etichetta ad alcuni oggetti. Dare l'etichetta corrisponde a definire una funzione dal nostro insieme degli oggetti a quello delle etichette possibili (ad un oggetto corrisponde una ed una sola etichetta). Se invece vogliamo associare più etichette ad uno stesso oggetto allora si deve generalizzare il concetto di funzione.

Un altro esempio è la funzione di *hash* usata per capire l'integrità di un messaggio.

La parola inglese significa pasticcio, fare confusione.

In crittografia, la funziona di hash serve per avere un controllo del messaggio.

L'idea è che questa funzione associa ad un messaggio di lunghezza arbitraria un messaggio di lunghezza fissata (valore di hash, hash message digest o somma di controllo)

Deve avere 4 proprietà:

- calcolare il message digest in modo facile e veloce;
- deve essere impossibile capire il messaggio dal hash;
- impossibile modificare un messaggio senza cambiare hash;
- impossibile trovare due messaggi con la stessa hash.

Quindi questa funzione è non invertibile, e soprattutto è iniettiva: se cambiamo anche minimamente il messaggio vogliamo grandi cambiamenti nell'hash di controllo.

Come si usa in pratica? Alice calcola l'hash del messaggio. Poi spedisce messaggio cifrato a Bob e in chiaro la hash trovata (tanto dall'hash non si può ritrovare messaggio proprio perché la funzione non è invertibile).

Chi riceve il messaggio lo decifra e poi calcola la hash. Se è diversa da quella spedita in chiaro, allora il messaggio è stato modificato o attaccato da qualcuno.

La funzione di hash viene anche usata per aumentare la sicurezza: sarebbe sempre meglio conservare la hash e non la password.

Check list. In questo capitolo abbiamo introdotto le funzioni e abbiamo studiato varie nozioni tra cui: grafico, immagine, controimmagine, funzioni, iniettive, suriettive, biettive, composta di funzioni, funzioni invertibili ed inversa.

4. Contare gli elementi di un insieme

È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese. (II parte)

In questa sezione vediamo come applicare la definizione di funzioni biettive per contare gli elementi di un insieme.

Quanti elementi ha l'insieme $\{a, b\}$? Quanti elementi ha l'insieme $\{a, *, n, b\}$? Vogliamo rispondere formalmente a questa domanda. Contare gli elementi è un procedimento del tutto naturale. Nel contare, associamo ad ogni elemento un numero 1,2,3...., prendiamo tutti gli elementi (suriettiva) e non contiamo uno stesso elemento due volte (iniettiva).

Definizione 30. (EQUIPOTENTI) Due insieme A e B si dicono *equipotenti*, oppure che hanno la *stessa cardinalità*, oppure la stessa potenza, se esiste una funzione biettiva tra A e B.

Osservazione 18. Terminologia: Una funzione biettiva spesso è chiamata anche corrispondenza biunivoca.

Esempio 82. Sia $A = \mathbb{N}$ e $P = \{\text{numeri naturali pari}\} = \{n \in \mathbb{N} \mid \exists t \in \mathbb{N} \text{ tale che } n = 2t\}$. Consideriamo $f : \mathbb{N} \to P$ la funzione tale che $\forall n \in \mathbb{N}$, $f(n) = 2n$. Allora f è una funzione biettiva e quindi A e B sono equipotenti, ovvero hanno la stessa cardinalità.

Lo stesso vale per $C = \{$ numeri naturali dispari$\}$.

Esempio 83. Gli insiemi $A = \mathbb{N}$ e $D = \{7n \mid n \in \mathbb{N}\}$ sono equipotenti.

Esempio 84. Siano $A = \{., :, >\}$ e $B = \{1, 2, 3\}$. Definiamo $g : A \to B$ la funzione $g(.) = 2, g(:) = 3, g(>) = 1$. Allora g è una funzione biettiva e quindi gli insieme A e B sono equipotenti. Qui abbiamo fatto una scelta di una funzione biettiva, vedremo quante sono le funzioni biettive in seguito (Osservazione 38). Fare Diagramma di Venn.

Esempio 85. Siano $A = \{a, b, c, d\}$ e $B = \{1, 2, 3\}$. Non sono equipotenti.

Consideriamo gli insieme J_n, al variare di $n \in \mathbb{N}$ e $n \neq 0$ definiti da

$$J_n = \{1, 2, ..., n\} \subseteq \mathbb{N},$$

Quindi $J_1 = \{1\}$, $J_2 = \{1, 2\}$, $J_3 = \{1, 2, 3\}$, etc..

Definizione 31. (FINITO) Un insieme $A \neq \emptyset$ si dice *finito*, se per qualche $n \in \mathbb{N}$, con $n \neq 0$, si ha che A è equipotente a J_n. In questo caso, diremo che la *cardinalità* dell'insieme finito A è n e scriveremo $|A| = n$. Un insieme che non è finito si dice *infinito*.

Osservazione 19. Alcuni testi usano $I_n = \{0, 1, 2, ..., n - 1\}$, che è un insieme sempre con n elementi.

Osservazione 20. La cardinalità di J_n: $|J_n| = n$ e se esiste $g : A \to J_n$ biunivoca allora $|A| = |J_n| = n$.

Osservazione 21. Usando il simbolo di cardinalità, due insiemi finiti A e B sono equipotenti se e solo se $\mid A \mid = \mid B \mid$ ovvero hanno la stessa cardinalità.

Osservazione 22. Per convenzione: Se $A = \emptyset$ allora A è un insieme finito e $|A| = 0$.

Esempio 86. $J_6 = \{1, 2, 3, 4, 5, 6\}, |J_6| = 6$.

Esempio 87. Quale è la cardinalità di $A = \{x, b, a, d\}$? è 4. Infatti esiste una funzione biettiva con J_4.

(J_n sono insiemi di riferimento e sono tutti non equipotenti tra loro).

Definizione 32. (MINORE o UGUALE) Diremo che l'insieme A ha cardinalità minore o uguale a quello di B, e scriveremo $|A| \leq |B|$ se e solo se esiste $f : A \to B$ funzione iniettiva.

Esempio 88. Sia X sottoinsieme di A, $X \subseteq A$, allora l'inclusione $X \to A$ è iniettiva e $|X| \leq |A|$

Nota Bene 8. Per ogni $n \in \mathbb{N}$, gli insiemi $J_n = \{1, \ldots, n\}$, hanno la proprietà che non contengono sottoinsiemi propri equipotenti, ovvero $\nexists\, C \subsetneq J_n$ sottoinsieme proprio con $f : C \to J_n$ biettiva.

(Gli insiemi J_n sono tutti non equipotenti tra loro, per n diversi sono uno contenuto propriamente nell'altro. Quindi non esiste corrispondenza biunivoca tra loro.)

Esempio 89. $J_5 = \{1, 2, 3, 4, 5\}$ ha 5 elementi, non esistono sottoinsiemi propri con 5 elementi.

Infine, si può dimostrare che:
un insieme è finito se e solo se non si può mettere in corrispondenza biunivoca con un suo sottoinsieme proprio.
un insieme è finito se e solo se non esiste una funzione dall'insieme in se stesso che sia iniettiva ma non suriettiva.

Definizione 33. (INFINITO) Un insieme $A \neq \emptyset$ è *infinito*, se e soltanto se non è finito.
Equivalentemente se e solo se esiste un suo sottoinsieme proprio che si può mettere in corrispondenza biunivoca con l'insieme stesso.
Equivalentemente A è un insieme infinito se e solo se esiste una applicazione iniettiva ma non suriettiva da A in se.

Esempio 90. Consideriamo l'insieme $\mathbb{N}$. Nell'Esempio 82 abbiamo dimostrato che esiste una corrispondenza biunivoca tra $\mathbb{N}$ e il sottoinsieme proprio dei numeri pari P. Pertanto $\mathbb{N}$ è infinito.
Oppure, consideriamo $g : \mathbb{N} \to \mathbb{N}$, tale che per ogni $n \in \mathbb{N}$ si ha $n \mapsto 2n + 1$. L'immagine sono i numeri dispari, la funzione g è iniettiva ma non suriettiva, quindi l'insieme $\mathbb{N}$ è infinito.

Per Saperne di più.

Esempio 91. $f : \mathbb{Z} \to \mathbb{N}$, tale che

$$f(x) = \begin{cases} 0 & \text{se } x = 0, \\ 2|x| & \text{se } x < 0, \\ 2x - 1 & \text{se } x > 0; \end{cases}$$

La funzione f è biettiva pertanto $\mathbb{N}$ e $\mathbb{Z}$ sono equipotenti.

Definizione 34. Un insieme A si dice che ha la potenza del *numerabile* (o che è numerabile) se è equipotente ad $\mathbb{N}$, ovvero se si può mettere in corrispondenza biunivoca con $\mathbb{N}$.

Osservazione 23. L'Esempio 91, dimostra che $\mathbb{Z}$ è numerabile. Usando il procedimento diagonale di Cantor, si dimostra che anche $\mathbb{Q}$ è numerabile. Al contrario, $\mathbb{R}$ non è numerabile, si dice che ha la *potenza del continuo*, che è strettamente maggiore.

Check list. In questo capitolo abbiamo introdotto la cardinalità di un insieme e abbiamo definito quando un insieme è finito e quando è infinito.

5. Principio di Induzione

Dato un insieme A abbiamo visto che è infinito oppure è finito. Se è finito abbiamo definito la cardinalità di A usando i sottoinsiemi J_n e l'abbiamo denotata con $|A|$.

Se A è un insieme finito, con $|A| = n$, quale è la cardinalità di $\mathscr{P}(A)$, insieme delle parti di A (Definizione 10)? Ovvero, se $|A| = n$ quanto vale $|\mathscr{P}(A)| =$?

Esempio 92. Se $A = \emptyset$ $\mathscr{P}(\emptyset) = \{\emptyset\}$. Allora $|\mathscr{P}(A)| = 2^0 = 1$.

Se $A = \{1\}$, allora $\mathscr{P}(A) = \{\emptyset, \{1\}\} = \{\emptyset, A\}$. Allora $|\mathscr{P}(A)| = 2^1 = 2$.

Se $A = \{1, 2\}$ allora $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Allora $|A| = 2$ e $|\mathscr{P}(A)| = 4 = 2^2$.

Se $A = \{1, 2, 3\}$, allora $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}, \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Allora, $|A| = 3$ e $|\mathscr{P}(A)| = 8 = 2^3$.

Notiamo che in questo ultimo caso abbiamo scritto gli 8 elementi di $\mathscr{P}(A)$, in modo che i primi 4 non contenessero il nuovo elemento 3 (e quindi sono come quelli del caso $|A| = 2$) e gli altri sono ottenuti dai primi 4 aggiungendo il nuovo elemento 3. Questo tecnica sarà utilizzata nella dimostrazione del caso generale.

Vogliamo dimostrare un risultato che vale per ogni $n \in \mathbb{N}$.

Teorema 2. *Siano n in $\mathbb{N}$ e A un insieme finito con $|A| = n$, allora $|\mathscr{P}(A)| = 2^n$.*

Nota Bene 9. Vogliamo dimostrare l'uguaglianza *per ogni* $n \in \mathbb{N}$, quindi per infiniti casi. *Non* si può dimostrare con degli esempi, altrimenti dovremmo fare un numero infinito di casi.

Per dimostrarlo introduciamo uno strumento matematico potentissimo: il *Principio di Induzione*.

Supponiamo di avere per ogni intero $n \in \mathbb{N}$ una proposizione $P(n)$ che dipende da n e di voler dimostrare che $P(n)$ è vera per ogni $n \in \mathbb{N}$ ovvero $\forall n \geq 0$.

5.1. **Principio di Induzione (prima forma).** Enunciamo il Principio di Induzione (prima forma).

Base induzione: Dimostrare che $P(0)$ è vera.

Passo induttivo: Dimostrare che $\forall\ k \in \mathbb{N}$ si ha che

$$P(k) \text{ vera } \implies P(k+1) \text{ vera.}$$

Allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Osservazione 24. In alcuni testi il passo induttivo è $P(k-1)$ vera $\implies P(k)$ vera $\forall\ k \geq 1$.

5.2. **Principio di Induzione (seconda forma).** Enunciamo il Principio di Induzione (seconda forma).

Base induzione: Dimostrare che $P(0)$ è vera.

Passo induttivo: Dimostrare che $\forall\ k \in \mathbb{N}$ si ha che

$$P(0), P(1), P(2), ..., P(k) \text{ vere } \implies P(k+1) \text{ vera.}$$

Allora $P(n)$ è vera $\forall n \geq 0$ ovvero per ogni $n \in \mathbb{N}$.

Osservazione 25. Il passo induttivo in questa seconda forma si può esprimere nella forma equivalente:

Passo induttivo: Dimostrare che $\forall\ k \in \mathbb{N}$ si ha che

$$P(h) \text{ vera } \forall h \text{ tale che } 0 \leq h \leq k \implies P(k+1) \text{ vera.}$$

Idea del perché funziona:

Ogni sottoinsime U di $\mathbb{N}$ che contiene 0 e ha la proprietà che se $k \in U$ allora $k+1 \in U$ deve coincidere con $\mathbb{N}$ ovvero $U = \mathbb{N}$.

Quindi dobbiamo dimostrare due cose: la base di induzione e il passo induttivo. Per la base di induzione dobbiamo dimostrare che una proposizione è vera: $P(0)$ vera. Per il passo induttivo *non* dobbiamo dimostrare che $P(k)$ è vera $\forall k \geq 0$, ma dobbiamo dimostrare solo una implicazione: per un qualsiasi $k \in \mathbb{N}$ se $P(k)$ è vera allora la proposizione successiva $P(k+1)$ è vera.

Forniamo una dimostrazione del Teorema 2.

Teorema 2. Siano n in $\mathbb{N}$ e A un insieme finito con $|A| = n$, allora $|\mathscr{P}(A)| = 2^n$.

Dimostrazione. Usiamo il principio di induzione (prima forma). Vogliamo dimostrare che $\forall n \in \mathbb{N}$ la seguente proposizione è vera:

$$P(n): \text{ Se } |A| = n, \text{ allora } |\mathscr{P}(A)| = 2^n.$$

Dobbiamo dimostrare due cose.

1) Base induzione: Dimostrare che $P(0)$ è vera: se $|A| = 0$, allora $|\mathscr{P}(A)| = 2^0 = 1$.

Se $n = 0$, $|A| = 0$, quindi $A = \emptyset$ allora $\mathscr{P}(A) = \{\emptyset\}$ Quindi $|\mathscr{P}(A)| = 1$. Quindi $P(0)$ è vera.

2) Passo induttivo: Dimostrare che $\forall k \in \mathbb{N}$ si ha che $P(k)$ vera $\implies P(k+1)$ vera.

Quindi supponiamo vera

$P(k)$: Se $|A| = k$, allora $|\mathscr{P}(A)| = 2^k$;

e dimostriamo che questa implica

$P(k+1)$: Se $|A| = k+1$, allora $|\mathscr{P}(A)| = 2^{k+1}$.

Quindi, sia $|A| = k+1$ ovvero A ha $k+1$ elementi: $A = \{a_1, \ldots a_{k+1}\} = \{a_1, \ldots, a_k\} \cup \{a_{k+1}\} = A' \cup \{a_{k+1}\}$. Ora $|A'| = k$.

Dimostriamo che per contare i sottoinsiemi di A dobbiamo contare tutti i sottoinsiemi di A' due volte (generalizzando quanto detto nell'Esempio 92 con 3 elementi).

In effetti, ogni sottoinsieme di A o contiene a_{k+1} o non lo contiene. Se non contiente a_{k+1} allora è un sottoinsieme di A', se invece contiene a_{k+1} è ottenuto da un sottoinsieme di A' a cui abbiamo aggiunto a_{k+1}.

Quindi dobbiamo contare tutti i sottoinsiemi di A' (che sono anche sottoinsiemi di A) e quelli ottenuti aggiungendo ad ognuno di questi sottoinsiemi l'elemento a_{k+1}. Quindi contiamo 2 volte i sottoinsiemi di A'.

Quindi quanti sono i sottoinsiemi di A? Sono tanti quanti quelli di A' contati due volte (una volta per contare quelli senza a_{k+1} e una volta per contare quelli con a_{k+1}).

Ora $|A'| = k$ quindi per il passo induttivo ($P(k)$ vera) sappiamo che $|\mathscr{P}(A')| = 2^k$ ma allora

$$|\mathscr{P}(A)| = 2|\mathscr{P}(A')| = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

ovvero P(k+1) è vera. Quindi abbiamo dimostrato che $\forall k \geq 0$ si ha che $P(k)$ vera $\implies$ $P(k+1)$ vera. Quindi il principio di induzione ci dice che $P(n)$ vera $\forall n \in \mathbb{N}$.

Osservazione 26. Daremo un altra dimostrazione di questo teorema usando tecniche diverse: Proposizione 8.

Esempio 93. (Gauss[8]) Dimostrare che $\forall n \in \mathbb{N}$ la somma dei numeri naturali minori o uguali a n è $\frac{n(n+1)}{2}$. Quindi:

$P(n)$: $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ per ogni $n \in \mathbb{N}$.

1) Base induzione: Dimostrare che $P(0)$ è vera.

P(0): La somma dei numeri naturali ≤ 0 (ovvero 0) è $\frac{0(0+1)}{2} = 0$, ovvero $0 = \frac{0(0+1)}{2} = 0$. Quindi $P(0)$ è vera.

2) Passo induttivo: Dimostrare che $\forall k \geq 0$, $P(k)$ vera implica $P(k+1)$ vera.

$P(k) : 0 + 1 + 2 + \ldots + k = \frac{k(k+1)}{2}$ è vera

[8]K.F. Gauss, 1777-1855, matematico tedesco.

Vogliamo dimostrare che
$P(k+1): 0+1+2+\ldots+k+(k+1)=\frac{(k+1)(k+1+1)}{2}$ sia vera
Allora

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

$$\frac{k(k+1)+2(k+1)}{2}=\frac{(k+2)(k+1)}{2}.$$

Ovvero $P(k+1)$ vera. Quindi abbiamo mostrato che $P(k)$ vera implica $P(k+1)$ vera. Quindi $P(n)$ è vera $\forall n \in \mathbb{N}$.

Quando si applica il principio di induzione si devono dimostrare due cose che $P(0)$ è vera e poi l'implicazione. Non si puo dire che $P(k)$ vera per ogni k dimostriamo $P(k+1)$. Si deve dire, che per ogni k, se $P(k)$ vera allora $P(k+1)$ è vera.

Prima di fare altri esempi, descriviamo due *generalizzazioni* del principio di induzione.
Vogliamo dimostrare che $P(n)$ è vera per ogni $n \in \mathbb{N}$ con $n \geq n_0$ per un certo fissato $n_0 \in \mathbb{N}$, prima $n_0 = 0$. Ovvero da n_0 in poi.

5.3. **Principio di Induzione Generalizzato (prima forma).** Enunciamo il Principio di Induzione Generalizzato (prima forma).
Base induzione: Dimostrare che $P(n_0)$ è vera.
Passo induttivo: Dimostrare che $\forall k \in \mathbb{N}$ con $k \geq n_0$ si ha che

$$P(k) \text{ vera } \implies P(k+1) \text{ vera}$$

Allora $P(n)$ è vera $\forall n \in \mathbb{N}$ con $n \geq n_0$

5.4. **Principio di Induzione Generalizzato (seconda forma).** Enunciamo il Principio di Induzione Generalizzato (seconda forma).
Base induzione: Dimostrare che $P(n_0)$ è vera.
Passo induttivo: Dimostrare che $\forall k \in \mathbb{N}$ con $k \geq n_0$ si ha che

$$P(n_0), P(n_0+1), , ..., P(k) \text{ vere } \implies P(k+1) \text{ vera.}$$

Allora $P(n)$ è vera $\forall n \in \mathbb{N}$ con $n \geq n_0$

Osservazione 27. Il passo induttivo in questa seconda forma si può esprimere nella forma equivalente:

Passo induttivo: Dimostrare che $\forall\ k \in \mathbb{N}$ si ha che

$$P(h) \text{ vera } \forall h \text{ tale che } n_0 \leq h \leq k \implies P(k+1) \text{ vera}$$

Facciamo esempi *sbagliati*: se non si applica il principio di induzione correttamente allora si possono concludere cose false.

Esempio 94. Ogni numero naturale è uguale al successivo (sappiamo gia che è sbagliata!!).
Vogliamo dimostrare che $\forall n \in \mathbb{N}$ la proposizione $P(n):\quad n = n+1$ è vera.
Passo induttivo: Dimostrare che $\forall k \geq 0$ se $P(k)$ vera allora $P(k+1)$ vera
$P(k):\quad k = k+1$ vera
vogliamo dimostrare che
$P(k+1):\quad k+1 = k+1+1$ sia vera.
$P(k)$ vera, quindi $k = k+1$ sommiamo 1 ad entrambi i membri dell'equazione e otteniamo $k+1 = k+1+1$. Ne segue che $P(k+1)$ vera.
Quindi abbiamo dimostrato l'implicazione, ovvero il passo induttivo.
Il problema è che $P(0)$ è falsa!! Ed è falsa per ogni base dell'induzione $n_0 \in \mathbb{N}$. Quindi è fondamentale fare entrambi i passi del principio di induzione.

Esempio 95. Tutti i gatti hanno lo stesso colore.

È come dire in ogni insieme di gatti tutti hanno lo stesso colore.

Vogliamo dimostrare che $\forall n \in \mathbb{N}^*$, in ogni insieme con n gatti questi hanno tutti lo stesso colore.

1) Base induzione: Mostriamo che $P(1)$ è vera.

$P(1)$: In un insieme di un gatto hanno tutti lo stesso colore.

Questo è vero, quindi $P(1)$ è vera.

2) Passo Induttivo: Mostriamo che $\forall k \geq 1$ $P(k)$ vera implica $P(k+1)$ vera

$P(k)$: In ogni insieme con k gatti questi hanno tutti lo stesso colore.

$P(k+1)$: In ogni insieme con $k+1$ gatti questi hanno tutti lo stesso colore.

Prendiamo un insieme con $k+1$ gatti, numeriamo i gatti da 1 a $k+1$. Per induzione quelli numerati da 1 a k hanno tutti lo stesso colore (sono un insieme con k gatti). Ad esempio hanno tutti lo stesso colore del gatto 2. Analogamente per i gatti numerati da 2 a $k+1$, questi sono k gatti e quindi hanno tutti lo stesso colore del gatto numero 2. Allora tutti i gatti hanno lo stesso colore..... eppure qualche dubbio rimane....

Esercizio 14. Dimostrare col principio di induzione che $\forall n \in \mathbb{N}$

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1.$$

Esercizio 15. Dimostrare col principio di induzione che $\forall n \in \mathbb{N}$

$$0 + 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Esercizio 16. Dimostrare col principio di induzione che $\forall n \in \mathbb{N}$

$$0 + 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Esercizio 17. Dimostrare col principio di induzione che per ogni fisato $q \in \mathbb{N} \setminus \{0, 1\}$ e $\forall n \in \mathbb{N}$ si ha

$$q^0 + q^1 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q}.$$

Check list. In questo capitolo abbiamo introdotto il Principio di Induzione matematico, strumento fondamentale.

6. Successioni

Dato un insieme, ci ricordiamo che non importa l'ordine in cui sono disposti gli elementi. Abbiamo visto $\{a, b, c, d\} = \{b, c, a, d\}$.

Ora siamo interessati a risolvere un altro problema: vogliamo disporre gli elementi ricordandoci l'ordine, (chi viene prima e chi viene dopo). Quindi etichettiamo gli oggetti con i numeri naturali e questa etichetta ci ricorda l'ordine-la posizione.

Definizione 35. (Successione) Una *successione* in un insieme A è una funzione f definita su un sottoinsieme dei numeri interi $\mathbb{Z}$ a valori in A, in genere $f : \mathbb{N} \to A$ oppure $f : \mathbb{N}^* \to A$. Per indicare l'immagine dell'elemento n, ovvero $f(n)$ si usa la notazione a_n, (l'etichetta n ci ricorda la posizione). Per indicare una successione si usa la notazione $\{a_n\}_{n\in\mathbb{N}}$ (oppure $\{a_n\}_{n\in\mathbb{N}^*}$) e a_n è detto il termine n-esimo della successione.

Osservazione 28. Notazione: $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Esempio 96. Consideriamo $A = \mathbb{N}$, $\mathbb{N} \subseteq \mathbb{Z}$ e la funzione $f : \mathbb{N} \to \mathbb{N}$ $f = Id_{\mathbb{N}}$, ovvero $\forall n \in \mathbb{N}$, $f(n) = n$. Quindi $a_n = f(n) = n$. In questo caso, $\{a_n\}_{n\in\mathbb{N}} = \{n\}_{n\in\mathbb{N}}$. Chi è il centesimo termine? $a_{100} = f(100) = 100$

Esempio 97. Consideriamo $A = \mathbb{Q}$, $\mathbb{N}^* \subseteq \mathbb{Z}$ e la funzione $f : \mathbb{N}^* \to \mathbb{Q}$ tale che $\forall n \in \mathbb{N}^* \quad f(n) = \frac{1}{3n}$. Quindi $\{a_n\}_{n\in\mathbb{N}^*} = \{\frac{1}{3n}\}_{n\in\mathbb{N}^*}$.

Chi è il centesimo termine? $a_{100} = f(100) = \frac{1}{300}$.

Esempio 98. Consideriamo $A = \mathbb{Q}$, $\mathbb{N} \subseteq \mathbb{Z}$ e la funzione $f : \mathbb{N} \to \mathbb{Q}$.

$$f(n) = \begin{cases} 0 & \text{se } n = 0, \\ \frac{1}{n} & \text{se } n \neq 0. \end{cases}$$

$a_0 = f(0) = 0$, quindi $\{a_n\}_{n\in\mathbb{N}} = \{0, 1, \frac{1}{2}, \dots\}$.

Chi è il centesimo termine? $a_{100} = f(100) = \frac{1}{100}$.

Esercizio 18. Data $f : \mathbb{N} \to \mathbb{R}$, tale che $f(n) = \sqrt{n}$, determinare a_4, a_5, a_{11}.

Esercizio 19. Data la successione

$$\{a_n\}_{n\in\mathbb{N}} = \{\frac{2}{3 + n^2}\}_{n\in\mathbb{N}},$$

calcolare i termini a_4, a_0, a_9.

Nota Bene 10. Notiamo che $\{a_n\}_{n\in\mathbb{N}} = \{a_j\}_{j\in\mathbb{N}}$.

Esempio 99. Esempio di successione: $\{a_n\}_{n\in\mathbb{N}} = \{2^n\}_{n\in\mathbb{N}}$. Ovvero $a_0 = 2^0 = 1$ $a_1 = 2^1$ $a_2 = 2^2$ $a_n = 2^n$ che possiamo vedere anche come $a_n = 2 \cdot 2^{n-1} = 2a_{n-1}$. Ogni volta moltiplichiamo per due. Quindi "sembrerebbe"uguale a

$$\begin{cases} a_0 = 2^0 = 1 \\ a_n = 2 \cdot a_{n-1}, n > 0. \end{cases}$$

Dopo dimostreremo cosa significa "sembrerebbe"uguale. Per ora vediamo che questa successione è definita in maniera diversa da quella di prima. Ora il termine $n + 1$ è espresso in funzione del precedente.

Esempio 100. Consideriamo $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = 1 \\ a_n = a_{n-1} + 3, n > 0. \end{cases}$$

Se chiediamo chi è il termine 1000, ovvero a_{1000}, dobbiamo calcolare tutti i termini prima per poterlo determinare.

Definizione 36. (RICORRENZA/RICORSIVA) Una successione si dice *definita per ricorrenza*, o per induzione, o successione ricorsiva se si definiscono i valori iniziali della successione per $n \leq n_0$ e si definisce una regola per determinare i valori della successione per ogni $n > n_0$ in funzione dei valori dei termini precedenti. Ovvero una successione ricorsiva esprime il termine n-esimo in funzione dei termini precedenti.

Osservazione 29. Molti algoritmi in informatica si basano sulla struttura ricorsiva.

Esempio 101. Consideriamo $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = 0 \\ a_n = a_{n-1} + n, n > 0. \end{cases}$$

Allora $a_1 = 1$ e a_4? $a_4 = a_3 + 4 = a_2 + 3 + 4 = a_1 + 2 + 3 + 4 = 1 + 2 + 3 + 4 = 10$.

Quindi a_0 è fissato ed abbiamo una legge per calcolare i termini in funzione del precedente.

Esempio 102. Progressione geometrica: x, d fisati in $\mathbb{R}^*$, definiamo $\{a_n\}_{n\in\mathbb{N}}$
$\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = x \\ a_n = da_{n-1}, n > 0. \end{cases}$$

Quindi $a_0 = x$, $a_1 = xd$, e sembrerebbe $a_n = xd^n$.

Esempio 103. Progressione aritmetica: siano x, d fissati in $\mathbb{R}$, definiamo $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = x \\ a_n = a_{n-1} + d, n > 0. \end{cases}$$

Quindi $a_0 = x$, $a_1 = x + d$, e sembrerebbe $a_n = x + nd$. Se $d = 0$ abbiamo successione costante.

Esempio 104. I numeri fattoriali: $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = 1 \\ a_n = n \cdot a_{n-1}, n > 0. \end{cases}$$

$a_0 = 1$, $a_1 = 1$, ...

Definizione 37. (FORMULA CHIUSA) La *formula chiusa* di una successione ricorsiva è una formula che esprime direttamente il termine n-simo a_n usando operazioni in funzione di n e non in funzione dei termini precedenti della successione.

Osservazione 30. Trovare la formula chiusa di una successione o algoritmo è un procedimento molto complicato: si usa l'analisi matematica, le funzioni generatrici e le equazioni differenziali. Quindi queste cose sono trattate nei corsi di analisi matematica, noi al più verifichiamo una formula chiusa.

Osservazione 31. Trovare una formula chiusa per un algoritmo è molto utile dal punto di vista informatico. Infatti è molto più veloce ed economico da un punto di vista computazionale calcolare un algoritmo con la formula chiusa piuttosto che usare la formula ricorsiva.

Esempio 105. Progressione geometrica: x, d fissati in $\mathbb{R}^*$ $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = x \\ a_n = da_{n-1}, n > 0. \end{cases}$$

Allora $a_0 = x$, $a_1 = xd$, ... Ogni volta moltiplichiamo per d. Consideriamo la successione $\{b_n\}_{n\in\mathbb{N}}$ con $b_n = xd^n$. Ci chiediamo è la formula chiusa? Ovvero le due

successioni coincidono? Ovvero $a_n = b_n$ per ogni $n \in \mathbb{N}$? Bisogna usare principio di induzione.

$P(n)$: $a_n = b_n$ e vogliamo dimostrare questa proposizione per ogni $n \in \mathbb{N}$.

BASE INDUZIONE. Dimostrare che P(0) è vera.

$P(0) : a_0 = b_0$. Vera in quanto $a_0 = x$ e $b_0 = xd^0 = x$.

PASSO INDUTTIVO: Dimostrare che $\forall k \geq 0$ se $P(k)$ vera allora $P(k+1)$ vera.

Assumiamo $P(k)$ vera, ovvero $a_k = b_k$ e dimostriamo $P(k+1) : \ a_{k+1} = b_{k+1}$ vera. abbiamo

$$a_{k+1} = da_k = db_k = d\, xd^k = xd^{k+1} = b_{k+1}$$

vero. Allora $a_n = b_n$ per ogni $n \in \mathbb{N}$.

Esempio 106. Progressione aritmetica: $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = x \\ a_n = a_{n-1} + d, n > 0. \end{cases}$$

$a_0 = x$, $a_1 = x+d$,.., consideriamo la successione $\{b_n\}_{n\in\mathbb{N}}$ con $b_n = x+nd$. Ci chiediamo è la formula chiusa? Ovvero le due successioni coincidono? Ovvero $a_n = b_n$ per ogni $n \in \mathbb{N}$? Bisogna usare principio di induzione.

Esempio 107. Consideriamo $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = 1 \\ a_n = n \cdot a_{n-1}, n > 0. \end{cases}$$

Introduciamo i *numeri fattoriali*:

$$0! = 1 \ e \ n! = n \cdot (n-1) \cdots 2 \cdot 1.$$

Consideriamo la successione $\{b_n\}_{n\in\mathbb{N}}$ con $b_n = n!$. Ci chiediamo è la formula chiusa? Ovvero le due successioni coincidono? Ovvero $a_n = b_n$ per ogni $n \in \mathbb{N}$? Bisogna usare principio di induzione.

Esercizio 20. Dimostrare che la successione $\{a_n\}_{n\in\mathbb{N}}$

$$\begin{cases} a_0 = 0 \\ a_n = a_{n-1} + n, n > 0. \end{cases}$$

ammette come formula chiusa $\{b_n\}_{n\in\mathbb{N}}$ con $b_n = \frac{n(n+1)}{2}$.

Esercizio 21. Dimostrare che la successione $\{a_n\}_{n\in\mathbb{N}}$:

$$\begin{cases} a_0 = 2^0 = 1 \\ a_n = 2 \cdot a_{n-1}, n > 0. \end{cases}$$

ammette come formula chiusa $\{b_n\}_{n\in\mathbb{N}} = \{2^n\}_{n\in\mathbb{N}}$.

6.1. **I numeri di Fibonacci.** I numeri di Fibonacci[9] sono definiti ricorsivamente: $\{f_n\}_{n\in\mathbb{N}}$

$$\begin{cases} f_0 = 0 \\ f_1 = 1 \\ f_n = f_{n-1} + f_{n-2}, n > 1. \end{cases}$$

Ogni termine della successione è somma dei due precedenti

f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	$\cdots$
0	1	1	2	3	5	8	13	$\cdots$

I numeri di Fibonacci sono molto studiati perché modellano la crescita di una popolazione di conigli. Infatti, supponiamo che:

(1) Una coppia di conigli diventa fertile/matura dopo un mese e genera un'altra coppia dopo un altro mese.

(2) Al mese zero non abbiamo conigli e al primo mese abbiamo una coppia non matura.

(3) I conigli non muoiono mai.

Quante coppie di conigli abbiamo al mese n?
mese $0 = 0$
mese $1 = 1$, mese 2=1 (fertile), mese 3=2 coppie (una nuova e una vecchia=fertile) mese 4= 3 coppie (una nuova e due vecchie= fertili) quindi tante fertili quanto quelle del passo prima e tante nuove quante quelle di due passi prima che sono fertili dopo un mese e generano una coppia dopo un altro mese.

Quindi al mese n abbiamo tante coppie quante erano al mese $n-1$ (non muoiono) e in piu le nuove coppie che sono tante quante le coppie mature al mese $n-1$ ovvero tante quante le coppie al mese $n-2$. Quindi $f_n = f_{n-1} + f_{n-2}$.

Quale è la formula chiusa?

Proposizione 3. *La successione dei numeri di Fibonacci* $\{f_n\}_{n\in\mathbb{N}}$

$$\begin{cases} f_0 = 0 \\ f_1 = 1 \\ f_n = f_{n-1} + f_{n-2}, n > 1, \end{cases}$$

ammette come formula chiusa la successione $\{b_n\}_n$ *con*

$$b_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \qquad \forall\ n \geq 0.$$

Il valore $\frac{1+\sqrt{5}}{2}$ si indica con Φ e si chiama rapporto aureo (Fidia). È sorprendente che nella formula di b_n compaiono potenze di numeri irrazionali, ma b_n è un numero naturale. La matematica non smette mai di stupirci.

Per i più curiosi:

Dimostrazione. (Non inclusa nel Programma)
Dobbiamo dimostrare chela proposizione $P(n)$: $f_n = b_n$ è vera per ogni n in $\mathbb{N}$.
SKETCH: Principio di induzione, seconda forma, dato che f_n non dipende solo da f_{n-1}.
Verifichiamo che $P(0)$ e $P(1)$ sono vere
$a_0 = 0$
$b_0 = \frac{1}{\sqrt{5}}(1-1) = 0$
per $n = 1$
$a_1 = 1$

[9]Leonardo Fibonacci, matematico Italiano di Pisa, circa 1175-1235.

$b_1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \frac{1}{\sqrt{5}}\left(2\frac{\sqrt{5}}{2}\right) = 1$

Passo Induttivo: dimostriamo che $\forall k \in \mathbb{N}$, la proposizione $P(h)$ vera per ogni $0 \leq h \leq k$ implica $P(k+1)$ vera:

$$a_{k+1} = a_k + a_{k-1} = b_k + b_{k-1} =$$

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right] + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] =$$

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] =$$

$$\frac{1}{\sqrt{5}}\left[\left(1+\frac{1+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(1+\frac{1-\sqrt{5}}{2}\right)\right] =$$

$$\frac{1}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{3-\sqrt{5}}{2}\right)\right] =$$

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right] =$$

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right].$$

Infatti

$$\left(\frac{1 \pm \sqrt{5}}{2}\right)^2 = \frac{1+5 \pm 2\sqrt{5}}{4} = \left(\frac{3 \pm \sqrt{5}}{2}\right).$$

6.2. **Le Torri di Hanoi.** Il gioco delle Torre di Hanoi è stato pubblicato da E. Lucas[10] e consiste nel seguente problema. Supponiamo di avere tre aste (A,B,C) e su una di esse (A) siano posti n-dischi di diametro decrescente dal basso verso l'alto (tipo piramide).

Scopo del gioco: trasferire i dischi su un'altra asta in modo che formino la stessa piramide.

Regole:

1) I dischi vanno spostati uno alla volta.

2) Non può mai accadere che un disco di diametro maggiore sia poggiato su un disco di diamentro inferiore.

Quale è il numero minimo delle mosse con n dischi per raggiungere lo scopo del gioco?

Se $n = 0$, allora 0 mosse; se $n = 1$ allora 1 mossa, dobbiamo spostare un solo disco. Se $n = 2$ allora 3 mosse: spostiamo il disco piccolo su un asta vuota, poi spostiamo il disco grande su l'altra asta libera, e infine mettiamo il disco piccolo sul disco grande.

Indichiamo con $a_n =$ numero delle mosse. Allora

$$\{a_n\}_n = \begin{cases} a_0 = & 0 \\ a_n = & 2a_{n-1} + 1 \quad n \geq 1. \end{cases}$$

Infatti, consideriamo $n-1$ dischi, allora servono a_{n-1} mosse per spostarle su un'altra asta. Poi spostiamo il disco n-esimo (il più grande) e poi rispostiamo sopra gli $n-1$ dischi con altre a_{n-1} mosse. Quindi servono $a_{n-1} + 1 + a_{n-1} = 2a_{n-1} + 1$ mosse.

Proposizione 4. *Verificare che la seguente successione $\{a_n\}_n$ definita per ricorrenza*

$$\{a_n\}_n = \begin{cases} a_0 = & 0 \\ a_n = & 2a_{n-1} + 1 \quad n \geq 1. \end{cases}$$

ammette come formula chiusa la successione $\{b_n\}_n$ con $b_n = 2^n - 1$.

[10] Édouard Lucas, matematico Francese 1841-1891; gioco pubblicato nel 1883.

Dimostrazione. Dobbiamo dimostrare che $P(n)$: $a_n = b_n$ è vera per ogni n in $\mathbb{N}$.

Usiamo il Principio di induzione. Pirma cosa il passo base. Poi bisogna verificare il passo induttivo e concludere.

$P(n)$: $a_n = b_n$ e vogliamo dimostrare questa proposizione per ogni $n \in \mathbb{N}$.

BASE INDUZIONE. Dimostrare che $P(0)$ è vera.

$P(0) : a_0 = b_0$. Vera in quanto $a_0 = 0 = b_0$.

PASSO INDUTTIVO: Dimostrare che $\forall k \in \mathbb{N}$, $P(k)$ vera implica $P(k+1)$ vera.

Abbiamo:

$P(k) :$ $a_k = b_k$ (supponiamo vera)

$P(k+1) :$ $a_{k+1} = b_{k+1}$ (da dimostrare vera).

Allora

$$a_{k+1} = 2a_k + 1 = 2b_k + 1 = 2 \cdot (2^k - 1) + 1 = 2^{k+1} - 2 + 1 = 2^{k+1} - 1 = b_{k+1}$$

vero. Quindi $P(k+1)$ è vera e il principio di induzione implica che $P(n)$ è vera per ogni n in $\mathbb{N}$, ovvero $a_n = b_n$ per ogni $n \in \mathbb{N}$.

6.3. **Simbolo di Sommatoria.** Sia $\{a_n\}_n$ una successione. Introduciamo il simbolo di sommatoria: $\sum$.

$$\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + \cdots + a_n$$

dove $i = indice$. Questo simbolo indica solo la somma dei termini della successione a_i dall'indice $i = 0$ (partiamo da $i = 0$) fino ad $i = n$ (finiamo ad n). Oovvero dobbiamo fare la somma di questi termini. Il *simbolo* non ci dice quanto fa la somma!

Osservazione 32. Noi abbiamo dimostrato nell'Esempio 93 che

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

il simbolo in se non dice il risultato della somma.

Esempio 108. Altri esempi:

$$\sum_{i=0}^{3} 2i = 2 \cdot 0 + 2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3;$$

$$\sum_{i=-1}^{n+1} i^2 = (-1)^2 + 0 + 1^2 + 2^2 + 3^2 + \cdots + n^2 + (n+1)^2.$$

In generale,

$$\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + \cdots + a_n,$$

è la somma dei primi $n+1$ termini della successione $\{a_n\}_{n \in \mathbb{N}}$.

Proprietà della sommatoria.

(1) $\sum_{i=0}^{n} a_i = \sum_{j=0}^{n} a_j$ indice i o j è la stessa cosa;

(2) $\sum_{i=0}^{n} a_i = \sum_{0 \le i \le n} a_i$ altra notazione;

(3) Per ogni $q \in \mathbb{R}$, $\sum_{i=0}^{n} q = q + q + \cdots + q = (n+1) \cdot q$ sommiamo lo stesso numero q, $n+1$ volte.

(4) Per ogni $q \in \mathbb{R}$, $\sum_{i=0}^{n} q \cdot a_i = q \sum_{i=0}^{n} a_i$;

(5) $\sum_{i=0}^{n} (a_i + b_i) = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i$. (Associatività e Commutativita della somma)

(6) $\sum_{i=0}^{n} a_i = \sum_{i=0}^{t} a_i + \sum_{i=t+1}^{n} a_i$.

Esempio 109. (IMPORTANTE) Un'esempio dell'ultima proprietà che useremo frequentemente:

$$\sum_{i=0}^{k+1} a_i = \sum_{i=0}^{k} a_i + a_{k+1}.$$

Osservazione 33. Nel corso di analisi verranno studiate le successioni e le serie numeriche, che non sono altro che sommatorie con un numero infinito di termini, sarete interessati a capire la convergenza della serie.

Check list. In questo capitolo abbiamo definito le successioni, successioni definite per ricorrenza e formula chiusa, numeri di Fibonacci, Torre di Hanoi e introdotto il simbolo di sommatoria.

7. Combinatoria

La Repubblica riconosce a tutti i cittadini il diritto al lavoro e promuove le condizioni che rendano effettivo questo diritto. (I parte)

Siano A e B insiemi finiti. Abbiamo definito le cardinalità $|A|$ e $|B|$ (degli insiemi A e B). Adesso vogliamo determinare la cardinalità di $|A \cup B|$ o più in generale dell'unione di insiemi e del prodotto.

Esempio 110. A= insieme di 8 auto. B=insieme di 5 biciclette. Allora $|A| = 8$ $|B| = 5$ ed $A \cup B$ è un insieme con 8 auto e 5 biciclette. Quindi $|A \cup B| = 8 + 5 = 13$.

Esempio 111. Ci sono 8 penne blu e 5 penne bic. Se definiamo A= insieme di 8 penne blu e B=insieme di 5 penne bic. Allora $|A| = 8$ $|B| = 5$. $A \cup B$ è l'unione dei due insiemi, ma non è detto che $|A \cup B|$ sia 13, perché alcune penne bic potrebbero essere blu.

Ricordiamo la definizione di insiemi disgiunti (Definizione 6): due insiemi A e B si dicono disgiunti se $A \cap B = \emptyset$.

7.1. Regola della Somma.

Proposizione 5. *Se A e B sono insiemi finiti disgiunti, allora*

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

Quindi se $|A| = n$ e $|B| = t$ allora $|A \cup B| = |A| + |B| = n + t$.

In generale dati m-insiemi $A_1, A_2, \ldots, A_m$ a due a due disgiunti, ovvero $A_i \cap A_j = \emptyset$ $\forall i \neq j$. Se $|A_i| = n_i$, allora $|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots |A_m| = n_1 + n_2 + \cdots + n_m = \sum_{i=1}^{m} n_i$.

Quindi, se $A_1, A_2, \ldots, A_m$ sono insiemi a due a due disgiunti, con $|A_i| = n_i$. In quanti modi distinti possiamo scegliere un elemento? Ovviamente in $n_1 + n_2 + \cdots + n_m$ modi.

Esempio 112. In una classe, ci sono 6 Iphone, 11 Nokia e 8 Samsung. Quanti sono in tutto i cellulari?

Esempio 113. Abbiamo 3 penne blu, 3 gialle, 4 rosse, 5 verdi. Ogni penna ha solo una colorazione e quindi abbiamo in tutto 15 scelte di penne.

7.2. Principio di inclusione-esclusione.

In generale, dati due insiemi, la cardinalità di $|A \cup B|$ è data dal seguente risultato.

Proposizione 6. *Se A e B sono insiemi finiti, allora*

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

Dimostrazione. Dobbiamo sottrarre gli elementi che contiamo due volte, ovvero gli elementi contenuti nell'intersezione.

Fare diagramma di Venn.

Esempio 114. Abbiamo delle penne, Sia A= insieme di 8 penne blu. B=insieme di 5 penne bic e ci sono 3 bic blu Allora $|A| = 8$ $|B| = 5$, $|A \cap B| = 3$. Allora $|A \cup B| = |A| + |B| - |A \cap B| = 8 + 5 - 3 = 10$.

Esempio 115. In una autosalone ci sono 13 BMW e 14 auto grigie e 4 sono BMW grigie. Quante sono in tutto le auto BMW o grigie? Allora $|A| = 13$ $|B| = 14$, $|A \cap B| = 4$. Allora $|A \cup B| = |A| + |B| - |A \cap B| = 27 - 4 = 23$.

Esempio 116. Consideriamo i seguenti insiemi:
$A = \{x \in \mathbb{N} \,|\, x \text{ è pari e } 3 \leq x < 31\}$
$B = \{x \in \mathbb{N} \,|\, 0 \leq x \leq 65 \text{ e x multiplo di 6 }\}$
Determinare $|A \cup B|$.
$A = \{4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$
$B = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60\}$
Allora $|A| = 14$ $|B| = 11$, $|A \cap B| = |\{6, 12, 18, 24, 30\}| = 5$. Allora $|A \cup B| = |A| + |B| - |A \cap B| = 14 + 11 - 5 = 20$. Scrivere esplicitamente $A \cup B$.

Esempio 117. In una classe ci sono 90 studenti, 35 sono donne, 20 hanno l'Iphone, 15 donne hanno l'Iphone.
Quanti sono gli studenti maschi e senza Iphone?
E quanti maschi con l' Iphone? Quanti sono gli studenti o maschi o con Iphone?
Sketch: $90 - 35 = 55$ studenti maschi;
Maschi con Iphone: 20-15=5;
Quindi maschi senza iphone 55-5=50.
Gli studenti o Maschi o con Iphone: $|M \cup I| = |M| + |I| - |M \cap I| = 55 + 20 - 5 = 70$.

Questo vale per l'unione due insiemi. E se vogliamo studiare casi più generali? Ad esempio $|A \cup B \cup C|$? In tal caso basta generalizzare la Proposizione 6.

Proposizione 7. *Siano A, B, C insiemi finiti. Allora*

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

Dimostrazione. Idea della dimostrazione con i diagrammi di Venn. In $|A| + |B| + |C|$ stiamo contando due volte $|A \cap B|$ e $|C \cap B|$ e $|A \cap C|$ quindi li togliamo; in questo modo, togliamo 3 volte gli elementi in $A \cap B \cap C$ e quindi dobbiamo riaggiungerli ovvero dobbiamo sommare $|A \cap B \cap C|$.

Dimostriamo, usando il caso a due insiemi studiato nella Proposizione 6 e la proprietà distributiva della Proposizione 1:

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

Esercizio 22. Consideriamo i seguenti insiemi:
$A = \{x \in \mathbb{N} \,|\, x \text{ è pari e } 3 \leq x < 31\}$
$B = \{x \in \mathbb{N} \,|\, 0 \leq x \leq 65 \text{ e } x \text{ multiplo di } 6\}$
$C = \{x \in \mathbb{N} \,|\, 0 \leq x \leq 50 \text{ e } x \text{ multiplo di } 4\}$.
Determinare $|\, A \cup B \cup C \,|$.

Esempio 118. In una classe ci sono 76 studenti o di Bari o di Brindisi, 35 sono di Brindisi, 20 hanno occhi chiari, 25 sono di Brindisi e hanno occhi scuri.

Supponendo che gli occhi possono essere o chiari o scuri: Quanti sono gli studenti di Bari? Quanti sono gli studenti di Bari con occhi chiari? Quanti gli studenti di Bari con occhi scuri? Quanti sono studenti di Brindisi con occhi chiari?

Sketch: In tutto ci sono 76 studenti.
$76 - 35 = 41$ studenti di Bari ($|A \cup B| = |A| + |B|$);
$76 - 20 = 56$ studenti con occhi scuri ($|A \cup B| = |A| + |B|$);
$56 - 25 = 31$ studenti di Bari con occhi scuri;
$41 - 31 = 10$ studenti di Bari con occhi chiari;
$35 - 25 = 10$ studenti di Brindisi con occhi chiari.

7.3. **Regola del Prodotto.** Supponiamo ora che A e B siano due insiemi finiti con $|A| = n$ e $|B| = m$. Abbiamo definito il prodotto cartesiano $A \times B$. Ci chiediamo quale è la cardinalità di $|A \times B|$.

Ricordiamo che

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

Un elemento $a \in A$ può essere scelto in n modi, un elemento $b \in B$ può essere scelto in m modi distinti. Quindi possiamo fare $n \cdot m$ scelte: possiamo scegliere $a \in A$ in n modi e per ognuna di queste scelte possiamo scegliere un elemento $b \in B$ in m modi. Ovvero $|A \times B| = nm$.

Esempio 119. Sia $A = \{l, m\}$ e $B = \{a, b, c\}$.

$$A \times B = \{(l, a), (l, b), (l, c), (m, a), (m, b), (m, c)\}$$

Allora $|A \times B| = 6$.

Esercizio 23. Sia $A = \{1, 3, 5, 6, 7\}$ e $B = \{2, 3, x, y\}$. Allora $|A \times B| = 5 \cdot 4 = 20$.

Anche se abbiamo più insiemi basta moltiplicare le loro cardinalità. A, B e C siano insiemi finiti con $|A| = n$, $|B| = m$ e $|C| = t$. Allora $|A \times B \times C| = nmt$.

Esercizio 24. Abbiamo 5 modelli di cellulare 4s, 5c ,5s ,6, 6plus e abbiamo disponibili 4 colori per ogni modello.

Quante scelte di cellulari diversi abbiamo? (Risposta 20).

Esercizio 25. Abbiamo 5 modelli di cellulare 4s, 5c, 5s , 6, 6plus. Abbiamo disponibili 4 colori per ogni modello. Inoltre possiamo scegliere, le versioni 8gb, 16gb, 32gb, 64gb.

Quanti scelte di cellulari diversi abbiamo?

Check list. In questo capitolo abbiamo studiato la cardinalità dell'unione di insiemi disgiunti o non disgiunti, Regola della somma, Principio di Inclusione-Esclusione, Regola del prodotto.

8. Combinazioni e disposizioni

Ogni cittadino ha il dovere di svolgere, secondo le proprie possibilità e la propria scelta, un'attività o una funzione che concorra al progresso materiale o spirituale della società. (II parte)

Nella sezione precedente ci siamo interessati a quanti modi abbiamo per scegliere un elemento con la regola della somma (scegliere un elemento in una unione di insiemi) e con la regola del prodotto (scegliere un elemento nel prodotto cartesiano di insiemi). In questa sezione invece abbiamo un insieme non vuoto e vogliamo scegliere più di un elemento. Inoltre volgiamo determinare il numero delle funzioni iniettive tra due insiemi e il numero delle funzioni biettive.

Sia A un insieme finito non vuoto con n elementi: $\mid A \mid = n$.

Obiettivo: Studiare come si possono scegliere k elementi in un insieme con n elementi.

Sicuramente dobbiamo fare delle distinzioni:

Caso 1) scegliere k elementi senza ripetizioni (2 sottocasi: se l'ordine è importante o no);

Caso 2) scegliere k elementi con ripetizioni (2 sottocasi: se l'ordine è importante o no).

8.1. **Caso 1) scegliere k elementi distinti.** In quanti modi possiamo scegliere k elementi distinti, ovvero senza ripetizioni, in un insieme di ordine n?

Importante: Sicuramente $k \leq n$, non possiamo scegliere più elementi distinti, di quanti ne possiede l'insieme.

Esistono due sottocasi:

i) Scegliere k elementi distinti ordine è importante (k-pla ordinata) "disposizione semplice di n oggetti di classe k".

ii) Scegliere k elementi distinti ordine non è importante (k sottoinsiemi) "combinazione semplice di n oggetti di classe k".

La parola semplice è usata per ricordarci senza ripetizioni, nella Sezione 8.3 vedremo il Caso 2) con ripetizioni.

8.1.1. *Caso 1) i): Disposizioni semplici di n oggetti di classe k.* In un insieme con n elementi, quanti sono i modi distinti per scegliere k elementi distinti ricordandoci l'ordine? Questo numero si indica con $D(n,k)$ e si ha

$$\begin{aligned} D(n,k) &= n \cdot (n-1) \cdot \ \cdots \ \cdot (n-(k-1)) \\ &= n \cdot (n-1) \cdot \ \cdots \ \cdot (n-k+1) \end{aligned}$$

Perchè?

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & \cdots & k \\ n & n-1 & n-2 & n-3 & n-4 & \cdots & n-(k-1). \end{array}$$

Si può scegliere il primo elemento in n modi, il secondo in $n-1$ modi (perché deve essere diverso dal primo), il terzo in $n-2$ modi (perché deve essere diverso dal primo e dal secondo già scelti) e così via. Osserviamo che $n-(k-1) = n-k+1$.

Esempio 120. Se $k = 4$. $D(n,k) = D(n,4) = n \cdot (n-1) \cdot (n-2) \cdot (n-3)$.

Esempio 121. Se $n = 6$ $k = 3$. $D(6,3) = 6 \cdot 5 \cdot 4$.

Esempio 122. Supponiamo $A = \{x, y, z\}$ allora $n = 3$, e sia $k = 2$. Allora $D(n, k) = D(3, 2) = 3(3 - (2 - 1)) = 3(3 - 1) = 3 \cdot 2 = 6$. Quindi ci sono 6 modi distinti per scegliere 2 elementi distinti ricordandoci l'ordine: il primo può essere scelto il 3 modi, il seondo elemento in 2 modi. Infatti, abbiamo xy, yx, xz, zx, yz, zy.

Esempio 123. Ci sono 50 autovetture in una gara. In quanti modi diversi possiamo assegnare il 1° premio, il 2° premio e il 3° premio (senza parimerito)? Ovviamente l'ordine è importante! In questo caso $n = 50$ e $k = 3$. $D(n, k) = D(50, 3) = 50(50 - 1)(50-2) = 50 \cdot 49 \cdot 48$. Il primo premio può essere assegnato ad una tra le 50 autovetture, il secondo ad una tra le 49 autovetture (tutte tranne quella che ha ricevuto il 1° premio) e il terzo ad una tra le 48 autovetture (tutte tranne le due che hanno ricevuto il 1° e 2° premio).

Osservazione 34. $D(n, 1) = n$: indica in quanti modi distinti possiamo scegliere un elemento in un insieme con n elementi. Infatti, in un insieme con n elementi ne possiamo scegliere uno in n modi distinti.

Osservazione 35. Osserviamo che $D(n, n) = n \cdot (n - 1) \cdot (n - 2) \cdots (n - (n - 1)) = n \cdot (n - 1) \cdot (n - 2) \cdots 1 = n!$

Ovvero in un insieme di n elementi possiamo scegliere $n!$ disposizioni semplici. Ovvero dati n elementi possiamo ordinarli in $n!$ modi distinti. Un ordinamento di n oggetti è detto *permutazione*. Quando introdurremo le strutture algebriche, studieremo il gruppo delle permutazioni su n elementi, che è un gruppo finito di cardinalità $n!$ (Sezione 15).

Osservazione 36. Notare che $D(n, k) = \frac{n!}{(n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-(k-1)) \cdot (n-k)!}{(n-k)!}$

Osservazione 37. Notiamo che $D(n, k) =$ *numero delle funzioni iniettive* da un insieme finito A con $|A| = k$ ad un insieme finito B con $|B| = n$ (ricordiamo $k \leq n$: Definizione 32). Infatti, se $A = \{a_1, a_2, \ldots, a_k\}$ immagine di a_1 può essere scelta in n modi, quella di a_2 in $n - 1$ modi etc.

(L'ordine è importante per definire una funzione).

Osservazione 38. $D(n, n) = n!=$ *numero delle funzioni biettive* da un insieme A ad un insieme B con $|A| = |B| = n$. Infatti, $n!$ è il numero delle funzioni iniettive ma abbiamo visto che sono anche suriettive, avendo gli insiemi la stessa cardinalità (Teorema **??**). Analogamente si può dimostrare considerando che l' immagine di a_1 la possiamo scegliere in n modi, l'immagine di a_2 in $n-1$ modi, ..., l'immagine di a_n in un unico modo. Quindi in tutto ci sono $n!$ funzioni biettive.

8.1.2. *Caso 1) ii): Combinazioni semplici di n oggetti di classe k.* Scegliere k elementi distinti in un insieme con n elementi e l'ordine non è importante. Ricordiamoci sempre che $k \leq n$. Il numero di combinazioni semplici di n oggetti di classe k è il numero dei sottoinsiemi con k elementi in un insieme di cardinalità n. Si indica con $\binom{n}{k}$ e si ha

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

Questo numero si chiama *coefficiente binomiale*. Non è altro che il numero delle k-ple ordinate $D(n, k)$ diviso numero di modi di ordinare le k-ple, che è $k!$ come visto nell'Osservazione 35. Analogamente, possiamo anche ragionare considerando

$$\binom{n}{k} k! = D(n, k),$$

infatti $\binom{n}{k}$ indica il numero di sottoinsiemi con k elementi e lo moltiplichiamo per $k!$ che è il numero degli ordinamenti possibili di k elementi (Osservazione 35).

Esempio 124. Calcolare $\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4 \cdot 3!}{3!2!} = 10$.

Esempio 125. Supponiamo $A = \{x, y, z\}$. Quanti sono i stottoinsiemi con 2 elementi? $\{x, y\}$, $\{x, z\}$,$\{y, z\}$ sono 3 infatti $\binom{3}{2} = \frac{3!}{2!(3-1)!} = 3$. Infatti per l'Esempio 122, abbiamo xy, yx, xz, zx, yz, zy e poi dividiamo per 2.

Esercizio 26. Abbiamo 50 vetture in gara, in quanti modi possiamo scegliere 3 vetture da premiare? Adesso non vogliamo distinguere tra 1°, 2° e 3°, ma solo dare uno stesso premio. Allora dobbiamo scegliere 3 vetture tra 50 ovvero

$$\binom{50}{3} = \frac{50!}{3!(50-3)!} = \frac{50 \cdot 49 \cdot 48 \cdot 47!}{3!47!} = \frac{50 \cdot 49 \cdot 48}{3!} = 50 \cdot 49 \cdot 8.$$

Proprietà di $\binom{n}{k}$ con $k \leq n$.

(1) $\binom{n}{0} = \frac{n!}{0!n!} = 1$, unico modo per non scegliere nulla;

(2) $\binom{n}{1} = \frac{n!}{1!(n-1)!} = n$, ovvero n modi per scegliere 1 elemento $(= D(n, 1))$;

(3) $\binom{n}{n} = \frac{n!}{n!(n-n)!} = 1$, ovvero unico modo per scegliere tutto;

(4) $\binom{n}{k} = \binom{n}{n-k}$ infatti $\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!}$ uno è scegliere k elementi tra n, l'altro scegliere $n-k$ elementi tra n.

(5) Per ogni $1 \leq k \leq n$, si ha $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Osservazione 39. La Proprietà (4) dipende dal fatto che scegliendo un sottoinsieme di k elementi in un insieme con n elementi, univocamente è determinato il suo compelmentare, ovvero un sottoinsieme con $n-k$ elementi. Quindi possiamo scegliere tanti sottoinsiemi di cardinalità k tante quante sono le scelte per i complementari, ovvero tanti quanti sono i sottoinsiemi di cardinalità $n-k$.

Esercizio 27. Dimostrare che $\forall k$, tale che $1 \leq k \leq n$, si ha $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

A cosa possono servire i coefficienti binomiali? Perché si chiamano coefficienti binomiali?

I coefficienti binomiali sono i coefficienti della formula dello sviluppo delle potenze di un binomio.

8.2. **Formula di Newton.** Per ogni $n \geq 0$ si ha che

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Per i più curiosi:

Dimostrazione. (Non inclusa nel Programma) Perché è vero?

Ricordiamo che $(x+y)^n = (x+y) \cdots (x+y)$ moltiplicato n volte. Ogni termine è prodotto di n fattori scelti tra x e y. Se scegliamo x allora non scegliamo y, quindi se x compare k volte, allora y compare $n-k$ volte.

Quindi quale è il coefficiente di $x^k y^{n-k}$? Basta scegliere k volte la x (poi la y sarà per forza scelta $n-k$ volte).

Quindi quanti sono i possibili modi di scegliere la x, quando non importa l'ordine? Esattamente il numero di modi di scegliere k elementi tra n, ovvero $\binom{n}{k}$.

Si può fornire una dimostrazione alternativa, usando il principio di induzione, ovvero voler dimostrare per ogni $n \in \mathbb{N}$ la proposizione:

$$P(n): \quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Triangolo di Tartaglia. Nel Triangolo di Tartaglia organizziamo i coefficienti binomiali per ottenere i coefficienti delle potenze di un binomio usando la formula di Newton. Usando la Proprietà (5) ogni coefficiente è somma di quello sopra e quello a sinistra.

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$
$n=0$	1				
$n=1$	1	1			
$n=2$	1	2	1		
$n=3$	1	3	3	1	
$n=4$	1	4	6	4	1
$n=5$	$\cdots$	$\cdots$			

Usiamo i coefficienti binomiali per dare una seconda dimostrazione della cardinalità dell'insieme delle parti di un insieme finito.

Proposizione 8. *Sia A un insieme finito con $|A| = n$, allora $|\mathscr{P}(A)| = 2^n$.*

Dimostrazione. (Seconda dimostrazione). Per definizione $\mathscr{P}(A)$ è l'insieme dei sottoinsiemi di A. Se $|A| = n$, allora ogni sottoinsieme di A può avere cardinalità $0, 1, 2 \cdots, n$. Per ogni $k \leq n$, esistono esattamente $\binom{n}{k}$ sottoinsiemi di cardinalità k. Infatti il numero $\binom{n}{k}$ è il numero dei sottoinsiemi di cardinalità k in un insieme con n elementi. Sommando tutti i coefficienti binomiali da $k = 0$ fino ad n, otteniamo il numero dei sottoinsiemi di A. Quindi

$$|\mathscr{P}(A)| = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n.$$

8.3. **Caso 2) Scegliere k elementi con ripetizione in un insieme con n elementi.** Sia A un insieme finito con n elementi.

Obiettivo: Studiare come si possono scegliere k elementi.

Nella Sezione 8.1 abbiamo analizzato la scelta di k elementi distinti, ovvero senza ripetizioni, in un insieme di ordine n. Assunzione fondamentale: $k \leq n$.

Ora siamo interessati al Caso 2) Scegliere k elementi anche con ripetizione in un insieme finito di ordine n.

Osservazione 40. Non serve più l'ipotesi $k \leq n$. Poiché possiamo avere ripetizioni, quindi possiamo anche scegliere sempre uno stesso elemento e quindi k può anche essere maggiore di n.

Vogliamo rispondere alla domanda:

Caso 2): In quanti modi possiamo scegliere k elementi (anche con ripetizione) in un insieme di ordine n?

Anche in questo Caso 2) esistono due sottocasi:

a) Scegliere k elementi con ripetizione ordine è importante: "disposizione con ripetizione di n oggetti di classe k".

b) Scegliere k elementi con ripetizione ordine non è importante: "combinazione con ripetizione di n oggetti di classe k".

8.3.1. *Caso 2) a): Disposizioni con ripetizioni di n oggetti di classe k.* In un insieme con n elementi, quanti sono i modi distinti per scegliere k elementi ricordandoci l'ordine? Possiamo scegliere il primo elemento in n modi, anche per il secondo abbiamo n scelte (non richiediamo più che sia diverso dal primo elemento scelto), anche per il terzo abbiamo n scelte e cosi via. Quindi abbiamo

$$n \cdot n \cdots n = n^k.$$

Esercizio 28. Quante targhe esistono della forma

$$LL\ NNN\ LL$$

dove $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e L appartiene all'alfabeto inglese senza I e O? $24 \cdot 24 \cdot 9 \cdot 9 \cdot 9 \cdot 24 \cdot 24 = 24^4 \cdot 9^3$.

Infatti, dobbiamo scegliere con ripetizione $k = 4$ lettere tra le $n = 24$ e $k = 3$ numeri tra le $n = 9$ cifre.

Quante senza lettera straniere? al posto di 24 mettiamo 24-5=19.

Quante con almeno una lettera straniera? Sono tutte tranne quelle senza lettera straniera.

Esempio 126. Quanti numeri naturali di 7 cifre hanno almeno una cifra pari? Quanti almeno una cifra dispari?

$$_\ _\ _\ _\ _\ _\ _$$

Non si parte da zero. Contiamo quelli che non hanno alcuna cifra pari: quindi solo dispari 1,3,5,7,9 sono 5 cifre, quindi quelle con tutte cifre dispari sono 5^7. Quanti sono i numeri in tutto? La prima cifra si può scegliere in 9 modi le altre in 10, ovvero $9 \cdot 10^6$. Quindi $9 \cdot 10^6 - 5^7$ sono i numeri naturali con almeno una cifra pari.

Quanti sono quelle con tutte cifre pari? Sono $4 * 5^6$.

Quindi $9 \cdot 10^6 - 4 \cdot 5^6$ sono i numeri naturali con almeno una cifra dispari.

Osservazione 41. Il numero n^k è il numero delle funzioni $f : A \to B$ da un insieme A ad un insieme B, dove $|A| = k$ e $|B| = n$.

Infatti per il primo elemento abbiamo n scelte possibili per fissare l'immagine in B, dato che $|B| = n$. Per il secondo anche n scelte (non richiediamo l'iniettività) e cosi via per tutti i k elementi di A. Ovvero, in tutto abbiamo n^k scelte.

Esercizio 29. Calcolare il numero delle funzioni tra $A = \{x, y\}$ e $B = \{1, 2, 3\}$.

Dobbiamo scegliere le immagini degli elementi x e y. Per ognuno abbiamo 3 scelte quindi, $3^2 = 9$.

Quante sono suriettive? (Nessuna).

Quante iniettive? $D(n, k) = D(3, 2) = 6$.

Esercizio 30. Calcolare il numero delle funzioni da $A = \{1, 2, 3\}$ a $B = \{x, y\}$, e scriverle esplicitamente.

Osservazione 42. Possiamo chiederci a cosa serve questo numero e se ha applicazioni nel campo dell'Informatica. Un esempio semplicissimo ci fa vedere che lo usiamo quotidianamente. Infatti, supponiamo che abbiamo un cellulare con un pin numerico di 4 cifre. Quanti sono i pin possibili? Ogni cifra può essere scelta tra 0 e 9 e quindi abbiamo 10 scelte. Quindi in tutto abbiamo $10 \cdot 10 \cdot 10 \cdot 10 = 10^4$ pin possibili. (Chiaramente l'ordine è importante).

8.3.2. *Caso 2) b): Combinazioni con ripetizioni di n oggetti di classe k.* In quanti modi si possono scegliere k elementi in un insieme con n oggetti, ammettendo anche ripetizioni e ordine non importante? In tal caso, abbiamo

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

In questo caso l'ordine non è importante quindi consideriamo uguali, le k-ple con gli stessi elementi anche in ordine diverso.

Esempio 127. Calcolare il numero di combinazioni con ripetizione (no ordine) di lunghezza 6 in $A = \{1, 2, 3, 4, 5\}$ $n = 5$ e $k = 6$, quindi:

$$\binom{5+6-1}{6} = \binom{10}{6} = \frac{10!}{6!4!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6!}{6!4 \cdot 3 \cdot 2} = 10 \cdot 3 \cdot 7.$$

Esempio 128. Calcolare il numero di combinazioni con ripetizione (no ordine) di lunghezza 5 delle lettere a e b. Ovvero $A = \{a, b\}$ $n = 2$ e $k = 5$, quindi:

$$\binom{2+5-1}{5} = \frac{6!}{5!1!} = 6.$$

Queste sono $aaaaa, aaaab, aaabb, aabbb, abbbb, bbbbb$.

Esempio 129. In quanti modi possiamo distribuire 5 caramelle a 2 bambini?

Questo numero corrisponde a scegliere $k = 5$ oggetti in un insieme con 2 elementi. Quindi, come nell'Esempio 128, abbiamo la formula:

$$\binom{2+5-1}{5} = \binom{6}{5} = 6.$$

Vediamolo in maniera esplicita. Abbiamo 5 caramelle da distribuire ai 2 bambini che possiamo chiamare a e b. Quindi per ogni caramella dobbiamo scegliere se darla al bambino a o al bambino b. È come dire la prima caramella la scegliamo nell'insieme $\{a, b\}$ che ha 2 elementi, la seconda anche e così via. Possiamo avere $aaaaa, aaaab, aaabb, aabbb, abbbb, bbbbb$. In questa scrittura $aaaaa$ corrisponde a 5+0, ovvero abbiamo scelto 5 volte la a e mai la b: abbiamo dato tutte le 5 caramelle al bambino a. La scrittura $aaabb$ corrisponde a 3 caramelle al bambino a e 2 al bambino b. A questo punto dovrebbe essere chiaro che l'ordine non è importante $ababa$ oppure $abbaa$ corrispondono sempre a scegliere il bambino a per 3 caramelle e il b per le altre 2. Quindi stiamo effettivamente contando le combinazioni semplici di $n = 2$ oggetti di classe $k = 5$, ovvero stiamo scegliendo 5 elementi in un insieme con 2 elementi ammettendo le ripetizioni e l'ordine non è importante.

Gli elementi $aaaaa, aaaab, aaabb, aabbb, abbbb, bbbbb$ corrispondono alle distribuzioni di caramelle: $5+0, 4+1, 3+2, 2+3, 1+4, 1+5$. (Confrontare Esercizio 128).

Esempio 130. In quanti modi possiamo distribuire 35 caramelle a 5 bambini, dandone almeno una a bambino?

La richiesta equivale a dare una caramella ad ogni bambino e poi distribuire 35-5=30 caramelle a 5 bambini. Ovvero dobbiamo scegliere 30 elementi tra i 5 dell'insieme $\{a, b, c, d, e\}$ (per forza con ripetizione). Quindi $n = 5,\ k = 30$ e allora

$$\binom{5+30-1}{30} = \frac{34!}{30!4!} = \frac{34 \cdot 33 \cdot 32 \cdot 31}{24}.$$

Non incluso nel Programma. In quanti modi si possono scegliere k elementi in un insieme con n oggetti, ammettendo anche ripetizioni e ordine non importante? In tal caso, abbiamo

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

In questo caso l'ordine non è importante quindi consideriamo uguali, le k-ple con gli stessi elementi anche in ordine diverso.

Dimostrazione. Sia $A = \{a_1, a_2, \ldots, a_n\}$, e consideriamo una combinazione di k elementi con ripetizione. Possiamo raggruppare gli elementi ripetuti: mettiamo vicino quelli uguali

$$a_i a_i a_i a_j a_j \cdots a_j \cdots\cdots a_r a_r \cdots a_r$$

dove abbiamo n_i volte a_i, n_j volte a_j.... n_r volte a_r con $n_i + n_j + \cdots + n_r = k$. A questo oggetto associamo la scrittura

$$xx \cdots x|xx \cdots x| \cdots |xx \cdots x$$

Al primo posto abbiamo n_i volte x, al secondo posto n_j volte x e così via. Mettiamo una sbarretta | ogni volta che passiamo da un elemento all'altro.

Esempio 131. Siano $A = \{1, 2, 3, 4\}$, quindi $n = 4$, e 123212443 una sequenza con $k = 9$. Allora prima cosa la trasformiamo in 112223344. Quindi associamo la scrittura $xx|xxx|xx|xx$. Abbiamo $3 = n - 1$ volte il simbolo | e $2 + 3 + 2 + 2 = 9$ volte la lettera x.

Esempio 132. Siano $A = \{1, 2, 3, 4, 5\}$, quindi $n = 5$, e 122212442 una sequenza con $k = 9$. Allora prima cosa la trasformiamo in 112222244. Quindi associamo la scrittura $xx|xxxxx||xx|$. Abbiamo $4 = n - 1$ volte il simbolo | e $2 + 3 + 2 + 2 = 9$ volte la lettera x.

Osservazione 43. Il simbolo | serve per separare elementi diversi e quindi ci indica il passaggio da un elemento all'altro.

Abbiamo $n - 1$ sbarrette e k elementi in tutto da ordinare quindi $(n - 1 + k)!$
Le sbarrette possiamo scambiarle tra loro quindi dividiamo per $(n - 1)!$
Le x possiamo scambiarle tra loro e quindi dividiamo per $k!$
Otteniamo quindi

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

9. Relazioni

La Repubblica, una e indivisibile, riconosce e promuove le autonomie locali; attua nei servizi che dipendono dallo Stato il più ampio decentramento amministrativo; adegua i principi ed i metodi della sua legislazione alle esigenze dell'autonomia e del decentramento

Definizione 38. Sia A un insieme non vuoto. Una relazione (binaria) $\mathscr{R}$ sull'insieme A è un sottoinsieme del prodotto cartesiano di $A \times A$.

Quindi $\mathscr{R} \subseteq A \times A$ è un sottoinsieme, ovvero è costituito da coppie ordinate $(a, b) \in A \times A$. Oltre alla notazione $(a, b) \in \mathscr{R}$ useremo spesso la notazione $a\mathscr{R}b$ e diremo a è in relazione con b (oppure a è associato a b nella relazione $\mathscr{R}$).

Osservazione 44. Sappiamo che $(a, b) \neq (b, a)$ poiché sono coppie ordinate, quindi dire $a\mathscr{R}b$ non è uguale a dire $b\mathscr{R}a$.

Esempio 133. Siano $A = \mathbb{Q}$ e $\mathscr{R} \subseteq \mathbb{Q} \times \mathbb{Q}$ definita da

$$\forall\, a, b \in \mathbb{Q} \qquad a\mathscr{R}b \iff 2b - 6a = 4$$

Quindi

$$\mathscr{R} = \{(a, b) \in \mathbb{Q} \times \mathbb{Q} \mid 2b - 6a = 4\}$$

Osserviamo $2b = (4 + 6a)$, quindi $b = 2 + 3a$.

Ad esempio $(0, 2), (1, 5), (-3, -7) \in \mathscr{R}$, ovvero $0\mathscr{R}2,\ 1\mathscr{R}5,\ -3\mathscr{R}-7$

Inoltre, possiamo chiedere 9 è in relazione con 11? ovvero $(9, 11) \in \mathscr{R}$? $2{*}11{-}6{*}9 \neq 4$, allora $(9, 11) \notin \mathscr{R}$ ovvero $9\ \not\mathscr{R}11$.

Esempio 134. Siano $A = \mathbb{R}$ e $\mathscr{R} \subseteq \mathbb{R} \times \mathbb{R}$ definita da

$$\forall\, a, b \in \mathbb{R} \qquad a\mathscr{R}b \iff a = b^2 + 3$$

Quindi

$$\mathscr{R} = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a = b^2 + 3\}$$

Possiamo fissare b e trovare a.

Ad esempio $(4, 1), (4, -1), (5, \sqrt{2}) \in \mathscr{R}$, ovvero $4\mathscr{R}1,\ 4\mathscr{R}-1,\ 5\mathscr{R}\sqrt{2}$.

Esempio, 0 è in relazione con qualcosa? Ovvero esiste b con $(0, b) \in \mathscr{R}$? No, ma $(3, 0) \in \mathscr{R}$, ovvero $3\mathscr{R}0$.

Osservazione 45. Ogni sottoinsieme di $A \times A$ è una relazione su A.

In particolare $\mathscr{R} = \emptyset$ è detto *relazione vuota* (nessun elemento di A è in relazione con un elemento di A).

$\mathscr{R} = A \times A$ è detta *relazione totale*, ogni elemento di A è in relazione con ogni elemento di A.

Infine possiamo considerare $\mathscr{R} = \{(x, x) \in A \times A\}$, ogni elemento di A è in relazione solo con se stesso: $\mathscr{R}$ è la *relazione identica* o *relazione di uguaglianza* su A.

9.1. Relazioni d'ordine.

In questa sezione introduciamo una classe importanti di relazioni: le relazioni d'ordine definite su un insieme A non vuoto, quindi $\mathscr{R} \subseteq A \times A$.

Definizione 39. (ORDINE PARZIALE) Una relazione $\mathscr{R}$ definita su un insieme A non vuoto si dice *relazione d'ordine parziale* se verifica le seguenti proprietà

(1) Proprietà RIFLESSIVA: $\forall a \in A$ allora $a\mathscr{R}a$.

(2) Proprietà ANTISIMMETRICA: $\forall a, b \in A$ se $a\mathscr{R}b$ e $b\mathscr{R}a$ allora $a = b$.

(3) Proprietà TRANSITIVA: $\forall a, b, c \in A$ se ha $a\mathscr{R}b$ e $b\mathscr{R}c$ allora $a\mathscr{R}c$.

Osservazione 46. Una relazione $\mathscr{R}$ su A:

(1) Per non essere riflessiva, basta che $\exists a \in A$ tale che $(a, a) \notin \mathscr{R}$, ovvero $a \not\mathscr{R}a$;

(2) Per non essere antisimmetrica, basta che $\exists a, b \in A$ tale che $a\mathscr{R}b$ e $b\mathscr{R}a$ e $a \neq b$;

(3) Per non essere transitiva, basta che $\exists a, b, c \in A$ tale che $a\mathscr{R}b$ e $b\mathscr{R}c$ ma $a \not\mathscr{R}c$.

Esempio 135. Sia $A = \{s, t, r, x, v\}$. Sia $\mathscr{R} \subseteq A \times A$ con

$$\mathscr{R} = \{(s, s), (s, t), (t, t), (r, r), (x, t), (t, s), (t, v)\}$$

$\mathscr{R}$ è sottoinsieme di $A \times A$? Si, quindi definisce una relazione.
(Sketch) Ci chiediamo è RIFL? ANTISIM? TRANSI? Relazione d'ordine?
Prima cosa: è RIFLE?
È vero che $\forall a \in A$ si ha $a\mathscr{R}a$? se si è riflessiva, altrimenti no.
$(v, v) \notin \mathscr{R}$ quindi non riflessiva.
È antisim? No, perchè $(s, t), (t, s) \in \mathscr{R}$ ma $s \neq t$.
È transitiva? No perchè $x\mathscr{R}t, t\mathscr{R}v$ ma $x \not\mathscr{R}v$.

Esempio 136. Sia $A = \mathbb{N}$ numeri naturali. Sia $\mathscr{R} :=\leq$ ovvero

$$\forall\, a, b \in \mathbb{N} \quad a\mathscr{R}b \iff \exists x \in \mathbb{N} \text{ tale che } b = a + x$$

(b più grande di a, ovvero $a \leq b$).
Ad esempio $3 \leq 5$, $6 \leq 12$,$13 \leq 25$ e $5 \not\leq 2$, $3 \not\leq 2$.
(Sketch) Ci chiediamo è RIFL? ANTISIM? TRANSI? È una relazione d'ordine?
Prima cosa: è RIFLE?
È vero che $\forall a \in \mathbb{N}$ si ha $a \leq a$? Se si è riflessiva, altrimenti no.
Per definizione:

$$a\mathscr{R}a \iff \exists x \in \mathbb{N} \text{ tale che } a = a + x.$$

Si Riflessiva, basta prendere $x = 0 \in \mathbb{N}$.
È antisimmetrica? Ci chiediamo è vero che: $\forall a, b \in A$ se $a\mathscr{R}b$ e $b\mathscr{R}a$ allora $a = b$?
Allora $a\mathscr{R}b$ quindi esiste $x \in \mathbb{N}$ tale che $b = a + x$,
inoltre $b\mathscr{R}a$ quindi esiste $y \in \mathbb{N}$ tale $a = b + y$.
Quindi $b = a + x = b + x + y$ ovvero $0 = x + y$ ovvero $x = y = 0$ (siamo in $\mathbb{N}$!).
Quindi è antisimmetrica (chiaro: se $a \leq b$ e $b \leq a$ allora $a = b$).
È transitiva? Ci chiediamo è vero che: $\forall a, b, c \in A$ se ha $a\mathscr{R}b$ e $b\mathscr{R}c$ allora $a\mathscr{R}c$?
Allora $a\mathscr{R}b$ implica che esiste $x \in \mathbb{N}$ tale che $b = a + x$;
$b\mathscr{R}c$ implica che esiste $y \in \mathbb{N}$ tale che $c = b + y$;
Ci chiediamo è vero che $a\mathscr{R}c$? Questo è vero se e solo se esiste $z \in \mathbb{N}$ con $c = z + a$.
Allora $c = b + y = a + x + y$, quindi si esiste $z = x + y \in \mathbb{N}$.
(Chiaro: se $a \leq b$ e $b \leq c$ allora $a \leq c$.)

Esempio 137. Sia A un insieme finito, consideriamo l'insieme delle parti di A: $\mathscr{P}(A)$.
Definiamo una relazione su $\mathscr{P}(A)$, ovvero $\mathscr{R} \subseteq \mathscr{P}(A) \times \mathscr{P}(A)$.

$$\forall X, Y \in \mathscr{P}(A) \qquad X\mathscr{R}Y \iff X \subseteq Y$$

ovvero $\mathscr{R} = \{(X, Y) \in \mathscr{P}(A) \times \mathscr{P}(A) \mid X \subseteq Y\}$, $\mathscr{R} =\subseteq$ è la relazione di inlcusione.
(Sketch)
Ci chiediamo è RIFL? ANTISIM? TRANSI? relazione d'ordine?
Prima cosa: è RIFLE?

È vero che $\forall X \in \mathscr{P}(A)$ si ha $X \mathscr{R} X$? Se si è riflessiva, altrimenti no.
Vero, $\forall X \in \mathscr{P}(A)$ si ha $X \subseteq X$.
È antisim? Ci chiediamo è vero che: $\forall X, Y \in \mathscr{P}(A)$ se $X \mathscr{R} Y$ e $Y \mathscr{R} X$ allora $X = Y$?
Allora $X \mathscr{R} Y$ quindi $X \subseteq Y$; $Y \mathscr{R} X$ quindi $Y \subseteq X$ ma allora $X = Y$.
Quindi è antisimmetrica.
Infine, è transitiva? ci chiediamo è vero che: $\forall X, Y, Z \in \mathscr{P}(A)$ se $X \mathscr{R} Y$ e $Y \mathscr{R} Z$ allora $X \subseteq Z$?
$X \subseteq Y$ e $Y \subseteq Z$ implica $X \subseteq Y \subseteq Z$ quindi $X \subseteq Z$.
Quindi è transitiva. Pertanto è una relazione di ordine parziale.

Definizione 40. (PARZIALMENTE ORDINATO) Un insieme A si dice *parzialmente ordinato* se è definita su A una relazione $\mathscr{R}$ di ordine parziale. In tal caso, scriveremo $(A, \mathscr{R})$ o $(A, \leq)$ è un insieme parzialmente ordinato.

Esempio 138. Esempi $(\mathbb{N}, \leq)$ e $(\mathscr{P}(A), \subseteq)$.

Osservazione 47. Nella definizione di relazione d'ordine non richiediamo che presi comunque due elementi a e b essi siano confrontabili.

Definizione 41. (TOTALMENTE ORDINATO) Un insieme A si dice *totalmente ordinato* se è parzialmente ordinato ed ogni coppia di elementi è confrontabile, ovvero presi comunque due elementi $a, b \in A$, si ha che $a \mathscr{R} b$ o $b \mathscr{R} a$.

Esempio 139. $(N, \leq)$ è totalmente ordinato. Infatti, presi $a, b \in \mathbb{N}$, si ha che $a \leq b$ o $b \leq a$. (Infatti, $\exists\, x \in \mathbb{N}$ tale che $b = a + x$ oppure $\exists\, y \in \mathbb{N}$ tale che $a = b + y$).

Esempio 140. $(\mathscr{P}(A), \subseteq)$ non è totalmente ordinato se $\mid A \mid \geq 2$. Infatti, in generale non è vero che presi comunque due sottoinsiemi X e Y di A, si ha che $X \subseteq Y$ oppure $Y \subseteq X$.

Esempio 141. $A = \{a, b, c\}$, allora $\mathscr{P}(A) = \{\emptyset, A, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$. Allora ad esempio: $\{a, b\}$ e $\{c\}$ non sono confrontabili.

9.2. **Relazioni di equivalenza.** In questa sezione introduciamo una classe importante di relazioni: le relazioni di equivalenza definite su un insieme A non vuoto, quindi $\mathscr{R} \subseteq A \times A$.

Definizione 42. (EQUIVALENZA) Una relazione $\mathscr{R}$ definita su un insieme A si dice *relazione d'equivalenza* se verifica le seguenti proprietà

(1) Proprietà RIFLESSIVA: $\forall a \in A$ allora $a \mathscr{R} a$.

(2) Proprietà SIMMETRICA: $\forall a, b \in A$ se $a \mathscr{R} b$ allora $b \mathscr{R} a$.

(3) Proprietà TRANSITIVA: $\forall a, b, c \in A$ se ha $a \mathscr{R} b$ e $b \mathscr{R} c$ allora $a \mathscr{R} c$.

Definizione 43. Sia $\mathscr{R}$ una relazione di equivalenza su un insieme A. Se due elementi a e b in A sono tali che $a \mathscr{R} b$ allora si dice che a è *equivalente a* b.

Osservazione 48. Una relazione $\mathscr{R}$ su A:
Per non essere simmetrica, basta che $\exists a, b \in A$ tale che $a \mathscr{R} b$ ma $b \not\mathscr{R} a$.

Osservazione 49. Sia $\mathscr{R}$ una relazione simmetrica e anti simmetrica, se $a \mathscr{R} b$ allora per la simmetria si ha $b \mathscr{R} a$. Ora per antisimmetria $a = b$. Quindi nelle relazioni simmetriche e antisimmetriche, un elemento può essere in relazione solo con se stesso.
Se anche riflessiva allora è relazione identica.

Vediamo gli esempi analizzati nella Sezione 9.1.

Esempio 142. Sia $A = \{s, t, r, x, v\}$. Sia $\mathscr{R} \subseteq A \times A$ con

$$\mathscr{R} = \{(s,s), (s,t), (t,t), (r,r), (x,t), (t,s), (t,v)\}$$

Non è di equivalenza. Non è simmetrica perché $(x,t) \in \mathscr{R}$ ma $(t,x) \notin \mathscr{R}$.

Esempio 143. Sia $A = \mathbb{N}$ numeri naturali. Sia $\mathscr{R} := \leq$ ovvero

$$\forall\, a, b \in \mathbb{N} \quad a\mathscr{R}b \iff \exists x \in \mathbb{N} \text{ tale che } b = a + x$$

Ci chiediamo se è simmetrica: è vero che $\forall a, b \in A$ se $a\mathscr{R}b$ allora $b\mathscr{R}a$. Se $a\mathscr{R}b$ vuol dire $a \leq b$, ma questo non implica $b \leq a$. Esempio: $3\mathscr{R}5$ dato che $3 \leq 5$, ma $5 \not\leq 3$ non è simmetrica.

Esempio 144. Sia A un insieme finito, consideriamo l'insieme delle parti di A: $\mathscr{P}(A)$. Definiamo una relazione su $\mathscr{P}(A)$, ovvero $\mathscr{R} \subseteq \mathscr{P}(A) \times \mathscr{P}(A)$

$$\forall X, Y \in \mathscr{P}(A) \qquad X\mathscr{R}Y \iff X \subseteq Y$$

è simmetrica? No. Se $X\mathscr{R}Y$ allora $X \subseteq Y$ e questo non implica $Y \subseteq X$.

Esempio 145. Sia $A = \{x, y, z\}$. Sia $\mathscr{R} \subseteq A \times A$ con

$$\mathscr{R} = \{(x,x), (y,y), (z,z), (x,z), (z,x)\}$$

Stabilire se è riflessiva, simmetrica e transitiva.

Esempio 146. Sia $\mathscr{R}$ la relazione totale su un insieme A (Osservazione 45), allora è riflessiva, simmetrica, transitiva.

Esercizio 31. Sia A un insieme. La relazione identica su A è una relazione di equivalenza (Osservazione 45). Dove

$$\forall\, a, b \in A \quad a\mathscr{R}b \iff a = b$$

Esercizio 32. Sia $A = \{$ insieme delle rette nel piano $\}$. Definiamo la relazione

$$\forall\, a, b \in A \quad a\mathscr{R}b \iff a \text{ è parallela a } b : \; a//b$$

Determinare se la relazione è riflessiva, simmetrica, transitiva, antisimmetrica, d'equivalenza, d'ordine.

(Sketch della soluzione)

È riflessiva? $\forall a \in A$ si ha $a\mathscr{R}a$?

Per ogni retta $r \in A$, si ha $r//r$? si.

È SIMMETRICA? È vero che $\forall a, b \in A$ se $a\mathscr{R}b$ allora $b\mathscr{R}a$? È vero che $\forall r, s \in A$ se $r//s$ allora $s//r$? Si. Quindi è simmetrica.

È TRANSITIVA? È vero che $\forall a, b, c \in A$ se $a\mathscr{R}b$ e $b\mathscr{R}c$ allora $a\mathscr{R}c$?

Se $r//s$ e $s//t$ allora $r//t$. Si. (Considerando le direzioni delle rette: $d_r = d_s$ e $d_s = d_t$ allora $d_r = d_t$). Quindi $\mathscr{R} = //$ è una relazione di equivalenza.

È antisimmetrica? $\forall a, b \in A$ se $a\mathscr{R}b$ e $b\mathscr{R}a$ allora $a = b$ se $r//s$ è simmetrica quindi vero $s//r$ ma non è vero che $s = r$ esistono rette parallele ma non coincidenti.

9.3. **Classi di equivalenza e Insieme quoziente.** Abbiamo definito le relazioni di equivalenza su un insieme $A \neq \emptyset$.

Definizione 44. (CLASSE di EQUIVALENZA) Sia $\mathscr{R}$ una relazione d'equivalenza sull'insieme A. Si definisce *classe di equivalenza* modulo $\mathscr{R}$ di un elemento $a \in A$ l'insieme di tutti gli elementi di A che sono equivalenti ad a. Si denota con $[a]_{\mathscr{R}}$ (oppure solo $[a]$ quando è chiaro chi sia $\mathscr{R}$), ovvero

$$[a]_{\mathscr{R}} = \{x \in A \mid a\mathscr{R}x\} = \{x \in A \mid x\mathscr{R}a\} = \{x \in A \mid (a,x) \in \mathscr{R}\} = \{x \in A \mid (x,a) \in \mathscr{R}\}$$

dato che $\mathscr{R}$ è simmetrica.

Osservazione 50. Tutti gli elementi di una classe di equivalenza sono tutti equivalenti fra loro. Infatti, se $x, y \in [a]_{\mathscr{R}}$, allora $x\mathscr{R}a$ e $y\mathscr{R}a$. Per la proprietà simmetrica, questo implica che $x\mathscr{R}a$ e $a\mathscr{R}y$ e quindi, per la proprietà transitiva, si ha che $x\mathscr{R}y$.

Esempio 147. Si consideri un insieme non vuoto A con $\mathscr{R}$ relazione identica su A. Allora $\mathscr{R}$ è di equivalenza e

$$[a]_{\mathscr{R}} = \{x \in A \mid a\mathscr{R}x\} = \{a\}.$$

Esempio 148. Si consideri un insieme non vuoto A con $\mathscr{R}$ relazione totale su A, ovvero $\mathscr{R} = A \times A$. Allora $\mathscr{R}$ è di equivalenza e

$$[a]_{\mathscr{R}} = \{x \in A \mid a\mathscr{R}x\} = A$$

Esempio 149. A= insieme delle rette del piano con $\mathscr{R}$ relazione di parallelismo. Allora $\mathscr{R}$ è di equivalenza e

$$[a]_{\mathscr{R}} = \{x \in A \mid a\mathscr{R}x\} = \{ \text{ rette parallele ad } a\}.$$

Osservazione 51. Per la proprietà riflessiva $a\mathscr{R}a$ ovvero $a \in [a]_{\mathscr{R}}$ (SEMPRE). Quindi $\forall a \in A$ si ha che $[a]_{\mathscr{R}} \neq \emptyset$: le classi di equivalenza non sono mai vuote.

Teorema 3. *Sia $\mathscr{R}$ una relazione di equivalenza su un insieme non vuoto. Allora*

(1) *$\forall a \in A$ si ha $a \in [a]_{\mathscr{R}}$;*

(2) *$\forall a, b \in A$: $a\mathscr{R}b \iff [a]_{\mathscr{R}} = [b]_{\mathscr{R}}$;*

(3) *$\forall a, b \in A$: $[b]_{\mathscr{R}} \neq [a]_{\mathscr{R}} \iff [a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \emptyset$.*

Osservazione 52. 1) Già vista nell'Osservazione 51: ogni elemento appartiene alla sua classe di equivalenza, quindi le classi di equivalenza non sono mai vuote.

2) Se a è equivalente a b allora a e b hanno la stessa classe di equivalenza, ovvero una classe di equivalenza è determinata da un suo qualsiasi elemento.

3) Se le classi sono diverse allora le classi sono disgiunte, ovvero classi distinte non hanno alcun elemento in comune.

Quindi le classi di equivalenza o coincidono o sono disgiunte.

Dimostrazione. 1) Per la proprietà riflessiva: $\forall a \in A$ si ha $a\mathscr{R}a$ e quindi $a \in [a]_{\mathscr{R}}$.

2) Dimostriamo $(\Longleftarrow)$: $\forall a, b \in A$ se $[a]_{\mathscr{R}} = [b]_{\mathscr{R}} \Longrightarrow a\mathscr{R}b$.

Se $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$ per la 1) $a \in [a]_{\mathscr{R}}$. Allora $a \in [a]_{\mathscr{R}} = [b]_{\mathscr{R}}$ ovvero $a \in [b]_{\mathscr{R}}$ e quindi $a\mathscr{R}b$.

Viceversa dimostriamo $(\Longrightarrow)$: $\forall a, b \in A$ $a\mathscr{R}b \Longrightarrow [a]_{\mathscr{R}} = [b]_{\mathscr{R}}$

Se $a\mathscr{R}b$ bisogna dimostrare una uguaglianza di insiemi $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$ ovvero la doppia inclusione $[a]_{\mathscr{R}} \subseteq [b]_{\mathscr{R}}$ e $[b]_{\mathscr{R}} \subseteq [a]_{\mathscr{R}}$.

Sia $x \in [a]_{\mathscr{R}}$ allora $x\mathscr{R}a$ per ipotesi $a\mathscr{R}b$ e quindi per la transitività $x\mathscr{R}b$ ovvero $x \in [b]_{\mathscr{R}}$ quindi $[a]_{\mathscr{R}} \subseteq [b]_{\mathscr{R}}$.

Viceversa se $x \in [b]_{\mathscr{R}}$ allora $x\mathscr{R}b$, per ipotesi $a\mathscr{R}b$ e quindi per simmetria $b\mathscr{R}a$. Applichiamo la transitività e otteniamo $x\mathscr{R}a$ ovvero $x \in [a]_{\mathscr{R}}$ quindi $[b]_{\mathscr{R}} \subseteq [a]_{\mathscr{R}}$.

3) $\forall a, b \in A$: $[b]_{\mathscr{R}} \neq [a]_{\mathscr{R}} \iff [a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \emptyset$

Dimostriamo $(\Longrightarrow)$: Se $[b]_{\mathscr{R}} \neq [a]_{\mathscr{R}}$ allora $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \emptyset$. Supponiamo per assurdo $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} \neq \emptyset$ allora esiste $x \in A$ con $x \in [a]_{\mathscr{R}} \cap [b]_{\mathscr{R}}$ allora $x \in [a]_{\mathscr{R}}$ e $x \in [b]_{\mathscr{R}}$. Quindi $x\mathscr{R}a$ e $x\mathscr{R}b$. Per la simmetria abbiamo $a\mathscr{R}x$ e $x\mathscr{R}b$. Per la transitività otteniamo $a\mathscr{R}b$. Quindi per 2) $[b]_{\mathscr{R}} = [a]_{\mathscr{R}}$. Assurdo.

Viceversa, dimostriamo $(\Longleftarrow)$: $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \emptyset \Longrightarrow [b]_{\mathscr{R}} \neq [a]_{\mathscr{R}}$

Per assurdo, se $[b]_{\mathscr{R}} = [a]_{\mathscr{R}}$. Allora $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = [a]_{\mathscr{R}} \cap [a]_{\mathscr{R}} = [a]_{\mathscr{R}} \neq \emptyset$. Assurdo.

Esempio 150. $A = \{$insieme rette del piano $\}$ e $\mathscr{R}$ la relazione di parallelismo che è di equivalenza. La classe di equivalenza di una retta a, è l'insieme di tutte le rette parallele alla retta a.

Ogni retta parallela a è una retta parallela a se stessa e quindi appartiene alla sua classe di equivalenza.

Se due rette sono parallele allora gli insiemi delle rette parallele all'una o all'altra coincidono.

Se due rette non sono parallele allora non esistono rette che sono parallele ad entrambe.

Definizione 45. (PARTIZIONE) Sia A un insieme non vuoto. Una *partizione* dell'insieme A è una collezione di sottoinsiemi $\{A_i\}_{i\in I}$ dove I è un insieme di indici tali che

(1) Ogni sottoinsieme è non vuoto: $\forall i \in I \qquad A_i \neq \emptyset$.

(2) Gli insiemi sono disgiunti tra loro $\forall i \neq j \qquad A_i \cap A_j = \emptyset$.

(3) Gli insiemi ricoprono A ovvero: $\bigcup_{i\in I} A_i = A$.

In altre parole ogni elemento di A appartiene ad un unico sottoinsieme della partizione. Gli insieme A_i sono detti elementi della partizione.

Esempio 151. $A = \mathbb{N}$, $A_1 = \{$ numeri pari $\}$, $A_2 = \{$ numeri dispari $\}$. $\mathbb{N} = A_1 \bigcup A_2$ e $A_1 \neq \emptyset$, $A_2 \neq \emptyset$ e $A_1 \cap A_2 = \emptyset$.

Come sono legate le partizioni alle relazioni di equivalenza?

Teorema 4. *Sia $\mathscr{R}$ una relazione di equivalenza su un insieme A non vuoto. Le classi di equivalenza di $\mathscr{R}$ costituiscono una partizione di A.*

Osservazione 53. Il teorema afferma che ogni relazione di equivalenza su A determina una partizione di A i cui elementi sono le classi di equivalenza. È vero il viceversa?

Teorema 5. *Ogni partizione di un insieme A determina una relazione di equivalenza $\mathscr{R}$ su A le cui classi di equivalenza sono gli elementi della partizione considerata.*

Definizione 46. (INSIEME QUOZIENTE) Sia $\mathscr{R}$ una relazione di equivalenza su un insieme A non vuoto. Si definisce l'*insieme quoziente* di A rispetto a $\mathscr{R}$, e si indica con $A/\mathscr{R}$ l'insieme

$$A/\mathscr{R} = \{[a]_{\mathscr{R}} \mid a \in A\} = \{ \text{ classi di equivalenza } \}$$

(Si deve prendere un rappresentante per ogni classe di equivalenza, ovvero elementi che non sono equivalenti tra loro. Infatti, se due elementi sono equivalenti, allora stessa classe di equivalenza, quindi rappresentano lo stesso elemento nell'insieme quoziente, e quindi non lo scriviamo due volte.)

Osservazione 54. Elementi equivalenti in A sono uguali in $A/\mathscr{R}$.

Esercizio 33. $A = \{1, 3, 4, 5, 7, 8, 9\}$ definiamo la relazione $\mathscr{R}$ su A

$$\forall\, a, b \in A \quad a\mathscr{R}b \iff a - b \text{ pari}$$

Scrivere tutti gli elementi della relazione $\mathscr{R}$ dire se è riflessiva, simmetrica, transitiva, d'equivalena e se si calcolare l'insieme quoziente.

$$\begin{array}{ccccc} 1\mathscr{R}1 & 1\mathscr{R}3 & 1\mathscr{R}5 & 1\mathscr{R}7 & 1\mathscr{R}9 \\ 3\mathscr{R}1 & 3\mathscr{R}3 & 3\mathscr{R}5 & 3\mathscr{R}7 & 3\mathscr{R}9 \\ & & 4\mathscr{R}4 \quad 4\mathscr{R}8 & & \\ 5\mathscr{R}1 & 5\mathscr{R}3 & 5\mathscr{R}5 & 5\mathscr{R}7 & 5\mathscr{R}9 \end{array}$$

$$7\mathscr{R}1 \quad 7\mathscr{R}3 \quad 7\mathscr{R}5 \quad 7\mathscr{R}7 \quad 7\mathscr{R}9$$
$$8\mathscr{R}4 \quad 8\mathscr{R}8$$
$$9\mathscr{R}1 \quad 9\mathscr{R}3 \quad 9\mathscr{R}5 \quad 9\mathscr{R}7 \quad 9\mathscr{R}9$$

Quindi i numeri dispari sono in relazione tra loro e i numeri pari sono in relazione fra loro. È riflessiva? Si. È simmetrica? Si. È transitiva? Si. Pertanto, $\mathscr{R}$ è una relazione di equivalenza. Classi di equivalenza

$$[1]_{\mathscr{R}} = \{x \in A \mid 1\mathscr{R}x\} = \{1, 5, 3, 7, 9\} = [3]_{\mathscr{R}} = [5]_{\mathscr{R}} = [7]_{\mathscr{R}} = [9]_{\mathscr{R}}$$
$$[8]_{\mathscr{R}} = \{x \in A \mid 8\mathscr{R}x\} = \{4, 8\} = [4]_{\mathscr{R}} = [8]_{\mathscr{R}}$$

quindi $A/\mathscr{R} = \{[8]_{\mathscr{R}}, [5]_{\mathscr{R}}\}$, oppure $A/\mathscr{R} = \{[4]_{\mathscr{R}}, [5]_{\mathscr{R}}\} = \{[7]_{\mathscr{R}}, [8]_{\mathscr{R}}\}$.

Esercizio 34. (per casa) Si consideri la relazione su $A = \mathbb{Z}$

$$\forall\, a, b \in \mathbb{Z} \quad a\mathscr{R}b \iff a - b \text{ pari.}$$

Stabilire se si tratta di una relazione di equivalenza, d'ordine, d'ordine totale. Se si tratta di una relazione di equivalenza stabilire le classi di 0, 2,1 e -2. Descrivere l'insieme quoziente.

Esempio 152. Sia $\mathscr{R}$ la relazione identica su un insieme A non vuoto, cioè $\forall\, a \in A$ si ha $a\mathscr{R}a$. Allora $[a]_{\mathscr{R}} = \{a\}$. Quindi $A/\mathscr{R} = A$.

Esempio 153. Sia $\mathscr{R}$ la relazione totale su un insieme A non vuoto, cioè $\forall\, a, b \in A$ si ha $a\mathscr{R}b$. Allora $[a]_{\mathscr{R}} = A$, per ogni $\forall\, a \in A$. Quindi $A/\mathscr{R} = \{[a]_{\mathscr{R}}\}$ ha un unico elemento.

Esercizio 35. Sia fissato $n \in \mathbb{N}^*$ e definiamo la relazione su $A = \mathbb{Z}$

$$\forall\, a, b \in \mathbb{Z} \quad a\mathscr{R}b \iff \exists k \in \mathbb{Z} \text{ tale che } a - b = kn$$

ovvero $a - b$ multiplo di n.

Stabilire se si tratta di una relazione di equivalenza. Se si tratta di una relazione di equivalenza stabilire le classi di 0 e 1.

(Sketch della soluzione)

È riflessiva? $\forall a \in A$ si ha $a\mathscr{R}a$?

$a\mathscr{R}a$ se e solo se $\exists k \in \mathbb{Z}$ tale che $a - a = kn$ ovvero $a - a = 0 = kn$ scegliamo $k = 0$.

È SIMMETRICA? È vero che $\forall a, b \in A$ se $a\mathscr{R}b$ allora $b\mathscr{R}a$?

se $a\mathscr{R}b$ allora $\exists k \in \mathbb{Z}$ tale che $a - b = kn$ allora $b - a = (-k)n$ e $-k \in \mathbb{Z}$, quindi $b\mathscr{R}a$.

È TRANSITIVA? È vero che $\forall a, b, c \in A$ se $a\mathscr{R}b$ e $b\mathscr{R}c$ allora $a\mathscr{R}c$?

Supponiamo $a\mathscr{R}b$ e $b\mathscr{R}c$.

Allora $a\mathscr{R}b$ implica $\exists k \in \mathbb{Z}$ tale che $a - b = kn$

$b\mathscr{R}c$ implica $\exists t \in \mathbb{Z}$ tale che $b - c = tn$

Sommiamo $a - c = tn + kn = (t + k)n$. Quindi $a\mathscr{R}c$.

Quindi equivalenza. Infine

$$[0]_{\mathscr{R}} = \{x \in A \mid 0\mathscr{R}x\} = \{x \in A \mid \exists k \in \mathbb{Z} \text{ tale che } x = kn\} = \{ \text{ multipli di n } \}$$
$$[1]_{\mathscr{R}} = \{x \in A \mid 1\mathscr{R}x\} = \{x \in A \mid \exists k \in \mathbb{Z} \text{ tale che } 1 - x = kn\} = \{x \in \mathbb{Z} \mid x = 1 - kn\}$$

Esercizio 36. Si consideri la relazione su $A = \mathbb{Z}$

$$\forall\, a, b \in \mathbb{Z} \quad a\mathscr{R}b \iff \exists k \in \mathbb{Z} \text{ tale che } 3a + 8b = 11k$$

Stabilire se si tratta di una relazione di equivalenza, d'ordine, d'ordine totale. Se si tratta di una relazione di equivalenza stabilire le classi di 0 e 1.

Ad esempio, la classe di equivalenza di 0 è

$$[0]_{\mathscr{R}} = \{x \in A \mid 0\mathscr{R}x\} = \{x \in A \mid \exists k \in \mathbb{Z} \text{ tale che } 8x = 11k\} =$$
$$\{x \in A \mid x\mathscr{R}0\} = \{x \in A \mid \exists k \in \mathbb{Z} \text{ tale che } 3x = 11k\}.$$

10. I Numeri Interi

La Repubblica tutela con apposite norme le minoranze linguistiche.

In questo capitolo ci occuperemo di numeri interi, di divisione, di massimo comun divisore e dell'algoritmo di Euclide per determinarlo.

10.1. **Divisione.** Ricordiamo la definizione di divisore, multiplo e di divisione.

Definizione 47. Dati $a, b \in \mathbb{Z}$ diremo che a *divide* b oppure che a è un divisore di b, e scriveremo $a \mid b$, se esiste un intero $c \in \mathbb{Z}$ tale che $b = a \cdot c$. Se a non divide b scriveremo $a \not| b$.

Osservazione 55. Se $a \mid b$ (rispettivamente $a \not| b$) diremo che b è divisibile per a (rispettivamente b non è divisibile per a) oppure che b è multiplo di a (rispettivamente b non è multiplo di a).

Esempio 154. Ad esempio $2 \mid 100$ ($100 = 2 \cdot 50$), $2 \mid -60$, $5 \mid 125$, $3 \not| 100$.

Osservazione 56. $\forall a \in \mathbb{Z}$ e per ogni $c \in \mathbb{Z}$ si ha che $a \mid ca$: ogni numero a divide un suo multiplo ca.

Osservazione 57. Sia $a \in \mathbb{Z}$, se $a \mid 1$, allora esiste un intero $c \in \mathbb{Z}$ tale che $1 = a \cdot c$. Ma siamo in $\mathbb{Z}$ quindi o $a = c = 1$ oppure $a = c = -1$. Quindi $a = \pm 1$. I divisori di 1 in $\mathbb{Z}$ sono solo 1 e -1.

Osservazione 58. Per ogni $a \in \mathbb{Z}$ si ha $a \mid 0$. Infatti, $a \mid 0$ se esiste un intero $c \in \mathbb{Z}$ tale che $0 = a \cdot c$. Basta prendere $c = 0$.

Osservazione 59. Al contrario $0 \mid a$ se esiste un intero $c \in \mathbb{Z}$ tale che $a = 0 \cdot c$. È possibile solo se $a = 0$.

Osservazione 60. Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Se $a \mid b$ e $b \mid a$ allora $a = \pm b$. In tal caso, a e b si dicono *associati*.

Dimostrazione: se $a \mid b$ allora $\exists h \in \mathbb{Z}$ tale che $b = ha$. Se $b \mid a$ allora $\exists t \in \mathbb{Z}$ tale che $a = tb$.

Allora $b = ha = htb$, che implica $b - htb = 0$. Quindi $b(1 - ht) = 0$ e poiché $b \neq 0$, possiamo concludere $1 - ht = 0$, ovvero $1 = ht$. Come visto nell'Osservazione 57, questo implica $h = t = 1$ oppure $h = t = -1$, ovvero $a = b$ oppure $a = -b$.

Osservazione 61. Se $a \mid b$ allora $\forall t \in \mathbb{Z}$ si ha $at \mid bt$. Infatti, se $a \mid b$ allora esiste un intero $c \in \mathbb{Z}$ tale che $b = a \cdot c$. Allora $bt = at \cdot c$ e quindi $at \mid bt$.

Esempio 155. $2 \mid 4$ quindi $200 \mid 400$, infatti $2 \cdot 100 \mid 4 \cdot 100$. Oppure $2 \cdot 25 = 50 \mid 100 = 4 \cdot 25$.

Il prossimo risultato è di fondamentale importanza e lo useremo molto spesso.

Teorema 6. *Siano $a, b, c, \in \mathbb{Z}$ se $c \mid a$ e $c \mid b$ allora $\forall x, y, \in \mathbb{Z}$ si ha $c \mid xa+yb$. Il numero intero $xa + yb$ è detto combinazione lineare di a e b. (Ovvero se un numero divide a e b allora divide ogni loro combinazione lineare).*

Dimostrazione. Per ipotesi $c \mid a$ e $c \mid b$, allora $\exists h \in \mathbb{Z}$ tale che $a = hc$ ed $\exists t \in \mathbb{Z}$ tale che $b = tc$. Allora $\forall x, y \in \mathbb{Z}$ si ha

$$ax + by = hcx + tcy = c(hx + ty)$$

ovvero $c \mid xa + yb$.

Esempio 156. Ad esempio se $c \mid a$ e $c \mid b$, allora $c \mid a-b$, $c \mid -a-b$, $c \mid -a+b$, $c \mid a+b$, $c \mid a - 2b$, etc... .

Teorema 7. *Siano $a, b \in \mathbb{Z}$ numeri interi con $b \neq 0$. Allora esistono e sono univocamente determinati due numeri interi $q, r \in \mathbb{Z}$ tali che*

$$a = bq + r \qquad\qquad e\ 0 \leq r < |b|$$

q è detto quoziente, r è detto resto.

Osservazione 62. Sottolineamo che il resto r non è un intero qualsiasi ma deve soddisfare la richiesta: $0 \leq r < |b|$.

Esempio 157. Consideriamo $a = 36$ e $b = 5$. Allora $36 = 5 \cdot 7 + 1$ e quindi $q = 7$ e $r = 1$.

Dimostrazione. Per i più curiosi la dimostrazione si trova su uno qualunque dei testi consigliati.

Vediamo negli esempi come funziona.

Esempio 158. Se $a = 0$, $b \neq 0$ qualsiasi, allora $a = 0 \cdot b + 0$. Quindi esistono quoziente e resto e si ha $q = r = 0$.

Osservazione 63. Se $b \mid a$ allora $\exists h \in \mathbb{Z}$ con $a = hb$ quindi $q = h$ e $r = 0$.

Esempio 159. Ad esempio $a = 100$ e $b = 20$, Allora $100 = 20 \cdot 5$, quindi $q = 5$ e $r = 0$.

Adesso studiamo degli esempi in tutti i casi possibili.

Esempio 160. CASO 1: $a \geq 0, b > 0$.
Consideriamo $a = 73$ e $b = 5$.
Allora $73 = 5 \cdot 14 + 3$ quindi $q = 14$ e $r = 3$ con $0 \leq 3 < 5$. Divisione come a scuola, il 5 nel 73 è contenuto 14 volte, resto 3.

Esempio 161. CASO 2: $a \geq 0, b < 0$.
Consideriamo $a = 111, b = -5$.
L'idea è di considerare $a = 111$, $b' = 5$. Ora è come nel Caso 1): a e b' sono entrambi positivi.
Allora $111 = 5 \cdot 22 + 1$ e quindi $111 = (-5)(-22) + 1$.
Ne segue che $q = -22$ e $r = 1$ con $0 \leq 1 < |-5|$.

Esempio 162. CASO 3: $a \leq 0, b > 0$.
Consideriamo $a = -82, b = 4$.
L'idea è di considerare $a' = 82$, $b = 4$.
Ora è come nel Caso 1): a' e b sono entrambi positivi.
Allora $82 = 4 \cdot 20 + 2$ con $0 \leq 2 < |4|$
e quindi
$-82 = 4 \cdot (-20) - 2$.
Non va bene cosi!! Perchè non è vero che il resto è positivo: $0 \leq -2 < |4|$ falso!
Aggiungiamo e togliamo -4. Così da ottenere
$-82 = 4 \cdot (-21) + 2$ con $0 \leq 2 < |4|$.

Esempio 163. CASO 4: $a \leq 0, b < 0$.

Consideriamo $a = -97, b = -6$.

L'idea è di considerare $a' = 97, b' = 6$. Ora è come nel Caso 1): a' e b' sono entrambi positivi.

Ne segue che $97 = 6 \cdot 16 + 1$ con $0 \leq 1 < |6|$

e quindi

$-97 = (-6) \cdot 16 - 1$.

Non va bene così, perchè non è vero che $0 \leq -1 < |-6|$. Aggiungiamo e togliamo 6 e otteniamo

$-97 = (-6) \cdot 17 + 5$ con $0 \leq 5 < |-6|$.

Esercizio 37. Fare: $a = 97, b = 8; a = -57, b = 5$.

10.2. **Massimo Comun Divisore.**

Definizione 48. (MASSIMO COMUN DIVISORE) Siano $a, b \in \mathbb{Z}$ non entrambi nulli[11]. *Un massimo comun divisore* tra i due interi a e b è un intero $d \in \mathbb{Z}$ tale che

(1) $d \mid a$ e $d \mid b$ (d divide a e b);

(2) $\forall d' \in \mathbb{Z}$, se $d' \mid a$ e $d' \mid b$ allora $d' \mid d$ (massimo divisore).

Esempio 164. Consideriamo $a = 18$ e $b = 12$. Allora $3 \mid 18$ e $3 \mid 12$ ma anche $6 \mid 18$ e $6 \mid 12$. Quindi 6 è un massimo comun divisore.

Ma anche $-6 \mid 18$ e $-6 \mid 12$. (Notare che $-6 \mid 6$ e $6 \mid -6$).

Esempio 165. Consideriamo $a = 32$ e $b = 20$. Allora $4 \mid 32$ e $4 \mid 20$ ma anche $-4 \mid 32$ e $-4 \mid 20$. Quindi 4 e -4 sono un massimo comun divisore.

Osservazione 64. Se d è un massimo comun divisore per a e b allora anche $-d$ lo è e sono gli unici interi che soddisfano la Definizione 48 di massimo comun divisore. Infatti, se d' e d'' sono entrambi massimo comun divisore, allora, per la (2) di Definizione 48, si ha che $d' \mid d''$ e $d'' \mid d'$. Quindi d e d' sono associati allora $d' = \pm d''$ (Osservazione 60).

Definizione 49. (MCD) Per convenzione **il** *massimo comun divisore* tra due interi a e b, non entrambi nulli, è il massimo comun divisore positivo e si indica $MCD(a, b)$. È unico!!

Prima di studiare un metodo per la sua determinazione, studiamo alcune proprietà.

PROPRIETÀ di MCD

(1) Se $a \neq 0$ allora $MCD(a, 0) = \mid a \mid$; perchè $|a| \mid 0$ e divide a.

(2) $MCD(a, b) = MCD(b, a)$.

(3) $MCD(a, b) = MCD(-a, b) = MCD(a, -b) = MCD(-a, -b)$.

(4) Se $b \mid a$ allora $MCD(a, b) = |b|$.

(5) Se $d = MCD(a, b)$. Allora $MCD(\frac{a}{d}, \frac{b}{d}) = 1$.

Esempio 166. Ad esempio $6 = MCD(12, 18)$, allora $MCD(\frac{12}{6}, \frac{18}{6}) = MCD(2, 3) = 1$.

Osservazione 65. Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Il numero 1 divide ogni intero in $\mathbb{Z}$, quindi $1 \mid a$ e $1 \mid b$. Pertanto, il $MCD(a, b)$ è "almeno"1.

[11]Escludiamo dalla definizione il caso in caso in cui $a = b = 0$. Ogni numero divide 0 e quindi non riusciamo a pensarne uno più grande di tutti. In realtà la definizione in (2) richiede più grande per la divisibilità ed è soddisfatta da 0. Quindi potremmo definire $MCD(0, 0) = 0$

Definizione 50. (COPRIMI) Due interi $a, b \in \mathbb{Z}$ non entrambi nulli sono *coprimi* se $MCD(a, b) = 1$.

Esempio 167. Ad esempio 2 e 7 oppure 11 e 144.

10.3. **Algoritmo di Euclide.**

Teorema 8. *Per ogni coppia di interi $a, b \in \mathbb{Z}$ non entrambi nulli esiste il MCD(a,b) e può essere espresso come combinazione lineare di a e b, ovvero esistono $x, y \in \mathbb{Z}$ tali che*

$$MCD(a, b) = ax + by.$$

Questa equazione si chiama identità di Bézout [12].

La dimostrazione è costruttiva e fornisce un metodo per determinare il Massimo Comun Divisore e l'identità di Bézout.

Dimostrazione. La dimostrazione si basa sull' *algoritmo di Euclide*[13] (algoritmo delle divisioni successive) che fornisce una dimostrazione costruttiva dell'esistenza del MCD (esiste e ci dice come si calcola!).

Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Per le proprietà viste del MCD, possiamo assumere $a, b \geq 0$.

Se uno dei due interi è zero, ad esempio $b = 0$, abbiamo fatto: perchè $MCD(a, 0) = a$ $(= a \cdot 1 + 0 \cdot 1)$.

Se $a = b$ allora $MCD(a, a) = a (= a \cdot 1 + a \cdot 0)$

Quindi possiamo supporre che entrambi gli interi a e b siano non nulli, positivi e diversi.

Quindi, basta studiare il caso $a, b \in \mathbb{Z}$ con $a > b > 0$.

Idea su cui si basa l'algoritmo: fare le divisioni successive.

Per ogni $a, b \in \mathbb{Z}$ con $a > b > 0$, possiamo dividere a per b e quindi esistono e sono univocamente determinati due interi q_1 ed r_1 tali che

$$\exists q_1, r_1 \in \mathbb{Z} \qquad a = bq_1 + r_1 \qquad \text{e} \qquad 0 \leq r_1 < |b| = b.$$

Se $r_1 = 0$ allora $a = bq$ ovvero $b \mid a$ e quindi $MCD(a, b) = b$. Quindi esiste il $MCD(a, b)$.

Se $r_1 \neq 0$ continuiamo con le divisioni e dividiamo b per r_1: quindi

$$\exists q_2, r_2 \in \mathbb{Z} \qquad b = r_1 q_2 + r_2 \qquad \text{e} \qquad 0 \leq r_2 < |r_1| = r_1.$$

Se $r_2 \neq 0$ continuiamo

$$\exists q_3, r_3 \in \mathbb{Z} \qquad r_1 = r_2 q_3 + r_3 \qquad \text{e} \qquad 0 \leq r_3 < r_2$$

$$\dots$$

$$\exists q_{n-1}, r_{n-1} \in \mathbb{Z} \qquad r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \qquad \text{e} \qquad 0 \leq r_{n-1} < r_{n-2}$$

$$\exists q_n, r_n \in \mathbb{Z} \qquad r_{n-2} = r_{n-1} q_n + r_n \qquad \text{e} \qquad 0 \leq r_n < r_{n-1}$$

$$\exists q_{n+1}, r_{n+1} = 0 \in \mathbb{Z} \qquad r_{n-1} = r_n q_{n+1}.$$

I resti delle divisioni successive sono tali che

$$b = |b| > r_1 > r_2 > \cdots > r_n \geq 0,$$

quindi è una successione strettamente decrescente di numeri positivi e ad un certo punto deve essere zero. Se $r_{n+1} = 0$. Allora r_n è l'ultimo resto non nullo. Allora $r_n = MCD(a, b)$.

Dimostriamo che l'ultimo resto non nullo r_n è il $MCD(a, b)$.

1) r_n è divisore (procedendo dal basso verso l'alto):

Infatti, r_n divide r_{n-1}.

[12] Étienne Bézout, matematico francese 1730-1783.

[13] Euclide, matematico greco vissuto intorno al 300 ac, autore degli: Elementi di Euclide che sono 13 libri.

Dalla "riga"sopra r_n dividendo r_n e r_{n-1} allora deve dividere r_{n-2}, che è combinazione lineare di r_n e r_{n-1} (Teorema 6).

Dalla "riga"sopra r_n dividendo r_{n-1} e r_{n-2} allora deve dividere r_{n-3}.

Alla fine, r_n divide r_2 e r_1 allora divide b.

Inoltre, r_n divide b e r_1 allora divide a.

Quindi, r_n divide a e b.

2) r_n è massimo comun divisore (procedendo dall'alto verso il basso).

Se $d \mid a$ e $d \mid b$, allora $d \mid r_1$, dato che r_1 è combinazione lineare di a e b (Teorema 6).

Dalla "riga"sotto, $d \mid b$ e $d \mid r_1$, allora $d \mid r_2$.

Procedendo verso il basso, $d \mid r_{n-2}$ e $d \mid r_{n-1}$, allora $d \mid r_n$.

Quindi abbiamo dimostrato che r_n, che è l'ultimo resto diverso da zero, è il $MCD(a, b)$.

Infine, per ottenere l'identità di Bézout: procediamo dall'alto verso il basso:

$$a = bq_1 + r_1 \qquad \Longrightarrow \qquad r_1 = a - bq_1$$

$$b = r_1q_2 + r_2 \qquad \Longrightarrow \qquad r_2 = b - r_1q_2 = b - q_2(a - bq_1)$$

$$\dots$$

Dalla prima equazione otteniamo $a - bq_1 = r_1$; sostituiamo nella seconda,quindi r_2 combinazione di a e b. Sostituiamo nella terza al posto di r_1 e r_2 e otteniamo r_3 come combinazione di a e b e così fino a r_n.

Esempio 168. Consideriamo $a = 200$ e $b = 16$. Trovare il MCD tra 200 e 16 e determinare l'identità di Bézout.

Sketch:

Prima cosa 16 divide 200? No. Quindi applichiamo l'algoritmo di Euclide.

$200 = 16 \cdot 12 + 8$, con $q_1 = 12$ e $r_1 = 8$;

$16 = 8 \cdot 2 + 0$ dove $r_2 = 0$.

Allora $r_1 = 8$ è l'ultimo resto non nullo e quindi è il MCD. Infatti, 8 divide 16 e 8 divide $200 = 25 \cdot 8$.

Dall'equazione $200 = 16 \cdot 12 + 8$, concludiamo che

$$8 = 200 - 16 \cdot 12 = a \cdot 1 + b \cdot (-12),$$

che è l'identità di Bézout.

Esercizio 38. Consideriamo $a = 420$ e $b = 11$; trovare il MCD e determinare l'identità di Bézout.

Sketch:

$420 = 11 \cdot 38 + 2$ con $b = 11$ e $r = 2$;

$11 = 2 \cdot 5 + 1$ con $r = 1$;

$2 = 2 \cdot 1 + 0$.

Ne segue che $MCD(420, 11) = 1$.

Inoltre, dall'equazione $420 = 11 \cdot 38 + 2$, segue che $2 = a - 38b$ e sostituendo in $11 = 2 \cdot 5 + 1$, otteniamo che

$$1 = 11 - 2 \cdot 5 = b - 5(a - 38b) = b - 5a + 38 \cdot 5b = -5 \cdot a + (38 \cdot 5 + 1)b = -5 \cdot a + 191 \cdot b.$$

Quindi l'identità di Bézout è: $1 = -5 \cdot a + 191 \cdot b = (-5) \cdot 420 + 191 \cdot 11$.

Infatti, $(-5) \cdot 420 + 191 \cdot 11 = -2100 + 2101 = 1$.

Esercizio 39. Consideriamo $a = -3110$ e $b = -580$; trovare il MCD e determinare l'identità di Bézout.

Sketch: Applichiamo l'algoritmo di Euclide.

$3110 = 580 \cdot 5 + 210$

$580 = 210 \cdot 2 + 160$

$210 = 160 \cdot 1 + 50$

$160 = 50 \cdot 3 + 10$

$50 = 10 \cdot 5$

Ne segue che 10=MCD(3110,580)=MCD(-3110,-580).
Inoltre,
$210 = a - 5b$
$160 = b - 2 \cdot 210 = b - 2a + 10b = -2a + 11b$
$50 = 210 - 160 = (a - 5b) - (-2a + 11b) = 3a - 16b$
$10 = 160 - 3 \cdot 50 = (-2a + 11b) - 3 \cdot (3a - 16b) = (-11) \cdot a + 59 \cdot b.$
Infatti, $(-11) \cdot a + 59 \cdot b = (-11)(3110) + 59(580) = -34210 + 34220 = 10.$
Quindi l'identità di Bézout è: $10 = (-11) \cdot a + 59 \cdot b = (-11)(3110) + 59(580).$
Infine, poiché avevamo: $a = -3110$ e $b = -580$, otteniamo:

$$10 = (-3110)(-11) + (-580)(-59).$$

Esercizio 40. Determinare $MCD(230, 8) = 2$; $MCD(170, 370) = 10$; $MCD(462, 702) = 6$. Inoltre, esprimere l'MCD come combinazione lineare.

10.4. **Minimo Comune Multiplo.**

Definizione 51. (MINIMO COMUNE MULTIPLO) Siano $a, b \in \mathbb{Z} \setminus \{0\}$. *Un minimo comune multiplo* tra i due interi a e b è un intero $m \in \mathbb{Z}$ tale che

(1) $a \mid m$ e $b \mid m$ (m multiplo di a e b);

(2) $\forall m' \in \mathbb{Z}$ se $a \mid m'$ e $b \mid m'$ allora $m \mid m'$ (m minimo multiplo).

Osservazione 66. Anche un minimo comune multiplo è definito a meno del segno, ovvero se m è un minimo comune multiplo tra a e b anche $-m$ lo è. Per convenzione *il minimo comune multiplo* tra a e b si indica con $mcm(a, b)$ ed è quello positivo.

Possiamo applicare quanto detto per il Massimo Comun Divisore per calcolare il Minimo Comune Multiplo.

Osservazione 67. Per ogni $a, b \in \mathbb{Z} \setminus \{0\}$, esiste sempre $mcm(a, b)$ ed inoltre

$$ab = MCD(a, b) \cdot mcm(a, b) \Longrightarrow mcm(a, b) = \frac{ab}{MCD(a, b)}$$

Quindi esiste sempre $mcm(a, b)$.

11. Equazioni diofantee

Lo Stato e la Chiesa cattolica sono, ciascuno nel proprio ordine, indipendenti e sovrani.
I loro rapporti sono regolati dai Patti Lateranensi.
Le modificazioni dei Patti, accettate dalle due parti, non richiedono
procedimento di revisione costituzionale.

Dati due interi $a, b \in \mathbb{Z}$ non entrambi nulli, abbiamo definito il $MCD(a, b)$ ed abbiamo dimostrato (Teorema 8) che esistono interi $x, y \in \mathbb{Z}$ tale che (identità di Bézout)

$$MCD(a, b) = ax + by$$

(Il MCD serve per trovare le soluzioni alle equazioni lineari).

Definizione 52. (EQUAZIONE DIOFANTEA[14]) Una equazione della forma

$$ax + by = c$$

con $a, b, c \in \mathbb{Z}$ interi della quale cerchiamo soluzioni intere (ovvero $x, y \in \mathbb{Z}$) è detta *equazione diofantea*. Una soluzione è una coppia $x_0, y_0 \in \mathbb{Z}$, tale che $ax_0 + by_0 = c$.

Osservazione 68. Noi consideriamo equazioni diofantee con a e b non nulli.

Osservazione 69. Notiamo $ax + by = c$ implica $by = c - ax$ e se $b \neq 0$ allora $y = \frac{c-ax}{b}$, ovvero cerchiamo i punti a coordinate intere della retta. Questi punti non è detto che esistano.

Esempio 169. Se $c = 0$ allora l'equazione diofantea $ax + by = 0$ ammette sempre soluzione. Infatti, $x_0 = -b$ e $y_0 = a$ è soluzione, oppure $x_0 = 0$ e $y_0 = 0$.

Esempio 170. $10x + 7y = 0$, se $x_0 = -7$ e $y_0 = 10$ è soluzione, ma anche $x_0 = 7$ e $y_0 = -10$, oppure $x_0 = 0, y_0 = 0$.

Esempio 171. $3x + 6y = 6$, ammette soluzioni (2,0) oppure (0,1) oppure (4,-1).

Esempio 172. $2x + 4y = 3$, non ammette mai soluzione, visto che a sinistra è sempre un numero pari e a destra dispari.

Come possiamo capire se esistono soluzioni? E soprattutto come possiamo trovarle?

Teorema 9. *Dati $a, b, c \in \mathbb{Z}$ l'equazione diofantea*

$$ax + by = c$$

ammette soluzioni (numeri interi) se e soltanto se $MCD(a, b) \mid c$.

La dimostrazione fornisce un metodo costruttivo per determinare le soluzioni.

Dimostrazione. ($\Longrightarrow$) Se $ax + by = c$ ammette soluzione allora $MCD(a, b) \mid c$.

Supponiamo $ax + by = c$ ammette soluzioni: ovvero esistono $x_0, y_0 \in \mathbb{Z}$ tale che $ax_0 + by_0 = c$. Sia $d = MCD(a, b)$ allora $d \mid a$ e $d \mid b$ allora, per la Teorema 6, d divide la combinazione lineare $ax_0 + by_0 = c$, ovvero $d \mid c$.

($\Longleftarrow$) Se $d = MCD(a, b) \mid c$ allora $ax + by = c$ ammette soluzione.

Per l'Identità di Bézout, se $d = MCD(a, b)$ allora esistono $\alpha, \beta \in \mathbb{Z}$ tale che

$$d = a\alpha + b\beta. \tag{1}$$

Inoltre, $d = MCD(a, b) \mid c$ quindi $\exists k \in \mathbb{Z}$ tale che $c = dk$. Allora moltiplichiamo l'Equazione (1) per h e otteniamo $c = dk = a\alpha k + b\beta k$ ovvero $x_0 = \alpha k$ e $y_0 = \beta k$ è soluzione. (È questo il metodo per trovarle!)

[14]Il nome diofantea è dovuto a Diofanto di Alessandria d'Egitto, matematico vissuto nel III secolo. Nella sua opera Arithmetica, si è occupato anche di soluzioni di equazioni.

Esempio 173. Nell' Esempio 171 si ha $MCD(3,6) = 3 \mid 6$; mentre nell'Esempio 172 $MCD(2,4) = 2 \not| 3$.

Come possiamo trovare tutte le soluzioni?

Teorema 10. *Siano $a, b, c \in \mathbb{Z}$ e sia (x_0, y_0) una soluzione dell'equazione diofantea*

$$ax + by = c,$$

allora tutte e sole le soluzioni intere di tale equazione sono

$$(x, y) = (x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) \qquad \forall\ t \in \mathbb{Z}, \tag{2}$$

dove $d = MCD(a, b)$.(Quindi se esiste una soluzione allora ce ne sono infinite!)

Dimostrazione. Verifichiamo solo che le coppie (x, y) descritte dall'Equazione (2) sono soluzioni. Per ipotesi (x_0, y_0) è soluzione quindi $ax_0 + by_0 = c$. Allora

$$a(x_0 - \frac{b}{d}t) + b(y_0 + \frac{a}{d}t) = ax_0 - \frac{ab}{d}t + by_0 + \frac{ba}{d}t = ax_0 + by_0 = c.$$

Osservazione 70. Se esiste una soluzione di una equazione diofantea, allora esistono infinite soluzioni.

Osservazione 71. Nella formula dell'Equazione (2), il numero t appartiene a $\mathbb{Z}$ quindi la formula è equivalente alla formula:

$$(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \qquad \forall\ t \in \mathbb{Z}. \tag{3}$$

Esempio 174. Consideriamo $3x + 6y = 6$; abbiamo visto che (2,0) è soluzione. Allora l'Equazione (2) afferma che per ogni $t \in \mathbb{Z}$ tutte e sole le soluzioni sono:

$$(x, y) = (x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) = (2 - \frac{6}{3}t, 0 + \frac{3}{3}t) = (2 - 2t, t) \qquad \forall\ t \in \mathbb{Z}.$$

Infatti, ritroviamo (0,1), (4,-1) ma scopriamo anche che per $t = 100$ si ha che (-198, 100) è soluzione.

Esempio 175. Consideriamo $10x + 7y = 0$. Abbiamo visto che $x_0 = 0, y_0 = 0$ è soluzione. Allora

$$(x, y) = (x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) = (-7t, 10t) \qquad \forall\ t \in \mathbb{Z}$$

sono tutte e sole le soluzioni. Infatti, ritroviamo $x_0 = -7$ e $y_0 = 10$ (per $t = 1$), ma anche $x_0 = 7$ e $y_0 = -10$ (per $t = -1$).

Esempio 176. Consideriamo $18x + 9y = 81$.

Il $MCD(18, 9) = 9$ e $9 \mid 81$ quindi esistono soluzioni.

Ad esempio $(x_0, y_0) = (0, 9)$ è soluzione quindi tutte le soluzioni sono

$$(x, y) = (x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) = (0 - \frac{9}{9}t, 9 + \frac{18}{9}t) = (-t, 9 + 2t) \qquad \forall\ t \in \mathbb{Z}.$$

Esercizio 41. Risolvere se possibile la seguente equazione diofantea indicandone tutte le soluzioni

$$585x + 165y = 15.$$

Sketch: Prima cosa trovare $MCD(585, 165)$.

$585 = 165 \cdot 3 + 90$,

$165 = 90 \cdot 1 + 75$,

$90 = 75 \cdot 1 + 15$

$75 = 15 \cdot 5$.

Quindi $MCD(585, 165) = 15$. Inoltre $15 \mid 15$ e pertanto l'equazione diofantea ammette soluzioni. Usiamo l'identità di Bézout

$90 = a - 3b$
$75 = b - 90 = 4b - a$
$15 = 90 - 75 = a - 3b - 4b + a = 2a - 7b = 2 \cdot 585 - 7 \cdot 165$;
ovvero $x_0 = 2$ e $y_0 = -7$ sono soluzioni e tutte le altre sono

$$(x, y) = (x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) = (2 - \frac{165}{15}t, -7 + \frac{585}{15}t) = (2 - 11t, -7 + 39t) \qquad \forall\, t \in \mathbb{Z}.$$

Osservazione 72. Dobbiamo risolvere $ax + by = c$ tale che $0 \neq d = MCD(a, b) \mid c$ allora dividiamo tutto per d, infatti $d \mid a$, $d \mid b$ e $d \mid c$ e risolviamo l'equazione ottenuta che è piu facile e le soluzioni sono le stesse.

È una cosa che abbiamo sempre fatto. Formalmente, se $a = a_0 d, b = b_0 d$ e $c = c_0 d$, consideriamo

$$ax + by = c \qquad \Longleftrightarrow \qquad a_0 dx + b_0 dy = c_0 d \qquad \Longleftrightarrow \qquad a_0 x + b_0 y = c_0.$$

Esercizio 42. Risolvere

$$585x + 165y = 15.$$

Possiamo dividere per 15, $39x + 11y = 1$,
$39 = 11 \cdot 3 + 6$
$11 = 6 \cdot 1 + 5$
$6 = 5 \cdot 1 + 1$. Quindi
$6 = 39 - 11 \cdot 3 \qquad 5 = 11 - 6 = 11 \cdot 4 - 39 \qquad 1 = 6 - 5 = 2 \cdot 39 - 7 \cdot 11.$
Ne segue che una soluzione è $(x_0, y_0) = (2, -7)$ e tutte e sole le soluzioni sono
$(x, y) = (2 - 11t, -7 + 39t) \qquad \forall\, t \in \mathbb{Z}$ (esattamente come nell'Esercizio 41).

Osservazione 73. Analogamente a quanto detto nell'Osservazione 72, se un intero k divide i coefficienti a, b e c di una equazione diofantea $ax + by = c$, possiamo dividere tutto per k e risolvere una equazione diofantea equivalente ma più semplice.

Esercizio 43. Risolvere se possibile la seguente equazione diofantea indicandone tutte le soluzioni

$$396x + 156y = 24.$$

Dividiamo per 2: 198x+ 78y=12; dividiamo ancora per 2: 99 x+ 39y=6; e dividiamo per 3: 33x+13y=2.

Adesso risolviamo questa equazione 33x+13y=2 (come se avessimo diviso per 12 l'equazione di partenza).

Il MCD(33,13)=1 quindi ammette soluzioni.

Facciamo le divisioni successive:
$33 = 2 \cdot 13 + 7$;
$13 = 1 \cdot 7 + 6$;
$7 = 1 \cdot 6 + 1$.

Quindi, sia $a = 33$ e $b = 13$, abbiamo
$7 = 33 - 13 \cdot 2 = a - 2b$;
$6 = 13 \cdot 3 - 7 = b - (a - 2b) = 3b - a$;
$1 = 7 - 6 = a - 2b - (3b - a) = a - 2b - 3b + a = 2a - 5b$.

Quindi, $1 = 2a - 5b$; ne segue che, $2 = 4a - 10b = 33 \cdot (4) + 13 \cdot (-10)$.

In conclusione, una soluzione è $x_0 = 4$ e $y_0 = -10$ e quindi tutte e sole le soluzioni sono $(x, y) = (4 - 13t, -10 + 33t) \qquad \forall\, t \in \mathbb{Z}$.

Esercizio 44. Risolvere se possibile la seguente equazione diofantea indicandone tutte le soluzioni

$$396x + 156y = 12. \qquad 385x + 33y = 143 \qquad 20x + 144y = 99 \qquad 819x + 221y = 26.$$

11.1. **I numeri primi.**

Definizione 53. (PRIMO) Un numero $p \in \mathbb{Z}$ $p \neq 0, 1, -1$ è un numero *primo* se ogni volta che p divide il prodotto di due numeri interi allora p divide uno dei due fattori, ovvero

$$\forall a, b \in \mathbb{Z} \text{ tale che } p \mid ab \Longrightarrow p \mid a \text{ oppure } p \mid b$$

Equivalentemente $p \in \mathbb{Z}$ $p \neq 0, 1, -1$ è primo se p è divisibile solo per ± 1 e $\pm p$.

Osservazione 74. Se p è primo allora $\forall a, b \in \mathbb{Z}$ tale che $p \mid ab$, se $p \not| a$ si ha che $p \mid b$.

Se p è primo e $p = ab$ allora $a = \pm 1$ e $b = \pm p$ o viceversa $a = \pm p$ e $b = \pm 1$.

Se n non è primo allora $\exists a, b \in \mathbb{Z}$ con $1 < |a|, |b| < |n|$ e $n = ab$.

Osservazione 75. Sia $n \geq 2$, se n non è primo, allora esistono $1 < a, b < n$ tale che $n = a \cdot b$. Allora o $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$. Infatti se non fosse vero, ovvero se entrambi $a > \sqrt{n}$ e $b > \sqrt{n}$. Allora $n = ab > \sqrt{n} \cdot \sqrt{n} = n$ ovvero $n > n$. Questo è assurdo.

Teorema 11. *(TEOREMA FONDAMENTALE DELL'ARITMETICA) Ogni numero intero n con $n \neq 0, 1, -1$ può essere scritto come prodotto di un numero finito di numeri primi p_j ovvero*

$$n = \pm p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$$

dove i p_j sono tutti primi distinti e gli esponenti h_j sono tutti strettamente positivi ($h_j > 0$).

La scrittura è detta: fattorizzazione di n come prodotto di potenze di primi distinti. Inoltre, tale fattorizzazione è unica, ovvero per ogni altra fattorizzazione di n:

$$n = \pm q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$$

dove q_i sono tutti primi distinti e $k_i > 0$, allora il numero di fattori è lo stesso ($t = s$) ed i primi q_i coincidono con i primi p_j a meno dell'ordine (e del segno).

Dimostrazione. Solo esistenza: vogliamo dimostrare che ogni $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ ammette fattorizzazione. Basta dimostrare per ogni $n \in \mathbb{N}$ con $n \geq 2$ la seguente proposizione:

$P(n)$: il numero n ammette fattorizzazione in primi.

Infatti, per i numeri interi negativi possiamo mettere il segno meno.

BASE INDUZIONE: Dimostrare che P(2) è vera.

L'intero $n = 2$ ammette fattorizzazione in primi: $n = 2 = 2^1$. Allora P(2) è vera.

PASSO INDUTTIVO: Dimostrare per ogni $k \geq 2$ che $P(h)$ vera $\forall h$ tale che $2 \leq h \leq k$ (esplicitamente: $P(2), P(3), \ldots, P(k)$ vere) $\Longrightarrow P(k+1)$ vera.

Ovvero stiamo assumendo che ogni intero h con $2 \leq h \leq k$ ammette fattorizzazione e vogliamo dimostrare che anche il numero intero $k+1$ ammette fattorizzazione.

Se $k+1$ è primo abbiamo già la fattorizzazione, se non è primo per l'Osservazione 74, esistono $a, b \in \mathbb{Z}$ con $1 < a, b < k+1$ e $k+1 = ab$. Per ipotesi induttiva, esiste la fattorizzazione in potenze di primi distinti per a e b (dato che $P(a)$ e $P(b)$ sono vere). Allora

$$a = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s} \qquad \text{e} \qquad b = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t},$$

quindi

$$k+1 = ab = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s} \cdot q_1^{k_1} q_2^{h_2} \cdots q_t^{k_t}.$$

Raccogliamo i primi uguali e sommiamo gli esponenti e abbiamo ottenuto la fattorizzazione di $k+1$. Quindi $P(k+1)$ è vera. Per il principio di induzione, segue che $P(n)$ è vera per ogni $n \geq 2$.

Esempio 177. Consideriamo $n = 100$. Allora, $100 = 10 \cdot 10$, $10 = 2 \cdot 5$.

Quindi $100 = 2 \cdot 5 \cdot 2 \cdot 5 = 2^2 \cdot 5^2$.

Consideriamo $n = 3600$. Allora, $n = 36 \cdot 100$; inoltre, si ha che $36 = 6^2 = 2^2 \cdot 3^2$ e $100 = 2^2 \cdot 5^2$.

Quindi $3600 = 2^2 \cdot 3^2 \cdot 2^2 \cdot 5^2 = 2^4 \cdot 3^2 \cdot 5^2$.

A cosa può servire la fattorizzazione? A trovare i divisori e a trovare il MCD.

Osservazione 76. Se $n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ allora i divisori di n a meno del segno sono della forma $d = p_1^{j_1} p_2^{j_2} \cdots p_s^{j_s}$ con $0 \leq j_i \leq h_i$ per ogni $i = 1, \ldots, s$.

Quanti sono a meno del segno? Quante scelte abbiamo per gli esponenti j_i? Ogni j_i può essere scelto in $h_i + 1$ modi, infatti $0 \leq j_i \leq h_i$. Quindi, a meno del segno, esistono

$$(h_1 + 1) \cdot (h_2 + 1) \cdot \cdots \cdot (h_s + 1)$$

divisori di n. Se vogliamo considerare anche il segno + o−, allora ci sono

$$2(h_1 + 1) \cdot (h_2 + 1) \cdot \cdots \cdot (h_s + 1)$$

divisori di n.

Esempio 178. Consideriamo $n = 3600 = 2^4 \cdot 3^2 \cdot 5^2$, quanti sono i divisori positivi? I divisori positivi sono della forma $2^x \cdot 3^y \cdot 5^z$ dove $x \in \{0, 1, 2, 3, 4\}$, $y \in \{0, 1, 2\}$ e $z \in \{0, 1, 2\}$. Quindi abbiamo 5 possibili scelte per la x, 3 possibili scelte per la y e 3 scelte per la z, quindi: ci sono $5 \cdot 3 \cdot 3 = 45$ divisori positivi.

Esempio 179. Consideriamo $n = 2^2 \cdot 3^2 \cdot 5$, quanti sono i divisori positivi? I divisori positivi sono della forma $2^x \cdot 3^y \cdot 5^z$ dove $x \in \{0, 1, 2\}, y \in \{0, 1, 2\}$ e $z \in \{0, 1\}$. Quindi abbiamo 3 possibili scelte per la x, 3 possibili scelte per la y e 2 scelte per la z, quindi: ci sono $3 \cdot 3 \cdot 2 = 18$ divisori positivi.

Esempio 180. Consideriamo $n = 18 = 2 \cdot 9 = 2 \cdot 3^2$. I divisori positivi sono $2 \cdot 3 = 6$ e sono della forma $2^x \cdot 3^y$ dove $x \in \{0, 1\}$ e $y \in \{0, 1, 2\}$. Infatti abbiamo: $1, 2, 3, 6, 9, 18$.

La fattorizzazione serve anche per trovare il massimo comune divisore.

Osservazione 77. Dati a e b con

$$a = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s} \qquad \text{e} \qquad b = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$$

allora il $MCD(a, b)$ ha come fattorizzazione in primi il massimo fattor comune, ovvero i primi in comune con il più piccolo esponente (che è il piu grande esponente comune).

Esempio 181. Siano $a = 3600 = 2^4 \cdot 3^2 \cdot 5^2$ e $b = 3^6 \cdot 5^{11} \cdot 7^2$.
Allora $MCD(a, b) = 3^2 \cdot 5^2$.

Esempio 182. Siano $a = 2^3 \cdot 3^2 \cdot 5^3 \cdot 11^2$ e $b = 2^3 \cdot 3^6 \cdot 5^{11} \cdot 11^2$.
Allora $MCD(a, b) = 2^3 \cdot 3^2 \cdot 5^3 \cdot 11^2 = a$ (infatti $a \mid b$).

Teorema 12. *I numeri primi sono infiniti.*

Dimostrazione. Suppponiamo per assurdo che i numeri primi siano finiti. Siano $p_1, p_2, \ldots, p_s$ tutti i numeri primi.
Sia ora $n = p_1 \cdot p_2 \cdots p_s + 1$, il prodotto di tutti i numeri primi a cui sommiamo 1.

Osserviamo che nessuno dei primi p_i divide n, altrimenti se un p_i dividesse n allora, dato che divide il suo multiplo $p_i \mid p_1 \cdot p_2 \cdots p_i \cdots p_s$, dovrebbe dividere la combinazione lineare $n - p_1 \cdot p_2 \cdots p_s = 1$. Questo implicherebbe che $p_i \mid 1$, ovvero $p_i = 1$ oppure -1 che è assurdo dato che p_i è un numero primo. Quindi $p_i \not| n$ per ogni $i = 1, \ldots, s$.

Per il Teorema fondamentale dell'aritmetica (Teorema 11) n è primo oppure oppure può essere scritto come prodotto di due o più primi. Quindi esiste un numero primo che non è nella lista. (Questo numero è n oppure un fattore primo di n). Questo è un assurdo in quanto avevamo elencato tutti i numeri primi.

Osservazione 78. Il teorema precedente dimostra che esistono infiniti numeri primi, ma non è una dimostrazione costruttiva nel senso che non fornisce un metodo costruttivo per trovarli tutti. Trovare i numeri primi grandi è un problema complesso, fortunatamente è molto complesso. Ci sono molte congetture legate ai numeri primi, alla loro frequenza, alla loro distribuzione, ai primi gemelli etc.

Abbiamo dimostrato che esistono infiniti numeri primi. Come possiamo trovarli? Anche questo è un problema molto complesso. Esistono alcuni algoritmi per trovare i numeri primi, diversi tra loro. Descriviamo un metodo noto con il nome di Crivello di Eratostene.[15]

11.2. **Crivello di Eratostene.** Fissato un intero $n \geq 2$, come si possono trovare tutti i numeri primi minori o uguali ad n? Un algoritmo che vediamo si chiama *Crivello di Eratostene.*

Algoritmo:

(1) Scrivere tutti i numeri $\leq n$

(2) Prendere 2, sottolinearlo e cancellare tutti i suoi multipli (diversi da 2).

(3) Prendere 3 (che non è stato cancellato) sottolinearlo e cancellare tutti i suoi multipli (diversi da 3).

(4) Poi sottolineare il prossimo numero non cancellato e cancellare i suoi multipli (diversi da se stesso).

(5) Procedere così fino a $\sqrt{n}$ (basta per l'Osservazione 75).

(6) I numeri sottolineati e quelli non cancellati sono tutti i primi più piccoli di n.

Esempio 183. Applicare il Crivello di Eratostene a $n = 41$.

11.3. **Metodi di Fattorizzazione.** A cosa serve conoscere i numeri primi? Serve per trovare la fattorizzazione di un numero intero n. Per trovare la fattorizzazione, possiamo suppore il numero positivo, se fosse negativo, una volta trovata la fattorizzazione, basta cambiare segno.

In generale, trovare la fattorizzazione di un numero è un problema molto difficile e computazionalmente complesso. Questa non è una disgrazia ma una fortuna: sulla complessità di questo problema si basa la sicurezza informatica e la crittografia.

Ci sono vari algoritmi per trovare la fattorizzazione di un numero, noi descriviamo quello che si basa sul Crivello di Eratostene.

11.3.1. *Metodo di Eratostene.* Sia n un intero maggiore di zero. Con il Crivello di Eratostene troviamo tutti i primi $\leq n$. A questo punto proviamo a dividere n per tutti i primi minori o uguali a $\sqrt{n}$.

Infatti se $n = ab$ allora, per l'Osservazione 75, $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

Se n non è divisibile per i primi minori di $\sqrt{n}$, ovvero se non lo cancelliamo nell'algoritmo di Eratostene, allora n è un numero primo. Se invece lo cancelliamo significa che è multiplo di qualcosa, ovvero troviamo un divisore e quindi $n = ab$, con $1 < a, b < n$. Consideriamo ora a e b e cerchiamo la loro fattorizzazione, etc.

[15]Eratostene di Cirene, matematico greco 275 a.C.- 195 a.C circa.

12. Congruenze modulo n

Tutte le confessioni religiose sono egualmente libere davanti alla legge.
(.....)

Fissiamo $n \in \mathbb{N}$ con $n \geq 2$ e consideriamo la relazione su $A = \mathbb{Z}$

$$\forall\, a, b \in \mathbb{Z} \quad a \mathscr{R} b \iff n \mid a - b.$$

È equivalente a richiedere: $\exists k \in \mathbb{Z}$ tale che $a - b = kn$ se e solo se $a - b$ multiplo di n. Nell'Esercizio 35, abbiamo già dimostrato che $\mathscr{R}$ è una relazione di equivalenza. Questa relazione di equivalenza su $\mathbb{Z}$ si chiama *relazione di congruenza modulo n*.

Se $a \mathscr{R} b$ (e quindi a è equivalente a b) allora diremo che a è *congruo* a b modulo n e scriveremo

$$a \equiv b \pmod{n}.$$

Si usa anche la notazione: $a \equiv_n b$.

Osservazione 79. Si considera $n \geq 2$, perché negli altri casi otteniamo relazioni già note. Se $n = 0$, $0 \mid a - b$ se e solo se $a = b$ e quindi otteniamo la relazione identica su $\mathbb{Z}$ (Osservazione 45).

Se $n = 1$, $1 \mid a - b$ per ogni scelta di a e di b; quindi otteniamo la relazione totale su $\mathbb{Z}$ (Osservazione 45).

Vogliamo studiare le classi di equivalenza e l'insieme quoziente.

Osservazione 80. Sia $a \in \mathbb{Z}$. Dividiamo a per n e otteniamo $a = n \cdot q + r$, con $0 \leq r < n$. Quindi, $a - r = n \cdot q$, ovvero $n \mid a - r$.

Ne segue che $a \mathscr{R} r$ e quindi $a \equiv r \pmod{n}$: **ogni numero intero è congruente modulo n al suo resto nella divisione per n.**

Osservazione 81. Comunque presi r, s tali che $0 \leq r, s < n$. Allora $r \equiv s \pmod{n}$ se e solo se $r = s$. Infatti dire $r \equiv s \pmod{n}$, implica che $n \mid (r - s)$. Dato che $0 \leq r, s < n$ si ha $0 \leq |r - s| < n$. Pertanto $n \mid (r - s)$ se e solo se $r = s$. Questo implica che i resti possibili nella divisione per n sono tutti non equivalenti tra loro.

Osservazione 82. Si può dimostrare che $a \equiv b \pmod{n}$ se e solo se a e b hanno lo stesso resto nella divisione per n.

Nella relazione di congruenza la classe $[a]_{\mathscr{R}}$ si indica con $[a]_{\equiv_n}$ oppure $[a]_n$. Per le osservazioni precedenti, si ha che

$$[a]_n = \{x \in \mathbb{Z} \mid x \mathscr{R} a\} = \{x \in \mathbb{Z} \mid n \mid x - a\} =$$

$$\{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \text{ tale che } x - a = kn\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \text{ tale che } x = a + kn\} = \{a + kn \mid k \in \mathbb{Z}\}$$

$$= \{x \in \mathbb{Z} \mid \ x \text{ e } a \text{ stesso resto nella divisione per } n\ \}.$$

La classe di equivalenza di un elemento è detta *classe resto modulo n* o *classe di congruenza modulo n* .

Inoltre, per l'Osservazione 80, ogni elemento è equivalente al suo resto, quindi

$$[a]_n = [r]_n,$$

dove r è il resto della divisione di a per n.

I resti possibili nella divisione per n sono $0, 1, 2, \ldots, n - 1$. Ne segue che

$$\mathbb{Z}/\mathscr{R} = \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n - 1]_n\}.$$

Notiamo che, $\mathbb{Z}/\mathscr{R}$ si denota anche con $\mathbb{Z}/\equiv_n$ o con $\mathbb{Z}/n\mathbb{Z}$ o $\mathbb{Z}_n$ ed ha n elementi.

Notiamo che la classe di equivalenza di 0 contiene tutti i multipli di n:

$$[0]_n = \{x \in \mathbb{Z} \mid x \mathscr{R} 0\} = \{x \in \mathbb{Z} \mid n \mid x - 0\} = \{x \in \mathbb{Z} \mid n \mid x\} =$$

$$= \{ \text{ multipli di } n \ \}.$$

Esempio 184. Sia $n = 5$ abbiamo $\mathbb{Z}_5 = \{[a]_5 \mid a \in \mathbb{Z}\} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. Ad esempio, $[0]_5 = [5]_5 = [100]_5$.

Quale è la classe di 6?

$[6]_5 = [1]_5 = [21]_5 = \{x \in \mathbb{Z} \mid x \text{ ha resto 1 nella divisione per 5 }\} = \{1 + 5t \mid t \in \mathbb{Z}\}$.

Quale è la classe di -2? Dobbiamo capire resto di -2 nella divisione per $n = 5$. Dato che $-2 = 5(-1) + 3$, si ha che il resto è 3, ovvero $[-2]_5 = [3]_5$.

Esempio 185. È vero che $81 \equiv 2 \pmod 4$? Bisogna determinare il resto di 81 nella divisione per 4. Poiché $81 = 20 \cdot 4 + 1$, il resto di 81 è 1 e quindi $81 \equiv 1 \pmod 4$. Pertanto è falso che $81 \equiv 2 \pmod 4$.

Esempio 186. È vero che $73 \equiv 3 \pmod 5$? Bisogna determinare il resto di 73 nella divisione per 5. Poiché $73 = 14 \cdot 5 + 3$, il resto di 73 è 3 e quindi è vero che $73 \equiv 3 \pmod 5$.

Proposizione 9. *La relazione di congruenza modulo n è compatibile con le operazioni di somma e prodotto in* $\mathbb{Z}$ *ovvero* $\forall\ a, b, c, d \in \mathbb{Z}$ *se* $a \equiv b \pmod n$ *e* $c \equiv d \pmod n$ *allora*

(1) $a + c \equiv b + d \pmod n$,

(2) $a \cdot c \equiv b \cdot d \pmod n$.

Questa proposizione ci permetterà di definire (Sezione 14.1)

$$[a]_n + [b]_n := [a + b]_n \qquad [a]_n \cdot [b]_n := [a \cdot b]_n :$$

possiamo fare la somma e il prodotto perché l'operazione non dipende dal rappresentante scelto.

Esempio 187. $[6]_5 + [-2]_5 = [4]_5$, $[3]_5 + [4]_5 = [7]_5 = [2]_5$,

Usando la Proposizione 9, possiamo concludere le seguenti proprietà.

Proprietà delle congruenze. Se $a \equiv b \pmod n$ allora

(1) $a^m \equiv b^m \pmod n$, per ogni $m \geq 1$;

(2) $ac \equiv bc \pmod n$, per ogni $c \in \mathbb{Z}$, dato che $c \equiv c \pmod n$;

(3) $a + kn \equiv b \pmod n$ per ogni $k \in \mathbb{Z}$, dato che $kn \equiv 0 \pmod n$;

(4) $a \equiv b + kn \pmod n$ per ogni $k \in \mathbb{Z}$, dato che $0 \equiv kn \pmod n$;

(5) $a - b \equiv 0 \pmod n$.

Esempio 188. Usando la prima proprietà: $12 \equiv 1 \pmod{11}$, quindi per ogni $m \geq 1$ si ha $12^m \equiv 1^m \pmod{11}$.

Esempio 189. Usando la terza proprietà: $2 \equiv 7 \pmod 5$, quindi ad esempio $2 + 25 \equiv 7 \pmod 5$.

Ulteriore Proprietà molto importante per gli esercizi

Proposizione 10. *Se* $ac \equiv bc \pmod n$ *allora* $a \equiv b \pmod{\frac{n}{d}}$, *dove* $d = MCD(c, n)$ *e viceversa. In particolare se* $1 = MCD(c, n)$ *e* $ac \equiv bc \pmod n$ *allora* $a \equiv b \pmod n$ *e viceversa.*

Esempio 190. Consideriamo $6 \equiv 14 \pmod 8$. Possiamo vederlo come $3 \cdot 2 \equiv 7 \cdot 2 \pmod{4 \cdot 2}$. Quindi per la Proposizione 10, la congruenza implica $3 \equiv 7 \pmod 4$ (ma non è vero $3 \equiv 7 \pmod 8$, bisogna dividere anche 8).

Inoltre, $6 \equiv 28 \pmod{11}$ ovvero $2 \cdot 3 \equiv 2 \cdot 14 \pmod{11}$, allora $3 \equiv 14 \pmod{11}$.

Teorema 13. *(Piccolo Teorema di Fermat[16]) Siano $a \in \mathbb{Z}$ e p un numero primo. Allora*

$$a^p \equiv a \pmod p.$$

Per i più curiosi: Si chiama piccolo, perchè esiste il seguente Teorema di Fermat.

Teorema 14. *L'equazione*

$$x^n + y^n = z^n$$

non ammette soluzioni intere non banali per $n \geq 3$.

Per banali, intendiamo soluzioni come ad esempio $x = 0$ e $y = z$ (quelle in cui $xyz = 0$).

Per $n = 1$, abbiamo una retta $x + y = z$ e abbiamo infinite soluzioni intere.

Per $n = 2$, le soluzioni sono infinite e sono dette terne pitagoriche, come ad esempio $x = 3, y = 4$ e $z = 5$, oppure $x = 5, y = 12$ e $z = 13$.

Per $n \geq 3$, il teorema è stato dimostrato da A. Wiles[17] nel 1994-1995.

Il Piccolo Teorema di Fermat vale se p primo. Allora, se $a \in \mathbb{Z}$ e p un numero primo

$$a^p \equiv a \pmod p.$$

Osservazione 83. Se p primo e $MCD(a, p) = 1$, allora per la Proposizione 10 dire $a^p \equiv a \pmod p$ implica $a^{p-1} \equiv 1 \pmod p$.

Se p non è primo cosa possiamo dire? Dobbiamo introdurre la funzione di Eulero.

Definizione 54. (FUNZIONE di EULERO) La funzione di Eulero è la funzione $\varphi : \mathbb{N}^* \to \mathbb{N}$, tale che $\varphi(n)$ è il numero degli interi positivi (> 0) minori di n e coprimi con n, ovvero conta quanti sono gli $a \in \mathbb{N}$ con $1 \leq a \leq n$ tale che $MCD(a, n) = 1$.

Esempio 191. Consideriamo i seguenti esempi:

$n = 2$, allora $\varphi(2) = 1$ (solo 1 è coprimo e minore o uguale a 2);

$n = 3$, allora $\varphi(3) = 2$ (solo 1, 2 sono coprimi e minori o uguali a 3)

$n = 5$ $\varphi(5) = 4$, infatti abbiamo 1,2,3,4.

Per $n = 10$ allora 1,3,7,9 sono coprimi e minori o uguali a 10 e quindi $\varphi(10) = 4$.

In generale, dato $n \in \mathbb{N}^*$ come possiamo calcolare $\varphi(n)$? Elenchiamo alcune proprietà della funzione di Eulero che serviranno per il suo calcolo.

Proprietà della funzione di Eulero.

(1) $\forall p$ primo $\varphi(p) = p - 1$;

(2) $\forall p$ primo e per ogni $h \geq 1$, $\varphi(p^h) = p^h - p^{h-1}$;

(3) $\forall a, b \in \mathbb{Z}$ se $MCD(a, b) = 1$, allora $\varphi(ab) = \varphi(a)\varphi(b)$.

Quindi, $\forall n \in \mathbb{N} \setminus \{0, 1\}$, se $n = p_1^{h_1} p_2^{h_2} \cdot \cdots \cdot p_s^{h_s}$ è la fattorizzazioni in primi di n, allora

$$\varphi(n) = \varphi(p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}) = \varphi(p_1^{h_1}) \cdot \varphi(p_2^{h_2}) \cdot \cdots \cdot \varphi(p_s^{h_s}) = (p_1^{h_1} - p_1^{h_1 - 1}) \cdots (p_s^{h_s} - p_s^{h_s - 1})$$

Esempio 192. Consideriamo i seguenti esempi:

$\varphi(13) = 12$, essendo 13 numero primo.

$\varphi(30) =?$ Usando la fattorizzazione $30 = 2 \cdot 3 \cdot 5$ quindi $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = 1 \cdot 2 \cdot 4 = 8$.

$\varphi(2^4 3^6 11^5) = \varphi(2^4)\varphi(3^6)\varphi(11^5) = (2^4 - 2^3)(3^6 - 3^5)(11^5 - 11^4)$.

[16]Pierre de Fermat, matematico francese 1601-1665

[17]A. Wiles, matematico nato nel 1953 a Cambridge, Professore presso la Unviersity of Oxford.

Teorema 15. *(TEOREMA di EULERO FERMAT) Sia $a \in \mathbb{Z}$ e $MCD(a,n) = 1$ allora*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Osservazione 84. Se $n = p$ primo, riotteniamo il Piccolo Teorema di Fermat.

Esempio 193. Dire se è vero o falso che $11^{48} \equiv 1 \pmod{104}$.
Allora 104 non è primo quindi non possiamo applicare il Piccolo Teorema Fermat.
Il MCD(11,104)=1 quindi possiamo applicare Teorema di Eulero Fermat.
Dobbiamo calcolare $\varphi(104)$. La fattorizzazione in primi è $104 = 52{\cdot}2 = 13{\cdot}4{\cdot}2 = 13{\cdot}2^3$.
Quindi $\varphi(104) = \varphi(2^3)\varphi(13) = (2^3 - 2^2)12 = 12 \cdot 4 = 48$.
Quindi la congruenza è vera.

Esempio 194. Dire se è vero o falso che $15^{353} \equiv 7 \pmod{8}$
Il numero 8 non è primo quindi non possiamo applicare il Piccolo Teorema Fermat.
Il $MCD(15,8) = 1$ quindi possiamo applicare Teorema di Eulero Fermat.
Dobbiamo calcolare $\varphi(8) = \varphi(2^3) = (2^3 - 2^2) = 4$ (infatti contiamo 1,3,5,7).
Quindi è vero che $15^4 \equiv 1 \pmod{8}$.
Vogliamo capire la classe di 353 modulo 4.
$353 = 4 \cdot 88 + 1$ Quindi $15^{353} = 15^{4\cdot 88+1} = 15^{4\cdot 88} \cdot 15$.
Quindi $15^{353} = (15^4)^{88} \cdot 15 \equiv_8 1^{88} \cdot 15 \equiv_8 1 \cdot 15 \equiv 7 \pmod{8}$.
Quindi la congruenza è vera.

12.1. **Criteri di Divisibilità.** Sia $x \in \mathbb{Z}$ e consideriamo la sua scrittura in base 10:

$$x = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10^1 + r_0$$

Osservazione 85. Considerando il numero 10 abbiamo che

(1) $10 \equiv 0 \pmod{2} \implies 10^m \equiv 0 \pmod{2}$, per ogni $m \geq 1$;
(2) $10 \equiv 0 \pmod{5} \implies 10^m \equiv 0 \pmod{5}$, per ogni $m \geq 1$;
(3) $10 \equiv 1 \pmod{3} \implies 10^m \equiv 1 \pmod{3}$, per ogni $m \geq 1$;
(4) $10 \equiv 1 \pmod{9} \implies 10^m \equiv 1 \pmod{9}$, per ogni $m \geq 1$;

12.1.1. *Criterio divisibilità per 2.* Il numero x è divisibile per 2 se e solo se è congruente a zero modulo 2. Applicando la (1) di Osservazione 85, si ha che

$$x = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10^1 + r_0 \equiv r_0 \pmod{2}.$$

Quindi x è divisibile per 2 se e solo se l'ultima cifra r_0 è divisibile per 2, ovvero se e solo se l'ultima cifra è pari.

12.1.2. *Criterio divisibilità per 5.* Il numero x è divisibile per 5 se e solo se è congruente a zero modulo 5. Applicando la (2) di Osservazione 85, si ha che

$$x = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10^1 + r_0 \equiv r_0 \pmod{5}.$$

Quindi x è divisibile per 5 se e solo se l'ultima cifra r_0 è divisibile per 5, ovvero se e solo se l'ultima cifra è 0 o 5.

12.1.3. *Criterio divisibilità per 3.* Il numero x è divisibile per 3 se e solo se è congrunete a zero modulo 3. Dato che $10^m \equiv 1 \pmod{3}$, si ha che

$$x = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10^1 + r_0 \equiv r_h + r_{h-1} + \cdots + r_0 \pmod{3}.$$

Quindi x è divisibile per 3 se e solo se la somma delle sue cifre è divisibile per 3.

12.1.4. *Criterio divisibilità per 9.* Il numero x è divisibile per 9 se e solo se è congrunete a zero modulo 9. Dato che $10^m \equiv 1 \pmod{9}$, si ha che

$$x = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10^1 + r_0 \equiv r_h + r_{h-1} + \cdots + r_0 \pmod{9}.$$

Quindi x è divisibile per 9 se e solo se la somma delle sue cifre è divisibile per 9.

12.2. **Congruenze lineari.**

Definizione 55. (CONGRUENZA LINEARE) Dati a e b interi e $n \geq 2$ si definisce una *congruenza lineare* nell'incognita x ogni espressione della forma

$$ax \equiv b \pmod{n}.$$

Una soluzione della congruenza lineare è un intero $x_0 \in \mathbb{Z}$ tale che $ax_0 \equiv b \pmod{n}$.

Esempio 195. Data $7x \equiv 1 \pmod{3}$, ad esempio $x_0 = 1$ è soluzione.

Esempio 196. Siamo interessati a trovare tutte le soluzioni di $30x \equiv 1 \pmod{2}$ oppure $18x \equiv 16 \pmod{44}$ o $104x \equiv 24 \pmod{600}$.

Dobbiamo risolvere due problemi. Come capire se esistono soluzioni e soprattutto come trovarle tutte.

Teorema 16. *(ESISTENZA) La congruenza lineare* $ax \equiv b \pmod{n}$ *ammette soluzioni intere se e soltanto se* $MCD(a, n) \mid b$.

Dimostrazione. Risolvere $ax \equiv b \pmod{n}$ equivale a dire $n \mid ax - b$ ovvero $\exists h \in \mathbb{Z}$ tale che $nh = ax - b$ ovvero $ax - nh = b$. Questa è una equazione diofantea ed ammette soluzioni se e solo se $MCD(a, n) \mid b$, vedere Teorema 9.

La dimostrazione del teorema è costruttiva, ovvero non solo ci dice se le soluzioni esistono ma ci spiega anche come trovarle: dobbiamo risolvere l'equazione diofantea associata.

Esempio 197. Consideriamo i seguenti esempi:
$7x \equiv 1 \pmod{3}$. Poiché $MCD(3, 7) = 1 \mid 1$, la congruenza ammette soluzioni.
$30x \equiv 1 \pmod{2}$. Poiché $MCD(30, 2) = 2 \not| 1$ la congruenza non ha soluzioni.
$18x \equiv 16 \pmod{44}$. Poiché $MCD(18, 44) = 2 \mid 16$, la congruenza ammette soluzioni.
$104x \equiv 24 \pmod{600}$. Abbiamo $104 = 52 \cdot 2 = 13 \cdot 4 \cdot 2 = 13 \cdot 2^3$, $600 = 6 \cdot 100 = 2 \cdot 3 \cdot 5^2 \cdot 2^2 = 2^3 \cdot 3 \cdot 5^2$, quindi $MCD(104, 600) = 8 \mid 24$ e pertanto la congruenza ammette soluzioni.

Come possiamo trovare tutte le soluzioni?

Teorema 17. *(SOLUZIONI) Se* x_0 *è una soluzione della congruenza lineare* $ax \equiv b \pmod{n}$ *allora tutte e sole le soluzioni di tale equazione sono*

$$x = x_0 + \frac{n}{d}t \qquad \forall t \in \mathbb{Z},$$

dove $d = MCD(a, n)$. *(Quindi se esiste una soluzione allora ne esistono infinite.)*
Tra queste soluzioni $x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$ *sono* d *soluzioni tutte non congruenti fra loro modulo* n. *Ogni altra soluzione è congruente a queste modulo* n.

Quindi, la congruenza $ax \equiv b \pmod{n}$ ammette esattamente $d = MCD(a, n)$ soluzioni non congruenti fra loro modulo n.

Osservazione 86. Sappiamo che erano fatte cosi le soluzioni della equazione diofantea per il Teorema 10.
Se $MCD(a, n) = 1$ allora la congruenza $ax \equiv b \pmod{n}$ ammette una unica soluzione modulo n. Tutte le altre soluzioni sono $x_0 + n$, $x_0 + 2n$, ... ovvero $x = x_0 + tn \qquad \forall t \in \mathbb{Z}$. Queste sono tutte congruenti modulo n; sono tutti i numeri che hanno resto x_0 nella divisione per n, ovvero possiamo anche scrivere $x \equiv x_0 \pmod{n}$.

Esempio 198. Consideriamo $7x \equiv 1 \pmod{3}$. Allora $x_0 = 1$ è soluzione, inoltre $MCD(1, 3) = 1$. Quindi $x_0 = 1$ è soluzione, ed è l'unica soluzione modulo 3. Altre soluzioni sono 4,7, -2, -5... ovvero $x = 1 + 3t$, $\forall t \in \mathbb{Z}$. Le possiamo scrivere tutte usando le congruenze: $x \equiv 1 \pmod{3}$.

Esercizio 45. Risolvere $18x \equiv 16 \pmod{44}$ indicandone tutte le soluzioni.

$MCD(18, 44) = 2$ e $2 \mid 16$, quindi ammette soluzioni. Risolvere la congruenza è come risolvere $44 \mid 18x - 16$ ovvero $44t = 18x - 16$ ovvero $18x - 44t = 16$. Quindi dobbiamo risolvere questa equazione diofantea e trovare x.

Dividiamo per 2 e otteniamo $9x - 22t = 8$. Abbiamo $MCD(9, 22) = 1$ e per ottenere l'Identità di Bézout abbiamo

$22 = 9 \cdot 2 + 4$

$9 = 4 \cdot 2 + 1$

Se $a = 9$ e $b = 22$, allora

$4 = 22 - 2 \cdot 9 = a - 2b$; $\quad 1 = 9 - 2 \cdot 4 = b - 2a + 4b = 5b - 2a$.

(Infatti, $1 = -2 \cdot 22 + 5 \cdot 9$.)

Quindi $8 = (-16) \cdot 22 + 40 \cdot 9$. Ne segue che $x_0 = 40$ è soluzione. Infatti $18x_0 = 18 \cdot 40 = 720 = 704 + 16 = 44 \cdot 16 + 16 \equiv 16 \pmod{44}$. Tutte le soluzioni sono $x = x_0 + \frac{n}{d}t = 40 + \frac{44}{2}t = 40 + 22t \ \forall t \in \mathbb{Z}$.

Inoltre, $MCD(18, 44) = 2$ quindi esistono $d = 2$ soluzioni non congrue modulo 44. Una soluzione L'altra soluzione è $x_0 + \frac{n}{d} = 40 + \frac{44}{2} = 40 + 22 = 62$ ovvero modulo 44: 62-44=18.

Quindi le soluzioni non congruenti modulo 44 sono 18 e 40, allora tutte le soluzioni sono $x \equiv 18 \pmod{44}$ e $x \equiv 40 \pmod{44}$.

Osservazione 87. La congruenza $ax \equiv b \pmod{n}$ ha soluzioni se $MCD(a, n) = d \mid b$, allora tutto divisibile per d. Dividiamo e semplifichiamo, ottenendo $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. Adesso, per le proprietà del massimo comun divisore si ha che $MCD(\frac{n}{d}, \frac{a}{d}) = 1$ e quindi esiste una unica soluzione modulo $\frac{n}{d}$.

Esempio 199. Risolvere $18x \equiv 16 \pmod{44}$ indicandone tutte le soluzioni.

$MCD(18, 44) = 2$, quindi ammette soluzioni.

Dividiamo per 2 e otteniamo: $9x \equiv 8 \pmod{22}$

Quindi $22 \mid 9x - 8$ e allora $9x - 22t = 8$. Come nell'Esercizio 45. Abbiamo già trovato la soluzione: $8 = (-16) \cdot 22 + 40 \cdot 9$.

$x_0 = 40$ è soluzione. Esiste una sola soluzione non congruente modulo 22 ed è 40, ovvero tutte le soluzioni sono $x \equiv 40 \pmod{22}$. Notiamo che $40 \equiv 18 \pmod{22}$, quindi possiamo anche scrivere che tutte le soluzioni sono $x \equiv 18 \pmod{22}$. Attenzione: otteniamo le stesse soluzioni dell'Esercizio 45! Infatti anche $x = 40$ è congruo a 18 modulo 22.

Esercizio 46. Risolvere $104x \equiv 24 \pmod{600}$. $MCD(104, 600) = 8 \mid 24$ dividiamo tutto per 8. Quindi si ottiene $13x \equiv 3 \pmod{75}$, che ha come soluzione: $x \equiv 6 \pmod{75}$.

Osservazione 88. Supponiamo di avere $ax \equiv b \pmod{n}$.

Dividiamo a per n, quindi $a = nq_a + r_a$ allora

$$ax \equiv b \pmod{n} \qquad \text{se e solo se} \qquad r_a x \equiv b \pmod{n}.$$

Infatti, $a \equiv r_a \pmod{n}$ e quindi $ax \equiv r_a x \pmod{n}$.

Lo stesso vale per b. Dividendo b per n, se $b = nq_b + r_b$ allora sappiamo che $b \equiv r_b \pmod{n}$ e quindi possiamo sostituire b con r_b.

Esempio 200. Risolvere la congruenza $11x \equiv 8 \pmod{5}$. Allora $11 \equiv 1 \pmod{5}$. Quindi possiamo ridurre la congruenza a $x \equiv 8 \pmod{5}$. Riduciamo anche 8 e otteniamo $x \equiv 3 \pmod{5}$. Ovvero $x_0 = 3$ è soluzione ed è unica soluzione modulo 5. Tutte le altre sono $x \equiv 3 \pmod{5}$.

Esempio 201. Risolvere la congruenza $14x \equiv 6 \pmod{4}$. Questa congruenza è equivalente a $2x \equiv 2 \pmod{4}$. Dividiamo ora per 2 e otteniamo $x \equiv 1 \pmod{2}$. Ovvero $x_0 = 1$ è soluzione ed è unica soluzione modulo 2. Tutte le altre sono $x \equiv 1 \pmod{2}$.

Esempio 202. Risolvere la congruenza $19x \equiv 3 \pmod 8$. Questa congruenza è equivalente a $3x \equiv 3 \pmod 8$. Quindi $x \equiv 1 \pmod 8$.

Per n piccolo possiamo anche procedere per tentativi senza risolvere l'equazione diofantea associata.

Esercizio 47. Risolvere la congruenza $3x \equiv 1 \pmod 7$. La congruenza ammette soluzione e modulo 7 è unica. Quindi, la soluzione è una delle classi resto modulo 7. Possiamo provare tutti i valori possibili e cercare la soluzione senza ricorrere alla equazione diofantea associata.

1 no, 2 no, 3 no, 4 no, 5 si: $3 \cdot 5 = 15 \equiv 1 \pmod 7$ quindi $x \equiv 5 \pmod 7$ è la soluzione.

Esercizio 48. Risolvere la congruenza $3x \equiv 7 \pmod{11}$. La congruenza ammette soluzione e modulo 11 è unica. Quindi, la soluzione è una delle classi resto modulo 11. Possiamo provare tutti i valori possibili e trovare la soluzione senza ricorrere alla equazione diofantea associata.

1 no, 2 no, 3 no, 4 no, 5 no, 6 si. Quindi $x_0 = 6$ è soluzione ed è unica soluzione modulo 11. Tutte le soluzioni sono $x \equiv 6 \pmod{11}$.

Esercizio 49. Risolvere $13x \equiv 3 \pmod{200}$.

12.3. **Sistemi di congruenze lineari.** Supponiamo di voler risolvere un *sistema di congruenze lineari*, ovvero

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \quad \cdots \quad \cdots \\ a_s x \equiv b_s \pmod{n_s}. \end{cases}$$

Una soluzione del sistema è un intero $x_0 \in \mathbb{Z}$ che risolve tutte le congruenze lineari.

Di sicuro è necessario che ogni congruenza sia risolubile, altrimenti non esiste soluzione al sistema. Inoltre, serve anche una compatibilità tra le congruenze.

Esempio 203. Consideriamo il seguente sistema di congruenze lineari

$$\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 2 \pmod 8. \end{cases}$$

Il sistema non ammette soluzioni perché la prima ha soluzioni solo dispari e la seconda solo numeri pari.

Proposizione 11. *Dato un sistema*

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \quad \cdots \quad \cdots \\ a_s x \equiv b_s \pmod{n_s} \end{cases}$$

tale che ogni congruenza ammette soluzione allora il sistema è equivalente ad un sistema della forma

$$\begin{cases} x \equiv c_1 \pmod{n_1'} \\ x \equiv c_2 \pmod{n_2'} \\ \quad \cdots \quad \cdots \\ x \equiv c_s \pmod{n_s'}. \end{cases}$$

Dimostrazione. Ogni singola congruenza $a_i x \equiv b_i \pmod{n_i}$ ammette soluzione, quindi $d_i = MCD(a_i, n_i) \mid b_i$. Dividiamo ogni congruenza per d_i e otteniamo una congruenza equivalente a quella precedente: $\frac{a_i}{d_i} x \equiv \frac{b_i}{d_i} \pmod{\frac{n_i}{d_i}}$ tale che $MCD(\frac{n_i}{d_i}, \frac{a_i}{d_i}) = 1$. Questa congruenza ammette una unica soluzione modulo $\frac{n_i}{d_i}$, esattamente $x \equiv c_i \pmod{\frac{n_i}{d_i}}$. Basta porre $\frac{n_i}{d_i} = n_i'$ e otteniamo il sistema equivalente richiesto.

Esempio 204. Consideriamo il seguente sistema di congruenze lineari

$$\begin{cases} 4x \equiv 8 \pmod{10} \\ 3x \equiv 3 \pmod{9}. \end{cases}$$

Si ha che $MCD(4, 10) = 2 \mid 8$, quindi dividendo per 2 abbiamo che $4x \equiv 8 \pmod{10}$ se e solo se $2x \equiv 4 \pmod{5}$. Possiamo ancora dividere per 2 (Proposizione 10) e ottenere

$$x \equiv 2 \pmod{5}.$$

Nella seconda $3x \equiv 3 \pmod{9}$, $MCD(3, 9) = 3 \mid 3$ dividiamo per 3 e otteniamo

$$x \equiv 1 \pmod{3}.$$

Quindi il sistema è equivalente a

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{3}. \end{cases}$$

Teorema 18. *(TEOREMA CINESE DEI RESTI) Siano $n_1, \ldots, n_s$ interi positivi tali che $MCD(n_i, n_j) = 1 \ \forall i \neq j$, allora il sistema di congruenze*

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \quad \cdots \quad \cdots \\ x \equiv c_s \pmod{n_s} \end{cases}$$

ammette soluzione unica modulo $n_1 \cdot n_2 \cdots n_s$.

Osservazione 89. Se gli interi non sono coprimi tra loro il teorema non ci dice nulla ma non è detto che non ci siano soluzioni.

Dimostrazione. Sia $N = n_1 \cdot n_2 \cdot \cdots \cdot n_s$ e $N_i = \frac{N}{n_i}$, ovvero il prodotto di tutti gli n_j tranne i-esimo. Ne segue che $MCD(N_i, n_i) = 1$.

Consideriamo

$$N_i x \equiv c_i \pmod{n_i}.$$

Questa congruenza ha una unica soluzione modulo n_i, dato che $MCD(N_i, n_i) = 1$. Chiamiamo tale soluzione x_i, ovvero $N_i x_i \equiv c_i \pmod{n_i}$. Lo facciamo per ogni i e troviamo tutte le varie soluzioni x_i. Allora

$$x_0 = N_1 \cdot x_1 + N_2 \cdot x_2 + \cdots + N_s \cdot x_s$$

è soluzione del sistema e $x \equiv N_1 \cdot x_1 + N_2 \cdot x_2 + \cdots + N_s \cdot x_s \pmod{N}$ è l'unica mod N.

Mostriamo che è soluzione del sistema. Infatti,

$$x_0 = N_1 \cdot x_1 + N_2 \cdot x_2 + \cdots + N_s \cdot x_s \equiv_{n_i} N_i x_i \equiv_{n_i} c_i$$

e questo per ogni i. Ne segue che x_0 risolve tutte le congruenze.

Esempio 205. Consideriamo il sistema dell'Esempio 204:

$$\begin{cases} 4x \equiv 8 \pmod{10} \\ 3x \equiv 3 \pmod{9} \end{cases}$$

Abbiamo visto che il sistema è equivalente a

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{3} \end{cases}$$

Applichiamo ora il Teorema Cinese dei Resti per risolverelo, infatti $MCD(3, 5) = 1$. Allor $N = 5 \cdot 3$, $N_1 = 3$ e $N_2 = 5$.

Consideriamo le due congruenze:

$$3x \equiv 2 \pmod{5} \qquad \text{e} \qquad 5x \equiv 1 \pmod{3}.$$

La prima ha come soluzione $x_1 \equiv 4 \pmod{5}$; la seconda $x_2 \equiv 2 \pmod{3}$. Quindi

$$x_0 = 3 \cdot 4 + 5 \cdot 2 = 22$$

è soluzione e tutte le soluzioni sono

$$x \equiv 22 \pmod{15} \quad \text{ovvero} \quad x \equiv 7 \pmod{15}.$$

Notiamo infatti che 7 soddisfa entrambe le congruenze del sistema.

13. Strutture Algebriche

La Repubblica promuove lo sviluppo della cultura e la ricerca scientifica e tecnica.
Tutela il paesaggio e il patrimonio storico e artistico della Nazione.

Definizione 56. (OPERAZIONE) Sia A un insieme non vuoto (finito o infinito). Una *operazione* su A è una qualunque funzione:

$$* : A \times A \to A \qquad \forall\, a, b \in A \qquad * (a, b) = a * b \in A.$$

La coppia ordinata $(A, *)$ si chiama *struttura algebrica.*

Osservazione 90. In alcuni testi, le operazioni vengono anche dette *leggi di composizione.*

Esempio 206. Consideriamo $A = \mathbb{N}$ e $* = +$. Allora $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, tale che $\forall\, a, b \in \mathbb{N}$ con $a * b = a + b$. Infatti $a + b \in \mathbb{N}$. È ben definita. Allora $(\mathbb{N}, +)$ è una struttura algebrica e $+$ è l'operazione di somma.

Esempio 207. Consideriamo $A = \mathbb{N}$ e $* = \cdot$. Allora $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, tale che $\forall\, a, b \in \mathbb{N}$ con $a * b = a \cdot b$. Infatti $a \cdot b \in \mathbb{N}$. È ben definita. Allora $(\mathbb{N}, \cdot)$ è una struttura algebrica e $\cdot$ è l'operazione di prodotto.

Esempio 208. Consideriamo $A = \mathbb{N}$ e $* = -$. Allora $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, tale che $\forall\, a, b \in \mathbb{N}$ con $a * b = a - b$. Non è una operazione su $\mathbb{N}$.

Esempio 209. Consideriamo $A = \mathbb{Z}$ e $* = -$. Allora $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tale che $\forall\, a, b \in \mathbb{Z}$ con $a * b = a - b$. Infatti $a - b \in \mathbb{Z}$, $\forall\, a, b \in \mathbb{Z}$, quindi è ben definita. Allora $(\mathbb{Z}, -)$ è una struttura algebrica.

Esempio 210. Esempi di strutture algebriche: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$.

Esempio 211. Consideriamo $A = \mathbb{Q}$ e definiamo $* : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, tale che $\forall\, a, b \in \mathbb{Q}$ con $a * b = 2a^2 - 4b^3$. Questa operazione è ben definita, infatti $\forall\, a, b \in \mathbb{Q}$ si ha che $a * b \in \mathbb{Q}$. Allora $(\mathbb{Q}, *)$ è una struttura algebrica.

Esempio 212. Consideriamo $A = \mathbb{Z}$ e definiamo $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tale che $\forall\, x, y \in \mathbb{Z}$ con $a * b = 2xy + x + y$. Questa operazione è ben definita, infatti $\forall\, x, y \in \mathbb{Z}$ si ha che $x * y \in \mathbb{Z}$. Allora $(\mathbb{Z}, *)$ è una struttura algebrica.

Definizione 57. (ASSOCIATIVA) Sia $(A, *)$ una struttura algebrica. L'operazione $*$ è associativa su A se

$$\forall\, x, y, z \in A \qquad (x * y) * z = x * (y * z).$$

In tal caso, diremo che $(A, *)$ è una struttura algebrica associativa.

Esempio 213. $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$ sono strutture algebriche associative, già visto (Sezione 10).

Esempio 214. $(\mathbb{Q}, \cdot)$ è una struttura algebrica associativa:

$$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \qquad \forall\, a, b \in \mathbb{Q} \qquad a * b = a \cdot b$$

è associativa: $\forall\, a, b, c \in \mathbb{Q}$ si ha $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Esempio 215. Ad esempio $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ sono strutture algebriche associative.

Esempio 216. Consideriamo $(\mathbb{R}, -)$ con

$$- : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \qquad \forall\, a, b \in \mathbb{R} \qquad a * b = a - b.$$

E ci chiediamo è associativa? Calcoliamo $(x * y) * z$ e $x * (y * z)$:

$$(x * y) * z = (x - y) - z = x - y - z \qquad \text{e} \qquad x * (y * z) = x - (y - z) = x - y + z;$$

i risultati non sono uguali, per ogni scelta di x, y e $z \in \mathbb{R}$. Ad esempio se $x = 0$, $y = 0$ e $z = 1$, allora $x - y - z = -1$; $x - y + z = 1$. Quindi $(\mathbb{R}, -)$ non è una struttura algebrica associativa.

Esempio 217. Sia B un insieme fissato non vuoto e $A = \{f : B \to B\}$ l'insieme delle funzioni da B in B. La composizione

$$\circ : A \times A \to A \qquad f * g = f \circ g$$

è una operazione su A ed abbiamo già visto che è associativa: $\forall f, g, h \in A$ si ha che $f \circ (g \circ h) = (f \circ g) \circ h$ (Sezione 3.4). Quindi $(A = \{f : B \to B\}, \circ)$ è una struttura algebrica associativa.

Definizione 58. (ELEMENTO NEUTRO) Una struttura algebrica $(A, *)$ ammette *elemento neutro* se

$$\exists\, e \in A \qquad \text{tale che} \qquad \forall x \in A \qquad x * e = e * x = x.$$

Osservazione 91. Nella definizione: $\exists e \in A$ tale che $\forall x \in A$; ovvero esiste un elemento e che "va bene"per ogni elemento x di A.

Esempio 218. Consideriamo $A = \mathbb{Z}$ con $* = +$, dove $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tale che $\forall\, a, b \in \mathbb{Z}$ con $+(a, b) = a + b \in \mathbb{Z}$. Allora $\exists e = 0 \in \mathbb{Z}$ tale che $\forall a \in \mathbb{Z}$ si ha $a + 0 = 0 + a = a$.

Osservazione 92. Se esiste un elemento neutro e in $(A, *)$, allora è unico. Infatti, se ne esistessero due: e_1 e e_2 in $(A, *)$. Allora

$$e_1 = e_1 * e_2 = e_2.$$

Nella prima uguaglianza, sfruttiamo che e_2 è elemento neutro, nella seconda che e_1 è elemento neutro.

Definizione 59. (MONOIDE) Una struttura algebrica $(A, *)$ associativa e dotata di elemento neutro, si chiama *monoide*.

Esempio 219. *Esempi di Monoide*:
$(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, associative ed $e = 0$ è elemento neutro.
$(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$,$(\mathbb{Q}, \cdot)$,$(\mathbb{R}, \cdot)$, associative ed $e = 1$ è elemento neutro.
$(A = \{f : B \to B\}, \circ)$ associativo ed $e = Id_B$ è elemento neutro.
Esempi di Non Monoide: $(\mathbb{Z}, -)$,$(\mathbb{Q}, -)$,$(\mathbb{R}, -)$, (perché sono strutture algebriche non associative).

Esempio 220. Consideriamo $A = \mathbb{Q}\backslash\{0\}$ e definiamo $* : \mathbb{Q}\backslash\{0\} \times \mathbb{Q}\backslash\{0\} \to \mathbb{Q}\backslash\{0\}$, tale che $\forall\, a, b \in \mathbb{Q}\backslash\{0\}$ con $a * b = a \cdot b$. Questa operazione è ben definita, infatti $\forall\, a, b \in \mathbb{Q}\backslash\{0\}$ si ha che $a \cdot b \in \mathbb{Q} \setminus \{0\}$ (il prodotto di due elementi diversi da zero è diverso da zero). Allora $(\mathbb{Q} \setminus \{0\}, \cdot)$ è una struttura algebrica. Inoltre l'operazione è associativa ed amette 1 come elemento neutro, esattamente come $(\mathbb{Q}, \cdot)$. Quindi $(\mathbb{Q} \setminus \{0\}, \cdot)$ è un monoide. Analogamente anche $(\mathbb{R} \setminus \{0\}, \cdot)$ è un monoide.

13.1. **Esempio: Monoide delle parole.** Sia L un insieme finito non vuoto, detto *alfabeto* (esempio lettere dell'alfabeto italiano o inglese o altro). Gli elementi dell'insieme L sono dette *lettere* dell'alfabeto. Una *parola* nell'alfabeto L è una sequenza (finita) di lettere (elementi) di L:

$$w = a_1 a_2 \dots a_n \qquad \text{con } a_i \in L, \quad \forall\, i = 1, \dots n;$$

w è una parola di lunghezza n (n =numero delle lettere della parola).

Notiamo che non è un prodotto, scriviamo le lettere vicino per formare una parola.

Poi abbiamo parola vuota e la indichiamo con $\emptyset$ ed è la sequenza vuota, quindi $\emptyset$ è la parola di lunghezza zero.

Definiamo A = insieme delle parole nell'alfabeto L; allora A è un insieme infinito.

Esempio 221. Sia $L = \{a, b, c\}$. Allora possiamo fare i seguenti esempi di parole: $\emptyset$, a, b, aa, bb, $aaabbbccacbabcbabbcc$.

Definiamo una struttura algebrica su A definendo la seguente operazione su A:

$$* : A \times A \to A \qquad\qquad * (w_1, w_2) = w_1 w_2$$

dove $w_1 w_2$ è la *concatenazione* di parole, ovvero scriviamo una parola dopo l'altra. Se $w_1 = a_1 a_2 \dots a_n$ e $w_2 = b_1 b_2 \dots b_m$ allora

$$w_1 * w_2 = a_1 a_2 \dots a_n b_1 b_2 \dots b_m.$$

Esempio 222. $L = \{a, b, c\}$; $w_1 = aabcaa$ $w_2 = abbb$ allora $w_1 w_2 = aabcaaabbb$. Oppure $w_2 w_1 = abbbaabcaa$.

Proprietà della struttura algebrica $(A, *)$

(1) $\forall w \in A$ si ha che $w * \emptyset = \emptyset * w = w$ (ovvero la parola vuota $\emptyset$ è l'elemento neutro).

(2) $\forall w_1, w_2, w_3 \in A$ si ha che $(w_1 * w_2) * w_3 = w_1 * (w_2 * w_3)$ (ovvero $*$ è associativa).

Quindi $(A, *)$ è una struttura algebrica associativa con elemento neutro $e = \emptyset$. Quindi $(A, *)$ è un monoide: il *monoide (libero) delle parole nell'alfabeto L.*

Osservazione 93. Il monoide delle parole su un alfabeto L è usato nei linguaggi di programmazione. Ad esempio, se $L = \{a, b, c\}$, il monoide A è spesso chiamato il monoide libero con 3 generatori. Studieremo il significato della parola generatori, quando affronteremo i gruppi (Sezione 14).

Definizione 60. (COMMUTATIVA) Sia $(A, *)$ una struttura algebrica. L'operazione $*$ soddisfa la *proprietà commutativa* se

$$\forall a, b, \in A \qquad \text{si ha } a * b = b * a.$$

Se in un monoide l'operazione è commutativa, allora il monoide si chiama *monoide commutativo.*

Esempio 223. *Esempi di Monoide Commutativo*:
$(\mathbb{N}, +)$, $(\mathbb{Z}, +)$,$(\mathbb{Q}, +)$,$(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$,$(\mathbb{Q}, \cdot)$,$(\mathbb{R}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$

Esempi di Monoide Non Commutativo:
$(A = \{f : B \to B\}, \circ)$, se B ha almeno due elementi.
Il monoide delle parole, se l'alfabeto è costituito da almeno due lettere.

Esercizio 50. Stabilire se $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ con $\forall x, y \in \mathbb{Z}$, $x * y = 2xy + x + y$ è una operazione associativa, ammette elemento neutro, è commutativa.

Esercizio 51. Stabilire se $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ con $\forall x, y \in \mathbb{Z}$, $x * y = xy + x$ è una operazione associativa, ammette elemento neutro, è commutativa.

Esercizio 52. Stabilire se $* : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ con $\forall x, y \in \mathbb{Q}$, $x * y = xy - x - y + 3$ è una operazione associativa, ammette elemento neutro, è commutativa.

Definizione 61. (elemento INVERTIBILE) Sia $(A, *)$ una struttura algebrica dotata di elemento neutro e. Un elemento $a \in A$ si dice *invertibile*, se esiste $a' \in A$ con

$$a * a' = a' * a = e.$$

Osservazione 94. Se non esiste elemento neutro, non si può parlare di elementi invertibili.

Proposizione 12. *Sia $(A, *)$ una struttura algebrica associativa dotata di elemento neutro e (ovvero è un monoide). Se $a \in A$ è invertibile, ovvero esiste $a' \in A$ con*

$$a * a' = a' * a = e$$

allora a' è unico e si chiama inverso di a.

Dimostrazione. Supponiamo per assurdo che esista un elemento $a \in A$ tale che esistano due elementi b e c in A che soddisfano le condizioni

$$e = a * b = b * a \qquad \text{ed} \qquad e = a * c = c * a.$$

Quindi

$$b = b * e \overset{c \ inv}{=} b * (a * c) \overset{ass}{=} (b * a) * c \overset{b \ inv}{=} e * c = c.$$

Allora $b = c$.

Osservazione 95. Sia $(A, *)$ una struttura algebrica con elemento neutro e, allora e è inverso di se stesso. SEMPRE!

Osservazione 96. Sia $(A, *)$ un monoide.

Se usiamo la notazione moltiplicativa allora $(A, \cdot)$, ovvero $* = \cdot$, elemento neutro $e = 1$ e l'inverso si indica con a^{-1}.

Se usiamo la notazione additiva allora $(A, +)$, ovvero $* = +$, elemento neutro $e = 0$, l'inverso si chiama opposto e si indica con $-a$.

Esempio 224. In $(\mathbb{Z}, +)$, l'opposto di $a = 5$ è -5. Infatti, $5 + (-5) = (-5) + 5 = 0$. L'opposto di $a = 7$ è -7 e l'opposto di $12 = 5 + 7$ è $-12 = (-5) + (-7)$.

Esempio 225. In $(\mathbb{N}, +)$ (monoide), $a + b = b + a = 0$ vero solo se $a = 0$, e $b = 0$. Quindi 0 è l'unico elemento che ammette opposto in $(\mathbb{N}, +)$.

In $(\mathbb{N}, \cdot)$ (monoide), $a \cdot b = b \cdot a = 1$ vero solo se $a = 1$ e in tal caso esiste $b = 1$ inverso. Quindi 1 è l'unico elemento che ammette inverso in $(\mathbb{N}, \cdot)$ e il suo inverso è 1.

In $(\mathbb{Z}, +)$ (monoide) ogni elemento ha opposto. Infatti $a + b = 0 = b + a$ ha soluzione per ogni $a \in \mathbb{Z}$, basta prendere $a' = -a$.

Analogamente ogni elemento in $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$ ammette opposto.

In $(\mathbb{Z}, \cdot)$ (monoide), $a \cdot b = 1 = b \cdot a$ ammette soluzione se e solo se $a = 1$ o $a = -1$. Se $a = 1$ allora inverso $b = 1$. Se $a = -1$ allora l'inverso è $b = -1$.

In $(\mathbb{Q}, \cdot)$ (monoide), $a \cdot b = 1 = b \cdot a$ ammette soluzione per ogni $a \neq 0$ basta prendere $a^{-1} = \dfrac{1}{a}$.

In $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot)$ (monoide), $a \cdot a' = 1 = a' \cdot a$ ammette soluzione per ogni $a \in \mathbb{Q}^*$: basta prendere $a^{-1} = \dfrac{1}{a}$.

Analogmanete, in $(\mathbb{R}, \cdot)$, ogni elemento $a \neq 0$ è invertibile e l'inverso è $a^{-1} = \dfrac{1}{a}$.

Analogamente, in $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot)$ (monoide) $a \cdot a' = 1 = a' \cdot a$ ammette soluzione per ogni $a \in \mathbb{R}^*$: basta prendere $a^{-1} = \dfrac{1}{a}$.

Consideriamo$(A = \{f : B \to B\}, \circ)$. Le funzioni biettive sono tutti e soli gli elementi invertibili.

In generale, in un monoide $(A, *)$ useremo la notazione a^{-1} per indicare l'inverso di A.

Osservazione 97. Se a è invertibile ed a^{-1} è inverso, allora $(a^{-1})^{-1} = a$. Infatti, $a * a^{-1} = a^{-1} * a = e$. Ma allora l'inverso di a^{-1} è a.

Osservazione 98. Sia $(A, *)$ un monoide. Se a e b sono invertibili, allora $a * b$ è invertibile e denotando con $(a * b)^{-1}$ l'inverso abbiamo:

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

Infatti

$$(a * b) * (b^{-1} * a^{-1}) = e \qquad \text{ed} \qquad (b^{-1} * a^{-1}) * (a * b) = e.$$

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

Osservazione 99. Abbiamo già visto queste proprietà per l'inversa di funzioni biettive nella Sezione 3.5.

Esempio 226. Consideriamo la struttura algebrica $(\mathbb{Q}, \cdot)$. Allora l'elemento neutro è $e = 1$. Se $a = 3$, allora $a^{-1} = \frac{1}{3}$. Allora $(a^{-1})^{-1} = \left(\frac{1}{3}\right)^{-1} = 3 = a$.

Se $b = 4$, allora $b^{-1} = \frac{1}{4}$. Allora $(b^{-1})^{-1} = \left(\frac{1}{4}\right)^{-1} = 4$.

Allora $a \cdot b = 12$ e $(a \cdot b)^{-1} = \frac{1}{12} = \frac{1}{4} \cdot \frac{1}{3}$.

14. Gruppi

(....) Lo straniero, al quale sia impedito nel suo paese l'effettivo esercizio delle libertà democratiche garantite dalla Costituzione italiana, ha diritto d'asilo nel territorio della Repubblica, secondo le condizioni stabilite dalla legge.(....)

Definizione 62. (GRUPPO) Una struttura algebrica $(A, *)$ è un *gruppo* se è un monoide in cui ogni elemento è invertibile, ovvero è una struttura algebrica associativa dotata di elemento neutro e ogni elemento è invertibile. Esplicitamente

(1) $*$ è associativa: $\forall a, b, c \in A$, si ha $(a * b) * c = a * (b * c)$.

(2) Esiste elemento neutro: $\exists e \in A$ tale che $\forall a \in A \qquad a * e = e * a = a$.

(3) Ogni elemento è invertibile: $\forall a \in A$, $\exists a' \in A$ con $a * a' = a' * a = e$.

Notazione. Per le strutture algebriche scriviamo $(A, *)$, per i gruppi si usa la notazione $(G, *)$.

Osservazione 100. Nella notazione di gruppo non si richiede che l'operazione sia commutativa.

Definizione 63. (Gruppo ABELIANO[18]) Un gruppo $(G, *)$ si dice *gruppo commutativo o gruppo abeliano*, se $*$ è commutativa, ovvero se

$$\forall a, b, \in A \qquad \text{si ha} \qquad a * b = b * a.$$

Esempio 227. $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ non sono gruppi.
$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,$(\mathbb{R}, +)$ sono gruppi abeliani.
$(\mathbb{Q}, \cdot)$,$(\mathbb{R}, \cdot)$ non sono gruppi, perché 0 non è invertibile.
$(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot)$,$(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot)$ sono gruppi abeliani.
B insieme non vuoto, $(A = \{f : B \to B \mid f \textit{ biettiva }\}, \circ)$ è un gruppo (non abeliano per $|B| \geq 3$). La Sezione 15 è dedicata a questo gruppo.

14.1. Operazioni compatibili con relazioni di equivalenza.

Definizione 64. Sia $(A, *)$ una struttura algebrica. Una relazione di equivalenza $\mathscr{R}$ su A si dice compatibile con l'operazione $*$ se:

$$\forall a, b, c, d \in A \qquad a \mathscr{R} b \text{ e } c \mathscr{R} d \Longrightarrow a * c \, \mathscr{R} \, b * d$$

ovvero se $(a, b) \in \mathscr{R}$ e $(c, d) \in \mathscr{R}$ allora $(a * c, b * d) \in \mathscr{R}$.

Ricordiamo che abbiamo visto la seguente proposizione (Proposizione 9).

Proposizione. 9 La relazione di congruenza modulo n è compatibile con le operazioni di somma e prodotto in $\mathbb{Z}$ ovvero $\forall\ a, b, c, d \in \mathbb{Z}$ se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ allora

(1) $a + c \equiv b + d \pmod{n}$,

(2) $a \cdot c \equiv b \cdot d \pmod{n}$.

[18] N.H. Abel, 1802-1829. Matematico Norvegese.

Esempio 228. 1) Sia $(A, *) = (\mathbb{Z}, +)$ e $\forall n \geq 2$ sia $\mathscr{R}=$ congruenza modulo n, ovvero $\equiv \pmod n$. Allora per la Proposizione 9, la relazione di congruenza modulo n è compatibile con la somma $+$ su $\mathbb{Z}$.

2) Sia $(A, *) = (\mathbb{Z}, \cdot)$ e $\forall n \geq 2$ sia $\mathscr{R}=$ congruenza modulo n, ovvero $\equiv \pmod n$. Allora per la Proposizione 9, la relazione di congruenza modulo n è compatibile con il prodotto $\cdot$ su $\mathbb{Z}$.

Teorema 19. *Sia $(A, *)$ una struttura algebrica e $\mathscr{R}$ una relazione di equivalenza su A compatibile con l'operazione $*$. Allora sull'insieme quoziente $A/\mathscr{R}$, ovvero*

$$A/\mathscr{R} = \{[a]_{\mathscr{R}} \mid a \in A\} = \{ \textit{ classi di equivalenza } \}$$

è definita l'operazione

$$*_{\mathscr{R}} : A/\mathscr{R} \times A/\mathscr{R} \to A/\mathscr{R}$$
$$\forall [a]_{\mathscr{R}}, [b]_{\mathscr{R}} \in A/\mathscr{R} \qquad *_{\mathscr{R}} ([a]_{\mathscr{R}}, [b]_{\mathscr{R}}) = [a]_{\mathscr{R}} *_{\mathscr{R}} [b]_{\mathscr{R}} = [a * b]_{\mathscr{R}}.$$

Scriveremo $(A/\mathscr{R}, *)$ al posto di $(A/\mathscr{R}, *_{\mathscr{R}})$.

Si verifica che $*$ è una operazione ben definita sull'insieme quoziente $A/\mathscr{R}$ e gode delle proprietà di $*$:

(1) Se $(A, *)$ è un monoide allora $(A/\mathscr{R}, *)$ è un monoide.

(2) Se $(A, *)$ è un gruppo allora $(A/\mathscr{R}, *)$ è un gruppo.

(3) Se $(A, *)$ è un gruppo commutativo allora $(A/\mathscr{R}, *)$ è un gruppo commutativo.

ESEMPIO FONDAMENTALE 1) Sia $(A, *) = (\mathbb{Z}, +)$ e $\forall n \geq 2$ sia $\mathscr{R}=$ congruenza modulo n, ovvero $\equiv \pmod n$. $\mathscr{R}$ è compatibile con la somma $+$ su $\mathbb{Z}$, quindi per il Teorema 19 è ben definita l'operazione di somma $+$ su $\mathbb{Z}/\equiv_n = \mathbb{Z}_n$:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

tale che $\forall [a]_n, [b]_n \in \mathbb{Z}_n$ si ha

$$[a]_n + [b]_n = [a + b]_n.$$

(La somma di due classi di equivalenza è la classe di equivalenza della somma).

Notiamo che $(\mathbb{Z}, +)$ è un gruppo abeliano quindi $(\mathbb{Z}_n, +)$ è un gruppo abeliano.

Esempio 229. Sia $n = 7$ e consideriamo $(\mathbb{Z}_7, +)$;

$$\mathbb{Z}_7 = \{[0]_7, [1]_7, \ldots, [6]_7\}$$

Ad esempio $[3]_7 + [5]_7 = [3 + 5]_7 = [8]_7 = [1]_7$, $[6]_7 + [1]_7 = [6 + 1]_7 = [7]_7 = [0]_7$.

Osservazione 101. Nel gruppo abeliano $(\mathbb{Z}_n, +)$, l'elemento neutro è $[0]_n$. Infatti:

$$\forall [a]_n \in \mathbb{Z}_n \qquad [a]_n + [0]_n = [0]_n + [a]_n = [0 + a]_n = [a]_n.$$

L'opposto di $[a]_n$ è $[-a]_n \in \mathbb{Z}_n$.

Esempio 230. Consideriamo $(\mathbb{Z}_7, +)$; allora l'opposto di $[5]_7$ è $[-5]_7 = [2]_7 \in \mathbb{Z}_7$, infatti

$$[5]_7 + [2]_7 = [5 + 2]_7 = [7]_7 = [0]_7.$$

ESEMPIO FONDAMENTALE 2) Sia $(A, *) = (\mathbb{Z}, \cdot)$ e $\forall n \geq 2$ sia $\mathscr{R}=$ congruenza modulo n, ovvero $\equiv \pmod n$. $\mathscr{R}$ è compatibile con il prodotto $\cdot$ su $\mathbb{Z}$. Quindi per il Teorema 19 è ben definita l'operazione di prodotto $\cdot$ su $\mathbb{Z}_n$:

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

tale che $\forall [a]_n, [b]_n \in \mathbb{Z}_n$ si ha

$$[a]_n \cdot [b]_n = [a \cdot b]_n.$$

(Il prodotto di due classi di equivalenza è la classe di equivalenza del prodotto).

Notiamo che $(\mathbb{Z}, \cdot)$ è un monoide commutativo, quindi $(\mathbb{Z}_n, \cdot)$ è un monoide commutativo.

Esempio 231. Ad esempio per $n = 8$, consideriamo $(\mathbb{Z}_8, \cdot)$:

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, \ldots, [7]_8\}.$$

Ad esempio $[3]_8 \cdot [5]_8 = [3 \cdot 5]_8 = [15]_8 = [7]_8$; $[2]_8 \cdot [4]_8 = [2 \cdot 4]_8 = [8]_8 = [0]_8$, $[3]_8 \cdot [3]_8 = [3 \cdot 3]_8 = [9]_8 = [1]_8$.

Osservazione 102. Nel monoide commutativo $(\mathbb{Z}_n, \cdot)$, l'elemento neutro è $[1]_n$. Infatti:

$$\forall [a]_n \in \mathbb{Z}_n \qquad [a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [1 \cdot a]_n = [a]_n.$$

Fino ad ora gli unici gruppi abeliani finiti che abbiamo studiato sono $(\mathbb{Z}_n, +)$, con $n \in \mathbb{N}$ e i suoi sottogruppi.

Consideriamo ora $(\mathbb{Z}_n, \cdot)$ monoide commutativo: $\cdot$ è associativa, commutativa, esiste elemento neutro $[1]_n$. Consideriamo un elemento in $[a]_n \in \mathbb{Z}_n$? Ammette inverso? Esiste $[x]_n \in \mathbb{Z}_n$ tale che $[a]_n \cdot [x]_n = [1]_n$?

Teorema 20. *Un elemento $[a]_n$ in $(\mathbb{Z}_n, \cdot)$ ammette inverso se e solo se $MCD(a, n) = 1$.*

Dimostrazione. Un elemento $[a]_n$ in $(\mathbb{Z}_n, \cdot)$ ammette inverso se e solo se esiste $[x]_n$ in $\mathbb{Z}_n$, tale che $[a]_n \cdot [x]_n = [1]_n$. Quindi, dobbiamo risolvere $[ax]_n = [1]_n$ ovvero la congruenza lineare $ax \equiv 1 \pmod{n}$. Questa congruenza ammette soluzioni se e solo se $MCD(a, n) \mid 1$, ovvero se e solo se $MCD(a, n) = 1$ (Teorema 16).

Osservazione 103. Notiamo che se il $MCD(a, n) = 1$, allora la soluzione della congruenza $ax \equiv 1 \pmod{n}$ è unica. Infatti, nei monoidi se l'inverso esiste è unico, come abbiamo dimostrato nella Proposizione 12.

Teorema 21. *Per ogni numero primo p, $(\mathbb{Z}_p^*, \cdot)$ è un gruppo abeliano.*

Dimostrazione. Osserviamo che $\cdot$ è una operazione su $\mathbb{Z}_p^*$: il prodotto di due classi non nulle in $\mathbb{Z}_p^*$ è ancora non nulla per la definizione di numero primo: $\forall [a]_p, [b]_p \in \mathbb{Z}_p^*$ allora $[a]_p \cdot [b]_p = [ab]_p \in \mathbb{Z}_p^*$. Infatti, se $[a]_p, [b]_p \in \mathbb{Z}_p^*$, allora $[a]_p \neq [0]_p$ e $[b]_p \neq [0]_p$. Quindi, $p \not| a$ e $p \not| b$. Allora poiché p è un numero primo, si ha che $p \not| ab$ ($p \mid ab$ se e solo se p divide uno dei due fattori). Quindi $[ab]_p \neq [0]_p$, ovvero $[ab]_p \in \mathbb{Z}_p^*$. Inoltre, l'operazione $\cdot$ è associativa, commutativa ed esiste elemento neutro $[1]_p$. Infine, ogni elemento non nullo ha inverso: essendo p primo, ogni elemento $[a]_p \in \mathbb{Z}_p^*$ è tale che $MCD(a, p) = 1$ e quindi è invertibile per il Teorema 20.

Esercizio 53. Determinare esplicitamente gli inversi di tutti gli elementi in $(\mathbb{Z}_5^*, \cdot)$ e $(\mathbb{Z}_7^*, \cdot)$

Definizione 65. (ORDINE o CARDINALITÀ) Sia $(G, *)$ un gruppo. Si dice *ordine* o *cardinalità* del gruppo la cardinalità dell'insieme G, e la indichiamo con $|G|$.

Se $|G| = +\infty$, allora diremo che $(G, *)$ è un *gruppo infinito*.

Se $|G| = n$, con $n \in \mathbb{N}^*$ allora diremo che $(G, *)$ è un *gruppo finito* di ordine o cardinalità n.

Esempio 232. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sono gruppi abeliani infiniti.

$(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$ sono gruppi abeliani infiniti.

$(\mathbb{Z}_n, +)$ gruppo abeliano finito di ordine o cardinalità n.

$(\mathbb{Z}_{11}, +)$ ha cardinalità 11.

Sia B un insieme con n elementi, allora $(A = \{f : B \to B \mid f \text{ biettiva } \}, \circ)$ è un gruppo (non abeliano se $|B| \geq 3$) finito con $n!$ elementi (Osservazione 35). La Sezione 15 è dedicata a questo gruppo.

Per ogni numero primo p, $(\mathbb{Z}_p^*, \cdot)$ è un gruppo abeliano di ordine $p - 1$.

14.2. **Sottogruppi e Gruppi Ciclici (Versione ridotta valida per A.A. 2023-2024, 2024-2025, 2025-2026).**

Definizione 66. (SOTTOGRUPPO) Un sottogruppo di un gruppo $(G, *)$ è un sottoinsieme non vuoto H dell'insieme G, che è un gruppo rispetto a $*$, ovvero rispetto alla stessa operazione di G: quindi $* : H \times H \to H$. Esplicitamente, $H \neq \emptyset$ è un sottogruppo di G se e solo se

(1) $\forall h, k \in H \Longrightarrow h * k \in H$ (H è chiuso rispetto alla operazione $*$, ovvero $*$ è una operazione su H).

(2) $e \in H$ (l'elemento neutro di G appartiene ad H).

(3) $\forall\ h \in H \Longrightarrow h^{-1} \in H$.

Notazione. Per indicare un sottogruppo si usa la notazione $H \leq G$.

Osservazione 104. La condizione 1) implica che $*$ è una operazione su H, l'associatività è automatica, ereditata da $*$ su G.

Esempio 233. In ogni gruppo $(G, *)$:
- il sottoinsieme costituito dal solo elemento neutro e, ovvero $\{e\}$, è un sottogruppo (SEMPRE!).
- $G \leq G$, ovvero ogni gruppo è sottogruppo di se stesso (SEMPRE!).

Proposizione 13. *Siano $(G, *)$ un gruppo e $g \in G$. Il sottoinsieme di G:*

$$< g >= \{g^t \mid t \in \mathbb{Z}\}$$

è un sottogruppo di G e si chiama sottogruppo ciclico di G generato da g.

Con la notazione g^t indichiamo le potenze di g in G. Se e denota l'elemento neutro, e g' l'inverso di g, allora $\forall t \in \mathbb{Z}$ le *potenze* t-esime di g sono

$$\begin{cases} g^0 = e, & \\ g^t = g * g * g \cdots * g \quad (t - volte) & \forall t > 0, \\ g^{-t} = (g')^t = g' * g' * g' \cdots * g' \quad (t - volte) & \forall t > 0. \end{cases}$$

Osservazione 105. In ogni gruppo $(G, *)$, il sottogruppo generato dall'elemento neutro e, contiene solo e. Ovvero, $< e >= \{e\}$.

Esempio 234. In $(\mathbb{Q}^*, \cdot)$, fissiamo $g = 2$. Allora

$$< 2 >= \{2^t \mid t \in \mathbb{Z}\} = \{2^0, 2^1, 2^2, 2^{-1}, 2^{-2}, \ldots\}.$$

Definizione 67. (CICLICO) Un gruppo $(G, *)$ si dice *ciclico* se esiste un elemento g con $G =< g >$ ovvero se il sottogruppo generato da g è G. In tal caso, g è detto *generatore* del gruppo. In particolare, è un gruppo abeliano.

Definizione 68. (ORDINE di un elemento) Siano $(G, *)$ un gruppo e $g \in G$. L'ordine dell'elemento g è l'ordine del sottogruppo generato dall'elemento g e si indica con $o(g)$, ovvero

$$o(g) = | < g > |.$$

Se $< g >$ ha ordine finito, ovvero se $| < g > | = n$, allora diremo che *l'elemento g ha ordine n* e scriviamo $o(g) = n$.

Se $< g >$ ha ordine infinito, ovvero $| < g > | = +\infty$, allora diremo che *l'elemento g ha ordine infinito* e scriviamo $o(g) = +\infty$.

Notazione: alcuni testo dicono *periodo* di un elemento al posto di ordine di un elemento

Osservazione 106. L'ordine dell'elemento neutro è 1 (SEMPRE!). Infatti, sia e l'elemento neutro in un gruppo $(G, *)$, sappiamo che $< e >= \{e\}$ (Osservazione 109). Quindi:

$$o(e) = |< e >| = |\{e\}| = 1.$$

Inoltre, l'elemento neutro è l'unico elemento in qualsiasi gruppo ad avere ordine 1.

Esempio 235. In $(\mathbb{Q}^*, \cdot)$, abbiamo che $o(1) = 1$, $o(-1) = 2$, $o(2) = +\infty$.

Proposizione 14. *Sia $(G, *)$, un gruppo $g \in G$. Allora valgono le seguenti proprietà:*

(1) *Se $o(g)$ è infinito, allora $\forall t, s \in \mathbb{Z}$ se $t \neq s$ si ha che $g^t \neq g^s$, ovvero tutte le potenze sono distinte. Analogamente in $(G, +)$, se $o(g)$ è infinito, allora $\forall t, s \in \mathbb{Z}$ se $t \neq s$ si ha che $tg \neq sg$, multipli distinti.*

(2) *Se $o(g)$ è finito e $o(g)=n$. Allora n è il più piccolo naturale positivo tale che $g^n = e$ (e elemento neutro di G). Inoltre, le potenze distinte di g sono esattamente n: $g^0, g^1, \ldots, g^{n-1}$. Infine, $\forall t, s \in \mathbb{Z}$ allora $g^t = g^s$, se e solo se $t \equiv s \pmod{n}$. Analogamente, in $(G, +)$, se $o(g) = n$, allora $tg = sg$ se e solo se $t \equiv s \pmod{n}$.*

Osservazione 107. Per definizione, preso g in un gruppo $(G, *)$:

$$o(g) = | < g > |,$$

ovvero l'ordine di un elemento g è l'ordine del sottogruppo generato dall'elemento g. La Proposizione 16 ci dice che se $o(g) = n$, allora n è il più piccolo intero tale che $g^n = e$, dove e indica l'elemento neutro del gruppo $(G, *)$ e

$$< g >= \{g^0 = e, g^1, \ldots, g^{n-1}\}.$$

14.3. **Sottogruppi e gruppi ciclici (versione standard non ridotta con dettagli ed esempi per anni accademici precedenti).**

Definizione 69. (SOTTOGRUPPO) Un sottogruppo di un gruppo $(G, *)$ è un sottoinsieme non vuoto H dell'insieme G, che è un gruppo rispetto a $*$, ovvero rispetto alla stessa operazione di G: quindi $* : H \times H \to H$. Esplicitamente, $H \neq \emptyset$ è un sottogruppo di G se e solo se

(1) $\forall h, k \in H \Longrightarrow h * k \in H$ (H è chiuso rispetto alla operazione $*$, ovvero $*$ è una operazione su H).

(2) $e \in H$ (l'elemento neutro di G appartiene ad H).

(3) $\forall\ h \in H \Longrightarrow h^{-1} \in H$.

Notazione. Per indicare un sottogruppo si usa la notazione $H \leq G$.

Osservazione 108. La condizione 1) implica che $*$ è una operazione su H, l'associatività è automatica, ereditata da $*$ su G.

Esempio 236. In ogni gruppo $(G, *)$:
- il sottoinsieme costituito dal solo elemento neutro e, ovvero $\{e\}$, è un sottogruppo (SEMPRE!).
- $G \leq G$, ovvero ogni gruppo è sottogruppo di se stesso (SEMPRE!).

Teorema 22. *(Lagrange[19]) Sia $(G, *)$ un gruppo finito, e $H \leq G$ sottogruppo di G, allora l'ordine di H divide l'ordine di G ovvero $|H| \mid |G|$.*

[19] Joseph Louis Lagrange circa 1736-1813 matematico nato a Torino.

Quindi se $|G| = n$ e $H \leq G$, allora $|H| = h$ e $h \mid n$.

Proposizione 15. *Siano $(G, *)$ un gruppo e $g \in G$. Il sottoinsieme di G:*

$$< g >= \{g^t \mid t \in \mathbb{Z}\}$$

è un sottogruppo di G e si chiama sottogruppo ciclico di G generato da g.

Con la notazione g^t indichiamo le potenze di g in G. Se e denota l'elemento neutro, e g' l'inverso di g, allora $\forall t \in \mathbb{Z}$ le *potenze* t-esime di g sono

$$\begin{cases} g^0 = e, & \\ g^t = g * g * g \cdots * g \quad (t - volte) & \forall t > 0, \\ g^{-t} = (g')^t = g' * g' * g' \cdots * g' \quad (t - volte) & \forall t > 0. \end{cases}$$

Se usiamo la notazione moltiplicativa, cioè il gruppo è $(G, \cdot)$, allora l'elemento neutro lo indichiamo con 1, l'inverso di un elemento g lo indichiamo con g^{-1}. Allora $\forall t \in \mathbb{Z}$, le potenze t-esime di g sono

$$\begin{cases} g^0 = 1_G & \\ g^t = g \cdot g \cdot g \cdots g \quad (t - volte) & \forall t > 0, \\ g^{-t} = (g^{-1})^t = g^{-1} \cdot g^{-1} \cdot g^{-1} \cdots g^{-1} \quad (t - volte) & \forall t > 0. \end{cases}$$

Quindi, in un gruppo $(G, \cdot)$ con la notazione moltiplicativa

$$< g >= \{g^t \mid t \in \mathbb{Z}\} = \{g^0 = 1, g, g^{-1}, g^2, g^{-2}, \ldots\}$$

è il sottogruppo ciclico di$(G, \cdot)$ generato da g.

Esempio 237. Consideriamo il gruppo $(\mathbb{Q}^*, \cdot)$, $1 \in \mathbb{Z}$. Allora
$< 1 >= \{1^n \mid n \in \mathbb{Z}\} = \{1\}$, gruppo finito di ordine 1, sottogruppo di $(\mathbb{Q}^*, \cdot)$.
$< -1 >= \{(-1)^n \mid n \in \mathbb{Z}\}$ =\{ potenze di -1\}=$\{1, -1\}$, gruppo finito di ordine 2, sottogruppo di $(\mathbb{Q}^*, \cdot)$.
In generale, per ogni elemento $h \in \mathbb{Q}^*$, abbiamo
$< h >= \{h^n \mid n \in \mathbb{Z}\}$ =\{ potenze di h\}.
Ad esempio
$< 3 >= \{3^n \mid n \in \mathbb{Z}\} = \{3, 1, \frac{1}{3}, ..\}$, che è un gruppo infinito, , sottogruppo di $(\mathbb{Q}^*, \cdot)$.

Se usiamo la notazione additiva, cioè il gruppo è $(G, +)$, allora l'elemento neutro lo indichiamo con 0, l'opposto di un elemento g lo indichiamo con $-g$. Allora $\forall t \in \mathbb{Z}$, le potenze t-esime di g di dicono multipli t-esimi di g e sono

$$\begin{cases} 0 \cdot g = 0 & \\ t \cdot g = g + g + g \cdots + g \quad (t - volte) & \forall t > 0 \\ (-t)g = t(-g) = (-g) + (-g) + \cdots + (-g) \quad (t - volte) & \forall t > 0 \end{cases}$$

Analogamente, in un gruppo $(G, +)$ con la notazione additiva

$$< g >= \{tg \mid t \in \mathbb{Z}\} = \{0g = 0, g, -g, 2g, -2g, 3g, \ldots\}$$

è il sottogruppo ciclico di$(G, +)$ generato da g.

Esempio 238. Consideriamo il gruppo $(\mathbb{Z}, +)$. Se fissiamo $g = 2 \in \mathbb{Z}$, allora
$< 2 >= \{t \cdot 2 \mid t \in \mathbb{Z}\}$ = \{ multipli di 2\}= insieme numeri pari=$2\mathbb{Z}$.
$< 5 >= \{t \cdot 5 \mid t \in \mathbb{Z}\}$ = \{ multipli di 5\}=$5\mathbb{Z}$.
Per ogni elemento $n \in \mathbb{Z}$ fissato,
$< n >= \{t \cdot n \mid t \in \mathbb{Z}\}$ =\{ multipli di n\} = $n\mathbb{Z}$.
$< 1 >= \{n \cdot 1 \mid n \in \mathbb{Z}\}$ =\{ multipli di 1\}= $\mathbb{Z}$.
$< -1 >= \{n \cdot (-1) \mid n \in \mathbb{Z}\}$ =\{ multipli di -1\}= $\mathbb{Z}$.
$< 0 >= \{0\}$.

Osservazione 109. In ogni gruppo $(G, *)$, il sottogruppo generato dall'elemento neutro e, contiene solo e. Ovvero, $< e >= \{e\}$.

Definizione 70. (ORDINE di un elemento) Siano $(G, *)$ un gruppo e $g \in G$. L'ordine dell'elemento g è l'ordine del sottogruppo generato dall'elemento g e si indica con $o(g)$, ovvero

$$o(g) = | < g > |.$$

Se $< g >$ ha ordine finito, ovvero se $| < g > | = n$, allora diremo che *l'elemento g ha ordine n* e scriviamo $o(g) = n$.

Se $< g >$ ha ordine infinito, ovvero $| < g > | = +\infty$, allora diremo che *l'elemento g ha ordine infinito* e scriviamo $o(g) = +\infty$.

Notazione: alcuni testo dicono *periodo* di un elemento al posto di ordine di un elemento

Esempio 239. In $(\mathbb{Z}, +)$, $o(0) = | < 0 > | = |\{0\}| = 1$,
$o(1) = | < 1 > | = |\mathbb{Z}| = +\infty$
$o(2) = \infty$, $o(3) = +\infty$. In $(\mathbb{Z}, +)$, tutti gli elementi non nulli hanno ordine infinito.

Esempio 240. In $(\mathbb{Q}^*, \cdot)$, abbiamo che $o(1) = 1$, $o(-1) = 2$, $o(a) = +\infty$, $\forall a \neq 1, -1$ (Esempio 237).

Osservazione 110. Siano G finito, diciamo $|G| = n$, e g un elemento di G. Poiché il sottogruppo $< g >$ generato da g è sottogruppo di G, per il Teorema di Lagrange (Teorema 22), si ha che $| < g > | \mid n$. Quindi **nei gruppi finiti, l'ordine $o(g)$ di un qualsiasi elemento g è un divisore dell'ordine del gruppo $|G|$.**

Osservazione 111. L'ordine dell'elemento neutro è 1 (SEMPRE!). Infatti, sia e l'elemento neutro in un gruppo $(G, *)$, sappiamo che $< e >= \{e\}$ (Osservazione 109). Quindi:

$$o(e) = | < e > | = |\{e\}| = 1.$$

Inoltre, l'elemento neutro è l'unico elemento in qualsiasi gruppo ad avere ordine 1.

Proposizione 16. *Sia $(G, *)$, un gruppo $g \in G$. Allora valgono le seguenti proprietà:*

(1) *Se $o(g)$ è infinito, allora $\forall t, s \in \mathbb{Z}$ se $t \neq s$ si ha che $g^t \neq g^s$, ovvero tutte le potenze sono distinte. Analogamente in $(G, +)$, se $o(g)$ è infinito, allora $\forall t, s \in \mathbb{Z}$ se $t \neq s$ si ha che $tg \neq sg$, multipli distinti.*

(2) *Se $o(g)$ è finito e $o(g)=n$. Allora n è il più piccolo naturale positivo tale che $g^n = e$ (e elemento neutro di G). Inoltre, le potenze distinte di g sono esattamente n: $g^0, g^1, \ldots, g^{n-1}$. Infine, $\forall t, s \in \mathbb{Z}$ allora $g^t = g^s$, se e solo se $t \equiv s \pmod{n}$. Analogamente, in $(G, +)$, se $o(g) = n$, allora $tg = sg$ se e solo se $t \equiv s \pmod{n}$.*

Osservazione 112. Per definizione, preso g in un gruppo $(G, *)$:

$$o(g) = | < g > |,$$

ovvero l'ordine di un elemento g è l'ordine del sottogruppo generato dall'elemento g. La Proposizione 16 ci dice che se $o(g) = n$, allora n è il più piccolo intero tale che $g^n = e$, dove e indica l'elemento neutro del gruppo $(G, *)$ e

$$< g >= \{g^0 = e, g^1, \ldots, g^{n-1}\}.$$

Esercizio 54. In $(\mathbb{Z}_6, +)$, calcolare l'ordine di $g = [2]_6, [3]_6, [5]_6$.

SKETCH: $|\mathbb{Z}_6| = 6$, quindi è un gruppo finito. Allora per il Teorema di Lagrange (Teorema 22) e l'Osservazione 110, l'ordine di ogni elemento è un divisore di 6, ovvero, può essere $1, 2, 3$ o 6. Ricordiamo che $< g >= \{tg \mid t \in \mathbb{Z}\}$ e $o(g) = | < g > |$.

Dobbiamo calcolare $o([2]_6)$. Per definizione $o([2]_6) = | < [2]_6 > |$. Quindi dobbiamo determinare il sottogruppo $< [2]_6 >$ e contare i suoi elementi. Si ha che $< [2]_6 >= \{[0]_6, [2]_6, [4]_6\}$. Questo è il sottogruppo generato da $[2]_6$ (ad esempio $-[2]_6 = [4]_6$).

Quindi si ha che $| < [2]_6 > | = 3$ da cui concludiamo che $o([2]_6) = | < [2]_6 > | = 3$.

Dobbiamo calcolare $o([3]_6)$. Per definizione $o([3]_6) = | < [3]_6 > |$. Quindi dobbiamo determinare il sottogruppo $< [3]_6 >$. Abbiamo che $< [3]_6 >= \{[0]_6, [3]_6\}$ Quindi: $o([3]_6) = | < [3]_6 > | = 2$.

Dobbiamo calcolare $o([5]_6) = | < [5]_6 > |$. Quindi $< [5]_6 >= \{[0]_6, [5]_6, [4]_6, [3]_6, [2]_6, [1]_6\}$ $o([5]_6) = | < [5]_6 > | = 6$. (Potevamo fermarci anche dopo aver calcolato $3 \cdot [5]_6 = [3]_6$. Infatti questo ci dice che l'ordine di $[5]_6$ non è ne 1, ne 2, ne 3. Poiché abbiamo detto che l'ordine può essere $1, 2, 3$ o 6, possiamo concludere che l'ordine di $[5]_6$ è 6).

Esempio 241. $4[2]_6 = [8]_6 = [2]_6$. Infatti, le potenze 4 e 1 di $[2]_6$ sono equivalenti modulo $o([2]_6) = 3$: $4 \equiv 1 \pmod 3$.

Esempio 242. In $(\mathbb{Z}_{12}, +)$, consideriamo $[4]_{12}$.
I multipli di $[4]_{12}$ sono: $[0]_{12}, [4]_{12}, [8]_{12}, [12]_{12} = [0]_{12}$. Quindi $o([4]_{12}) = 3$ e $< [4]_{12} >= \{[0]_{12}, [4]_{12}, [8]_{12}\}$.

Definizione 71. (CICLICO) Un gruppo $(G, *)$ si dice *ciclico* se esiste un elemento g con $G =< g >$ ovvero se il sottogruppo generato da g è G. In tal caso, g è detto *generatore* del gruppo.

Osservazione 113. $(G, \cdot)$ è un gruppo ciclico generato da g se $G =< g >$, quindi ogni elemento h di G è una potenza di g: $\forall h \in G \quad \exists t \in \mathbb{Z}$ tale che $h = g^t$.
$(G, +)$ è un gruppo ciclico generato da g se $G =< g >$, quindi ogni elemento h di G è un multiplo di g: $\forall h \in G \quad \exists t \in \mathbb{Z}$ tale che $h = tg$.

Esempio 243. Il gruppo $(\mathbb{Z}, +)$ è ciclico. Infatti, $< 1 >=< -1 >= \mathbb{Z}$. Sia 1 che -1 sono generatori: $(\mathbb{Z}, +)$ ha 2 generatori.
- $(\mathbb{Z}_6, +)$ è ciclico, abbiamo visto nell'Esercizio 54 che $[5]_6$ è generatore.

Osservazione 114. Per ogni $n \geq 2$, la classe $[1]_n$ è generatore in $(\mathbb{Z}_n, +)$. Infatti $< [1]_n >= \{[0]_n, [1]_n, \dots [n-1]_n\} = \mathbb{Z}_n$.
Quindi, $(\mathbb{Z}_n, +)$ è un gruppo ciclico per ogni n.

Proprietà dei gruppi CICLICI

(1) Ogni gruppo ciclico $(G, *)$ è un gruppo abeliano: $\forall h = g^t$ e $k = g^s \in G$, abbiamo $h * k = g^t * g^s = g^{t+s} = g^{s+t} = g^s * g^t = k * h$.

(2) Siano $(G, *)$ un gruppo ciclico di ordine n e g un generatore. Allora, l'elemento g^t di G ha ordine:
$$o(g^t) =| < g^t > |= \frac{n}{MCD(t, n)}.$$

Osservazione 115. In $(G, +)$, si ha che l'elemento tg di G ha ordine:
$$o(tg) =| < tg > |= \frac{n}{MCD(t, n)}.$$

CONSEGUENZA Sia $(G, *)$ gruppo ciclico finito di ordine n generato da g. Allora, i generatori sono tutti gli elementi g^t tali che $MCD(t, n) = 1$. (In $(G, +)$, sono gli elementi tg di G , con $MCD(t, n) = 1$). Quindi ci sono $\varphi(n)$ generatori, dove $\varphi(n)$ è la funzione di Eulero (Definizione 54).

Esempio 244. In $(\mathbb{Z}_n, +)$ i generatori sono tutti e soli gli elementi di $\mathbb{Z}_n$ che sono coprimi con n, ovvero $[h]_n \in \mathbb{Z}_n$ tali che $MCD(h, n) = 1$. Infatti, $o([h]_n) = \frac{n}{MCD(h,n)} = \frac{n}{1} = n$. Quindi in $(\mathbb{Z}_n, +)$ ci sono $\varphi(n)$ generatori, dove $\varphi(n)$ è la funzione di Eulero (Definizione 54).
In particolare, se $n = p$ primo $(\mathbb{Z}_p, +)$, allora ogni elemento $[h]_p \neq [0]_p$ è un generatore.

Esempio 245. In $(\mathbb{Z}_8, +)$, calcolare $o([2]_8)$ e $o([3]_8)$. Allora $\mathbb{Z}_8 =< [1]_8 >$. Quindi, $[2]_8 = 2[1]_8$ e $[3]_8 = 3[1]_8$. Ne segue che

$$o([2]_8) = \frac{8}{MCD(2,8)} = 4 \qquad o([3]_8) = \frac{8}{MCD(3,8)} = 8$$

Scrivere sottogruppo generato da $[2]_8$ e $[3]_8$. Il sottogruppo generato da $[2]_8$ contiene 4 elementi ed è

$$< [2]_8 >= \{[0]_8, [2]_8, [4]_8, [6]_8\}.$$

Il sottogruppo generato da $[3]_8$ contiene 8 elementi ed è tutto $\mathbb{Z}_8$:

$$< [3]_8 >= \{[0]_8, [3]_8, [6]_8, [1]_8, [4]_8, [7]_8, [2]_8, [5]_8\}.$$

Esempio 246. $(\mathbb{Z}_5^*, \cdot)$ è un gruppo abeliano.

L'ordine è $|\mathbb{Z}_5^*| = 4$. Determinare generatori e ordine di ogni elemento.

Determinare ordine di $[2]_5$. Per l'Osservazione 110, l'ordine può essere 1,2 o 4.

$[2]_5{}^0 = [1]_5$, $[2]_5{}^1 = [2]_5$, $[2]_5{}^2 = [4]_5 \neq [1]_5$. Allora ordine di $[2]_5$ non è né 1 né 2, quindi è necessariamente 4. Infatti $[2]_5{}^3 = [8]_5 = [3]_5$, $[2]_5{}^4 = [1]_5$. Quindi $o([2]_5) = 4$ e pertanto $[2]_5$ è un generatore.

Possiamo anche determinare tutti gli altri ordini, usando la formula dell'ordine nei gruppi ciclici.

$o([1]_5) = 1$. $o([3]_5) = o([2]_5{}^3) = \frac{4}{MCD(3,4)} = 4$. Quindi anche $[3]_5$ è un generatore.

$o([4]_5) = o([2]_5{}^2) = \frac{4}{MCD(2,4)} = 2$, infatti $< [4]_5 >= \{[1]_5, [4]_5\}$ ha 2 elementi.

Esempio 247. $(\mathbb{Z}_7^*, \cdot)$ è un gruppo abeliano.

L'ordine è $|\mathbb{Z}_7^*| = 6$. Determinare generatori e ordine di ogni elemento.

Determinare ordine di $[2]_7$. Per l'Osservazione 110, l'ordine può essere 1,2,3 o 6.

$[2]_7{}^0 = [1]_7$, $[2]_7{}^1 = [2]_7$, $[2]_7{}^2 = [4]_7$, $[2]_7{}^3 = [8]_7 = [1]_7$. Quindi $o([2]_7) = 3$. Quindi non è un generatore.

Determinare ordine di $[3]_7$. Può essere 1,2,3 o 6.

$[3]_7{}^0 = [1]_7$, $[3]_7{}^1 = [3]_7$, $[3]_7{}^2 = [2]_7$, $[3]_7{}^3 = [6]_7 \neq [1]_7$. Quindi $o([3]_7)$ non non è né 1, né 2 e né 3 quindi è necessariamente 6. Infatti, $[3]_7{}^4 = [4]_7$, $[3]_7{}^5 = [5]_7$, $[3]_7{}^6 = [1]_7$.

Quindi $o([3]_7) = 6$ e quindi $[3]_7$. Adesso che abbiamo un generatore possiamo determinare l'ordine di tutti gli elementi applicando la Proprietà (2) dei gruppi ciclici, senza dover determinare tutti i sottogruppi. Sappiamo che $o([1]_7) = 1$, $o([2]_7) = 3$ e $o([3]_7) = 6$.

$o([4]_7) = o([3]_7{}^4) = \frac{6}{MCD(4,6)} = 3$.

$o([5]_7) = o([3]_7{}^5) = \frac{6}{MCD(5,6)} = 6$. Quindi $[5]_7$ è un generatore.

$o([6]_7) = o([3]_7{}^3) = \frac{6}{MCD(3,6)} = 2$.

Quindi ci sono due generatori: $[3]_7$ e $[5]_7$, infatti, $\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 2$.

15. Gruppo Simmetrico

L'Italia ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo di risoluzione delle controversie internazionali; consente, in condizioni di parità con gli altri Stati, alle limitazioni di sovranità necessarie ad un ordinamento che assicuri la pace e la giustizia fra le Nazioni; promuove e favorisce le organizzazioni internazionali rivolte a tale scopo.

In questa sezione, approfondiamo lo studio del gruppo simmetrico.

Sia B un insieme. Abbiamo visto che

$$(A = \{f : B \to B \mid f \textit{ biettiva } \}, \circ)$$

è un gruppo (Esempio 227): la composizione $\circ$ è associativa, esiste l'elemento neutro che è la funzione identità ed inoltre ogni elemento è invertibile (Sezione 3) .

Se $|B| = n$, allora possiamo elencare elementi di B da 1 a n, ovvero:

$$B = \{1, 2, 3, \ldots, n-1, n\}.$$

Esempio 248. Sia $n = 8$, allora $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Allora un elemento di A è una funzione biettiva (o una corrispondenza biunivoca) $f : B \to B$; ad esempio $f : B \to B$, definita da $f(1) = 1, f(2) = 3, f(3) = 4, f(4) = 5, f(5) = 8, f(6) = 7, f(7) = 2, f(8) = 6$.

Definizione 72. (GRUPPO SIMMETRICO o GRUPPO DI PERMUTAZIONI)
Il gruppo delle funzioni biettive di un insieme con n elementi è detto *gruppo di permutazioni di n elementi*, o *gruppo simmetrico di n elementi* e si indica con S_n. La cardinalità di S_n è $|S_n| = n!$ (Osservazione 38).

Ci ricordiamo che le *funzioni biettive* vengono anche dette *corrispondenze biunivoche* in un insieme di n elementi o anche *permutazioni*.

Notazione: Dato un elemento $f \in S_n$, f si indica nel seguente modo:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

Ovvero sopra tutti elementi ordinati da 1 a n, sotto le immagini tramite f. Osserviamo che nella seconda riga compaiono tutti e soli gli elementi da 1 a n una ed una sola volta, al più cambia solo l'ordine.

Notazione: Spesso si usa la notazione $\sigma \in S_n$, o $\tau \in S_n$, ovvero gli elementi di S_n si indicano con le lettere greche:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Esempio 249. Siano $n = 8$, $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e $f : B \to B$ una corrispondenza biunivoca definita da $f(1) = 1, f(2) = 3, f(3) = 4, f(4) = 5, f(5) = 8, f(6) = 7, f(7) = 2, f(8) = 6$. Allora $f \in S_8$ corrisponde a

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix}.$$

Sia $g \in S_8$ data da

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix}.$$

Significa che $g : B \to B$ è la corrispondenza biunivoca tale che $g(1) = 2, g(2) = 6, g(3) = 7, g(4) = 5, g(6) = 1, g(7) = 3, g(8) = 4$.

Esempio 250. L'elemento identità di S_n è

$$Id = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Esempio 251. (n=2). Se $n = 2$ allora $|S_2| = 2! = 2$ Ci sono due elementi. $B = \{1, 2\}$ ovvero due modi di ordinare 2 elementi. Quindi i due elementi di S_2 sono:

$$Id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Il gruppo S_2 è commutativo: $f \circ Id = Id \circ f = f$.

Esempio 252. (n=3). Se $n = 3$ allora $|S_3| = 3! = 6$ Ci sono sei elementi. Ovvero sei modi di ordinare gli elementi $\{1, 2, 3\}$.

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Esercizio 55. Scrivere gli elementi di S_4.

Abbiamo detto che S_n è un gruppo, quindi è ben definita l'operazione $\circ$ di composizione e ogni elemento ammette inverso. La scrittura introdotta è comoda per determinare la composizione e l'inverso.

Definizione 73. (COMPOSIZIONE) Siano $f, g \in S_n$

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ g(1) & g(2) & g(3) & \cdots & g(n) \end{pmatrix}.$$

Allora la composizione $f \circ g \in S_n$ è la composizione delle funzioni ovvero $(f \circ g)(i) = f(g(i))$, per ogni $i = 1, \ldots, n$. Quindi $i \mapsto g(i) \mapsto f(g(i))$. Quindi consideriamo l'elemento i, vediamo l'immagine di i con g e poi applichiamo f.

Esempio 253. Consideriamo:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Allora

$$f_1 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad e \qquad f_2 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

In particolare: $f_1 \circ f_2 \neq f_2 \circ f_1$.

Osservazione 116. Se $n \geq 3$, allora il gruppo S_n non è abeliano (e quindi non è ciclico per le Proprietà dei gruppi ciclici).

Esempio 254. In S_8 abbiamo definito:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix}.$$

Allora $f \circ g$ prima applichiamo g e dopo f (muovendoci da destra verso sinistra):

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 2 & 8 & 6 & 1 & 4 & 5 \end{pmatrix}.$$

Calcoliamo l'altra composizione $g \circ f$, in questo caso prima applichiamo f e poi applichiamo g:

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 7 & 5 & 8 & 4 & 3 & 6 & 1 \end{pmatrix}.$$

Notiamo che $f \circ g \neq g \circ f$.

Esercizio 56. Calcolare $g \circ g$ e $f \circ f$.

Definizione 74. (INVERSO) Sia $f \in S_n$, allora sappiamo che $f^{-1} \in S_n$, infatti inverso di una funzione biettiva esiste sempre ed è una funzione biettiva. Sia

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

Allora f^{-1} è data da

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & f(3) & \cdots & f(n) \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

che poi riordiniamo affinché la prima riga sia $1, 2, \ldots, n$.

Esempio 255. Consideriamo $f \in S_8$:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix}$$

Allora f^{-1} è

$$f^{-1} = \begin{pmatrix} 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 2 & 3 & 4 & 8 & 6 & 5 \end{pmatrix}$$

Consideriamo $g \in S_8$:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix}.$$

Allora g^{-1} è

$$g^{-1} = \begin{pmatrix} 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 7 & 8 & 4 & 2 & 3 & 5 \end{pmatrix}$$

Siamo ora interessati a determinare l'ordine di un qualsiasi elemento di S_n.

Definizione 75. (CICLO) Consideriamo il gruppo S_n e sia $k \leq n$. Un *ciclo* di lunghezza k si indica con $(a_1 a_2 \ldots a_k)$, dove $a_i \in \{1, \ldots, n\}$ sono tutti elementi distinti e senza virgole[20], ed è la permutazione f tale che:

$$f(a_1) = a_2, \ \ldots, f(a_i) = a_{i+1}, \qquad f(a_k) = a_1,$$

inoltre $f(b) = b$, per tutti gli elementi b non appartenenti al ciclo.

I cicli di lunghezza 2 sono detti *trasposizioni o scambi.*

Esempio 256. Sia $n = 8$ e $k = 4$ e consideriamo il ciclo di lunghezza 4 in S_8: (2481). Questo ciclo corrisponde alla permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 3 & 8 & 5 & 6 & 7 & 1 \end{pmatrix}.$$

Esempio $k = 5$, consideriamo il ciclo (13546) in S_8. Questo ciclo corrisponde alla permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 6 & 4 & 1 & 7 & 8 \end{pmatrix}.$$

[20]Noi non metteremo le virgole, ma alcuni testi usano la notazione con le virgole.

Esempio $k = 2$, il ciclo (87) in S_8 corrisponde alla permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 \end{pmatrix}.$$

Esercizio 57. In S_7 scrivere le permutazioni associate a (2345) e a (675412).

Osservazione 117. Il ciclo $(a_1 a_2 \dots a_k)$ di lunghezza k può scriversi anche come $(a_2 \dots a_k a_1)$ oppure $(a_3 a_4 \dots a_k a_1 a_2)$. In tutto ci sono k modi per scrivere uno stesso ciclo di lunghezza k.

Esempio 257. In S_8, ad esempio il ciclo (13546) di lunghezza $k = 5$ corrisponde alla permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 6 & 4 & 1 & 7 & 8. \end{pmatrix}$$

Questa permutazione corrisponde anche al ciclo (35461) = (54613) = (46135) = (61354).

Osservazione 118. In particolare, i cicli di lunghezza 1 fissano l'elemento, ad esempio (a) fissa l'elemento a.

Quindi dato un ciclo abbiamo una permutazione, vale il viceversa?

Teorema 23. *Ogni permutazione è un ciclo oppure può essere scritta come prodotto di cicli disgiunti.*

Non dimostriamo il teorema in generale ma vediamo come funziona negli esempi.
I cicli di lunghezza 1 fissano l'elemento e possono essere omessi.

Esempio 258. In S_8 abbiamo definito:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} = (1)(2345867) = (2345867),$$

dato che possiamo omettere il ciclo di lunghezza 1.

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix} = (126)(37)(458),$$

g corrisponde ad un prodotto di cicli di lunghezza 3,2,3.

Esempio 259. In S_{10} abbiamo:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 3 & 2 & 8 & 10 & 7 & 6 & 4 & 9 & 5 \end{pmatrix} = (1)(23)(48)(5\ 10)(67)(9),$$

o anche seplicemente $f = (23)(48)(5\ 10)(67)$.

Osservazione 119. Se i cicli sono disgiunti, ovvero gli elementi che compaiono nei cicli sono distinti allora i cicli commutano tra loro. Equivalentemente se due permutazioni agiscono su elementi distinti commutano.

Finalmente, usando la scrittura in cicli possiamo determinare l'ordine di una permutazione in S_n.

Teorema 24. *1) Un ciclo di lunghezza k ha ordine k (sapevamo già che aveva ordine finito, poichè siamo in un gruppo finito)*

2) L'ordine di una qualsiasi permutazione è il minimo comune multiplo della lunghezza dei suoi cicli disgiunti (nella scrittura come prodotto di cicli disgiunti).

Esempio 260. In S_8 abbiamo:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} = (1)(2345867),$$

quindi f ha ordine 7. Consideriamo

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix} = (126)(37)(458),$$

allora g ha ordine $mcm(3,2,3) = 6$, ovvero l'ordine di g è 6.

Che significa $o(g) = 6$? Significa che $| < g > | = 6$, che $g^6 = g \circ g \circ g \circ g \circ g \circ g = Id$ e che $< g >= \{g^0 = Id, g, g^2, g^3, g^4, g^5\}$. Verifichiamo

$$g^2 = g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 3 & 8 & 4 & 2 & 7 & 5 \end{pmatrix} = (162)(3)(7)(485);$$

$$g^3 = g \circ g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 4 & 5 & 6 & 3 & 8 \end{pmatrix} = (37);$$

$$g^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 3 & 5 & 8 & 1 & 7 & 4 \end{pmatrix} = (126)(458);$$

$$g^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 7 & 8 & 4 & 2 & 3 & 5 \end{pmatrix} = (162)(37)(485);$$

$$g^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = Id.$$

Usando i cicli possiamo studiare un'altra proprietà.

Teorema 25. *Ogni ciclo di lunghezza $k > 1$ può essere scritto (in maniera non unica) come prodotto di trasposizioni, ovvero di cicli di lunghezza 2.*

Dimostrazione. $(a_1 a_2 \dots a_k) = (a_1 a_k)(a_1 a_{k-1})(a_1 a_3)(a_1 a_2)$.

Esempio 261. In S_8 abbiamo:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} = (1)(2345867) = (27)(26)(28)(25)(24)(23).$$

Esempio 262. In S_8, $(458) = (48)(45)$ oppure $(458) = (584) = (54)(58)$. In particolare, non è unico il modo.

Osservazione 120. CONSEGUENZA: Ogni permutazione può essere scritta come prodotto di trasposizioni: per il Teorema 23 ogni permutazione la possiamo scrivere come prodotto di cicli disgiunti e poi, per il Teorema 25 ogni ciclo prodotto di trasposizioni.

Esempio 263. In S_8 abbiamo:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix} = (126)(37)(458) = (16)(12)(37)(48)(45).$$

Definizione 76. (PARI) Una permutazione si dice *pari* se è prodotto di un numero pari di trasposizioni. Si dice *dispari* se è prodotto di un numero dispari di trasposizioni.

Osservazione 121. La scrittura non è unica come prodotto di trasposizioni, come abbiamo visto nell'Esempio 262, ma si può dimostrare che la parità è ben definita ovvero non dipende dalla scelta della scrittura in trasposizioni.

Esempio 264. In S_8 abbiamo:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 8 & 7 & 2 & 6 \end{pmatrix} = (1)(2345867) = (27)(26)(28)(25)(24)(23),$$

ne segue che f è pari. Consideriamo

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 5 & 8 & 1 & 3 & 4 \end{pmatrix} = (126)(37)(458) = (16)(12)(37)(48)(45)$$

ne segue che g è dispari.

Esercizio 58. Si consideri in S_7 la seguente permutazione

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 2 & 3 & 4 & 1 \end{pmatrix}.$$

(1) Scrivere h come prodotto di cicli disgiunti.
(2) Stabilire se h è pari o dispari.
(3) Calcolare l'ordine di h in S_7.
(4) Calcolare h^{-1}.
(5) Calcolare esplicitamente gli elementi del sottogruppo H generato da h.

Esercizio 59. Si considerino in S_9 le seguenti permutazioni:

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 8 & 3 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 4 & 2 & 7 & 9 & 1 & 6 & 8 \end{pmatrix}.$$

(1) Scrivere h come prodotto di cicli disgiunti.
(2) Stabilire se h è pari o dispari.
(3) Scrivere l'immagine di 3 e 8 tramite g.
(4) Calcolare h^{-1}.
(5) Calcolare $h \circ g$ e $g \circ h$.
(6) Calcolare l'ordine di h.
(7) Calcolare esplicitamente gli elementi del sottogruppo generato da h.

16. Anelli e Campi (valido fino al 2024/2025)

La bandiera della Repubblica è il tricolore italiano: verde, bianco e rosso, a tre bande verticali di eguali dimensioni.

Nelle sezioni precedenti abbiamo studiato le strutture algebriche, che sono insiemi non vuoti su cui è definita una operazione. In particolare, ci siamo interessati allo studio dei gruppi.

In questa sezione ci dedichiamo allo studio degli anelli e dei campi, che sono insiemi con due operazioni.

Definizione 77. (ANELLO) Un *anello* $(A, +, \cdot)$ è un insieme A dotato di due operazioni $+ : A \times A \to A$ e $\cdot : A \times A \to A$ tale che

(1) $(A, +)$ è un gruppo abeliano (quindi l'operazione $+$ è associativa, commutativa, $\exists 0$ elemento neutro e $\forall a \in A$ esiste inverso-opposto).

(2) $(A, \cdot)$ è una struttura algebrica associativa.

(3) Valgono le leggi distributive del prodotto rispetto alla somma:

$$\forall a, b, c \in A \qquad \text{si ha che} \qquad a(b+c) = ab + bc, \qquad (a+b)c = ac + bc.$$

Osservazione 122. In un anello $(A, +, \cdot)$ è importante l'ordine in cui scriviamo le operazioni! Si richiede che $(A, +)$ sia un gruppo abeliano, mentre basta che $(A, \cdot)$ sia una struttura algebrica associativa.

Definizione 78. (ANELLO UNITARIO) Sia $(A, +, \cdot)$ un anello, se $(A, \cdot)$ è un monoide, ovvero se $\exists 1 \in A$ tale che $\forall a \in A$, $a \cdot 1 = 1 \cdot a = a$, l'anello si dice *anello unitario*.

Osservazione 123. Gli anelli unitari possiedono sia lo 0 che l'1 che sono gli elementi neutri di $+$ e $\cdot$.

Definizione 79. (ANELLO COMMUTATIVO UNITARIO) Sia $(A, +, \cdot)$ un anello unitario, se $(A, \cdot)$ è un monoide commutativo, ovvero se l'operazione $\cdot$ è commutativa (oltre ad essere associativa e ad ammettere elemento neutro), allora $(A, +, \cdot)$ si dice un *anello commutativo unitario*.

Esempio 265. $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario. Infatti, $(\mathbb{Z}, +)$ è gruppo e $(\mathbb{Z}, \cdot)$ è un monoide commutativo e valgono le proprietà distributive.

Analogamente, $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono anelli commutativi unitari.

$(\mathbb{N}, +, \cdot)$ non è un anello, perché $(\mathbb{N}, +)$ non è un gruppo.

$(\mathbb{Z}, \cdot, +)$ (con operazioni scambiate) non è un anello, perché $(\mathbb{Z}, \cdot)$ non è un gruppo.

$(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo unitario, finito.

Esempio 266. Nel Capitolo 19 studieremo l'anello delle matrici.

Definizione 80. (DIVISORE dello ZERO) In un anello $(A, +, \cdot)$, un elemento $a \in A$, con $a \neq 0$ si dice *divisore dello zero* se $\exists\ b \in A$ con $b \neq 0$ e

$$a \cdot b = b \cdot a = 0.$$

In tal caso anche b è divisore dello zero.

Esempio 267. Consideriamo l'anello $(\mathbb{Z}, +, \cdot)$ e ci chiediamo se esistono divisori dello zero, ovvero esiste $a \in \mathbb{Z}^*$ tale che esiste $b \in \mathbb{Z}^*$ con

$$a \cdot b = b \cdot a = 0$$

Non esistono: se il prodotto di due interi è zero uno dei due interi deve essere zero!

Analogamente, anche in $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ non esistono divisori dello zero.

Esempio 268. Consideriamo $(\mathbb{Z}_8, +, \cdot)$ e ci chiediamo se esistono divisori dello zero. Quindi ci chiediamo se esiste $[a]_8 \in \mathbb{Z}_8^*$ tale che esiste $[b]_8 \in \mathbb{Z}_8^*$ con

$$[a]_8 \cdot [b]_8 = [0]_8.$$

Per verificare questa condizione, basta che $ab \equiv 0 \pmod 8$. Ad esempio, $a = [2]_8 \neq [0]_8$ e $b = [4]_8 \neq [0]_8$, e $[2]_8 \cdot [4]_8 = [0]_8$. Oppure $a = [4]_8$ e $b = [6]_8$. Quindi $[2]_8, [4]_8$ e $[6]_8$ sono divisori dello zero in $\mathbb{Z}_8$.

Esempio 269. Consideriamo $(\mathbb{Z}_{12}, +, \cdot)$. Ad esempio $a = [3]_{12} \neq [0]_{12}$ e $b = [4]_{12} \neq [0]_{12}$ e $[3]_{12} \cdot [4]_{12} = [12]_{12} = [0]_{12}$. Quindi, $[3]_{12}$ e $[4]_{12}$ sono divisori dello zero in $\mathbb{Z}_{12}$.

Osservazione 124. In $(\mathbb{Z}_n, +, \cdot)$ con n non primo esistono SEMPRE dei divisori dello zero. Infatti se n non è primo allora $n = a \cdot b$ con $1 < a, b < n$ quindi esistono $[a]_n \neq 0$ e $[b]_n \neq 0$ con

$$[a]_n \cdot [b]_n = [n]_n = [0]_n.$$

Il caso di n numero primo lo studiamo nell'Osserervazione 126.

Definizione 81. (INVERTIBILE) In un anello unitario $(A, +, \cdot)$, un elemento $a \in A$, con $a \neq 0$ si dice *invertibile (o unitario)* se ammette un inverso rispetto al prodotto, ovvero se $\exists\ a' \in A$ con $a' \neq 0$ e

$$a \cdot a' = a' \cdot a = 1$$

In tal caso, l'inverso lo denotiamo con a^{-1}.

Osservazione 125. La definizione è la stessa di quella data per la struttura algebrica $(A, \cdot)$ (Definizione 61). In particolare, poiché $(A, \cdot)$ è un monoide, l'inverso se esiste è unico (Proposizione 12).

Esempio 270. Consideriamo $(\mathbb{Z}, +, \cdot)$ e ci chiediamo se esistono elementi invertibili? Si sono solo 1 e -1 (Esempio 225).

Esempio 271. In $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ ogni elemento non nullo è invertibile (Esempio 225).

Esempio 272. In $(\mathbb{Z}_n, +, \cdot)$ gli elementi inveritibili sono le classi $[a]_n$ con $MCD(a, n) = 1$ (Teorema 20).

In $(\mathbb{Z}_p, +, \cdot)$ con p numero primo, ogni elemento non nullo è invertibile.

Teorema 26. *In un anello unitario $(A, +, \cdot)$, se un elemento è invertibile allora non è un divisore dello zero.*

Dimostrazione. Sia $a \in A$ invertibile; quindi $a \neq 0$ ed esiste $a^{-1} \in A$, con $a^{-1} \neq 0$ tale che

$$a \cdot a^{-1} = a^{-1} \cdot a = 1. \tag{4}$$

Se a fosse un divisore dello zero, per definizione esisterebbe un elemento $b \neq 0 \in A$ tale che

$$a \cdot b = b \cdot a = 0.$$

Moltiplicando l'Equazione (4) $a \cdot a^{-1} = 1$ per b ottentiamo

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

e quindi $(b \cdot a) \cdot a^{-1} = b$. Dato che $b \cdot a = 0$, ne segue $0 = 0 \cdot a^{-1} = b$, ovvero $b = 0$ che è un assurdo.

Osservazione 126. Dato che in $(\mathbb{Z}_p, +, \cdot)$ con p numero primo, ogni elemento non nullo è invertibile allora non ci sono divisori dello zero.

Osservazione 127. Il viceversa del Teorema 26 non è sempre vero: se un elemento non è divisore dello zero non implica che è un elemento invertibile: esempio in $(\mathbb{Z}, +, \cdot)$ 3 non è né invertibile, né divisore dello zero.

PROPRIETÀ: Sia $(A, +, \cdot)$ un anello commutativo unitario finito, ovvero $|A| < +\infty$, allora ogni elemento non nullo o è invertibile o è un divisore dello zero.

Esempio 273. In $(\mathbb{Z}_8, +, \cdot)$, ogni elemento non nullo o è invertibile o è un divisore dello zero.

Gli invertibili, sono le classi $[a]_8$ con $MCD(a, 8) = 1$, quindi $[1]_8, [3]_8, [5]_8, [7]_8$.

I divisore dello zero sono $[2]_8, [4]_8, [6]_8$. Infatti $[2]_8 \cdot [4]_8 = [0]_8$ e $[6]_8 \cdot [4]_8 = [0]_8$.

Se vogliamo determinare gli inversi degli elementi invertibili abbiamo che $[1]_8$ è inverso di se stesso. Inoltre, l'inverso di $[3]_8$ è $[3]_8$ dato che $[3]_8 \cdot [3]_8 = [9]_8 = [1]_8$; l'inverso di $[5]_8$ è $[5]_8$ dato che $[5]_8 \cdot [5]_8 = [25]_8 = [1]_8$; l'inverso di $[7]_8$ è $[7]_8$ dato che $[7]_8 \cdot [7]_8 = [49]_8 = [1]_8$.

Esempio 274. In $(\mathbb{Z}_{10}, +, \cdot)$, ogni elemento non nullo o è invertibile o è un divisore dello zero.

Gli invertibili, sono le classi $[a]_{10}$ con $MCD(a, 10) = 1$, quindi $[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}$.

I divisore dello zero sono $[2]_{10}, [4]_{10}, [5]_{10}, [6]_{10}, [8]_{10}$. Infatti $[2]_{10} \cdot [5]_{10} = [0]_{10}$, $[4]_{10} \cdot [5]_{10} = [0]_{10}$, $[6]_{10} \cdot [5]_{10} = [0]_{10}$ e $[8]_{10} \cdot [5]_{10} = [0]_{10}$.

Se vogliamo determinare gli inversi degli elementi invertibili abbiamo che $[1]_{10}$ è inverso di se stesso. Inoltre, l'inverso di $[3]_{10}$ è $[7]_{10}$ dato che $[3]_{10} \cdot [7]_{10} = [21]_{10} = [1]_{10}$; l'inverso di $[9]_{10}$ è se stesso, infatti $[9]_{10} \cdot [9]_{10} = [81]_{10} = [1]_{10}$.

Esercizio 60. (casa) Determinare i divisori dello zero e gli invertibili negli anelli:

$$(\mathbb{Z}_{11}, +, \cdot) \qquad (\mathbb{Z}_{12}, +, \cdot) \qquad (\mathbb{Z}_{14}, +, \cdot).$$

Inoltre calcolare gli inversi.

Definizione 82. (CAMPO) Un anello commutativo unitario in cui ogni elemento non nullo è invertibile, si dice CAMPO. Si usa la notazione $(\mathbb{K}, +, \cdot)$.

Osservazione 128. Ovvero in un campo $(\mathbb{K}, +, \cdot)$, anche $(\mathbb{K}^*, \cdot)$ è un gruppo abeliano

Osservazione 129. Se in un anello c'è almeno un divisore dello zero allora l'anello non è un campo.

Esempio 275. $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ sono campi.

$(\mathbb{Z}, +, \cdot)$ non è un campo, esistono elementi non invertibili.

$(\mathbb{Z}_n, +, \cdot)$ con n non primo non è un campo, esistono divisori dello zero.

$(\mathbb{Z}_p, +, \cdot)$ con p primo è un campo.

17. Anelli e Campi (valido dal 2025/2026)

La bandiera della Repubblica è il tricolore italiano: verde, bianco e rosso, a tre bande verticali di eguali dimensioni.

Nelle sezioni precedenti abbiamo studiato le strutture algebriche, che sono insiemi non vuoti su cui è definita una operazione. In particolare, ci siamo interessati allo studio dei gruppi.

In questa sezione ci dedichiamo allo studio degli anelli e dei campi, che sono insiemi con due operazioni.

Definizione 83. (ANELLO) Un *anello* $(A, +, \cdot)$ è un insieme A dotato di due operazioni $+ : A \times A \to A$ e $\cdot : A \times A \to A$ tale che

(1) $(A, +)$ è un gruppo abeliano (quindi l'operazione $+$ è associativa, commutativa, $\exists 0$ elemento neutro e $\forall a \in A$ esiste inverso-opposto).

(2) $(A, \cdot)$ è una struttura algebrica associativa.

(3) Valgono le leggi distributive del prodotto rispetto alla somma:

$$\forall a, b, c \in A \qquad \text{si ha che} \qquad a(b+c) = ab + bc, \qquad (a+b)c = ac + bc.$$

Osservazione 130. In un anello $(A, +, \cdot)$ è importante l'ordine in cui scriviamo le operazioni! Si richiede che $(A, +)$ sia un gruppo abeliano, mentre basta che $(A, \cdot)$ sia una struttura algebrica associativa.

Definizione 84. (ANELLO UNITARIO) Sia $(A, +, \cdot)$ un anello, se $(A, \cdot)$ è un monoide, ovvero se $\exists 1 \in A$ tale che $\forall a \in A$, $a \cdot 1 = 1 \cdot a = a$, l'anello si dice *anello unitario.*

Osservazione 131. Gli anelli unitari possiedono sia lo 0 che l'1 che sono gli elementi neutri di $+$ e $\cdot$.

Definizione 85. (ANELLO COMMUTATIVO UNITARIO) Sia $(A, +, \cdot)$ un anello unitario, se $(A, \cdot)$ è un monoide commutativo, ovvero se l'operazione $\cdot$ è commutativa (oltre ad essere associativa e ad ammettere elemento neutro), allora $(A, +, \cdot)$ si dice un *anello commutativo unitario.*

Esempio 276. $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario. Infatti, $(\mathbb{Z}, +)$ è gruppo e $(\mathbb{Z}, \cdot)$ è un monoide commutativo e valgono le proprietà distributive.

Analogamente, $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono anelli commutativi unitari.

$(\mathbb{N}, +, \cdot)$ non è un anello, perché $(\mathbb{N}, +)$ non è un gruppo.

$(\mathbb{Z}, \cdot, +)$ (con operazioni scambiate) non è un anello, perché $(\mathbb{Z}, \cdot)$ non è un gruppo.

$(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo unitario, finito.

Esempio 277. Nel Capitolo 19 studieremo l'anello delle matrici.

Definizione 86. (INVERTIBILE) In un anello unitario $(A, +, \cdot)$, un elemento $a \in A$, con $a \neq 0$ si dice *invertibile (o unitario)* se ammette un inverso rispetto al prodotto, ovvero se $\exists\, a' \in A$ con $a' \neq 0$ e

$$a \cdot a' = a' \cdot a = 1$$

In tal caso, l'inverso lo denotiamo con a^{-1}.

Osservazione 132. La definizione è la stessa di quella data per la struttura algebrica $(A, \cdot)$ (Definizione 61). In particolare, poiché $(A, \cdot)$ è un monoide, l'inverso se esiste è unico (Proposizione 12).

Esempio 278. Consideriamo $(\mathbb{Z}, +, \cdot)$ e ci chiediamo se esistono elementi invertibili? Si sono solo 1 e -1 (Esempio 225).

Esempio 279. In $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ ogni elemento non nullo è invertibile (Esempio 225).

Definizione 87. (CAMPO) Un anello commutativo unitario in cui ogni elemento non nullo è invertibile, si dice CAMPO. Si usa la notazione $(\mathbb{K}, +, \cdot)$.

Osservazione 133. Ovvero in un campo $(\mathbb{K}, +, \cdot)$, anche $(\mathbb{K}^*, \cdot)$ è un gruppo abeliano

Esempio 280. $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ sono campi.

$(\mathbb{Z}, +, \cdot)$ non è un campo, esistono elementi non invertibili.

Si puo' dimostrare che $(\mathbb{Z}_n, +, \cdot)$ con n non primo non è un campo e che $(\mathbb{Z}_p, +, \cdot)$ con p numero primo è un campo.

Nel Capitolo 18, studieremo il campo $(\mathbb{C}, +, \cdot)$ dei numeri complessi.

18. Campo dei numeri complessi (A.A 2025/2026)

La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti. (....)

Questa sezione è dedicata allo studio di un esempio di campo: il campo dei numeri complessi.

Vogliamo definire un campo $(\mathbb{C}, +, \cdot)$. Sia $\mathbb{C} = \mathbb{R}\times\mathbb{R}$ ovvero ogni elemento dell'insieme $\mathbb{C}$ è una coppia di numeri reali. Definiamo le due operazioni:

$$+ : \mathbb{C}\times\mathbb{C}\to\mathbb{C} \qquad \forall\ (a,b),(c,d)\in\mathbb{C} \qquad (a,b)+(c,d)=(a+c,b+d)$$
$$\cdot : \mathbb{C}\times\mathbb{C}\to\mathbb{C} \qquad \forall\ (a,b),(c,d)\in\mathbb{C} \qquad (a,b)\cdot(c,d)=(ac-bd,bc+ad).$$

Esercizio 61. Verificare le seguenti proprietà:

(1) $+$ e $\cdot$ sono commutative e associative;

(2) $+$ ammette elemento neutro $(0,0)$, infatti $\forall (a,b)\in\mathbb{C}$ si ha che $(a,b)+(0,0) = (a+0,b+0) = (a,b) = (0,0)+(a,b)$;

(3) $\cdot$ ammette elemento neutro $(1,0)$, infatti $\forall (a,b)\in\mathbb{C}$ si ha che $(a,b)\cdot(1,0) = (1,0)\cdot(a,b) = (a,b)$;

(4) $\forall\ (a,b)\in\mathbb{C}$, esiste opposto (inverso rispetto a $+$) ed è $(-a,-b)\in\mathbb{C}$, infatti $(a,b)+(-a,-b) = (a-a,b-b) = (0,0) = (-a,-b)+(a,b)$;

(5) valgono le proprietà distributive: $\forall (a,b),(c,d),(s,t)\in\mathbb{C}$ si ha che

$$(a,b)((c,d)+(s,t)) = (a,b)(c,d)+(a,b)(s,t) \qquad ((a,b)+(c,d))(s,t) = (a,b)(s,t)+(c,d)(s,t).$$

Quindi affinché $(\mathbb{C}, +, \cdot)$ sia un campo, dobbiamo dimostrare che $\forall (a,b)\in\mathbb{C}^* = \mathbb{C}\setminus\{(0,0)\} = \mathbb{R}\times\mathbb{R}\setminus\{(0,0)\}$ esiste inverso, ovvero $\exists (x,y)\in\mathbb{C}^* = \mathbb{C}\setminus\{(0,0)\} = \mathbb{R}\times\mathbb{R}\setminus\{(0,0)\}$ tale che $(a,b)(x,y) = (x,y)(a,b) = (1,0)$. Verfichiamo:

$$(a,b)(x,y) = (ax-by, bx+ay) = (1,0) \iff \begin{cases} ax-by = 1 \\ bx+ay = 0. \end{cases}$$

Se $b = 0$ (di sicuro $a\neq 0$) allora basta prendere $x = \dfrac{1}{a}, y = 0$ infatti

$$(a,0)(\frac{1}{a},0) = (1,0).$$

Se $b\neq 0$ allora dalla prima equazione $y = \dfrac{ax-1}{b}$; sostituendo nella seconda equazione, otteniamo

$$bx+ay = bx+a(\frac{ax-1}{b}) = 0 \iff \frac{b^2x+a^2x-a}{b} = 0 \iff x(a^2+b^2) = a \iff$$
$$x = \frac{a}{a^2+b^2}.$$

Quindi

$$y = \frac{ax-1}{b} = \frac{a(\frac{a}{a^2+b^2})-1}{b} = \frac{\frac{a^2-a^2-b^2}{a^2+b^2}}{b} = \frac{-b}{a^2+b^2}.$$

(Notiamo che $a^2 + b^2 \neq 0$ quindi è tutto ben definito.)

Quindi per ogni $(a, b) \neq (0, 0) \in \mathbb{C}$ esiste l'inverso ed è:

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right). \tag{5}$$

L'insieme $(\mathbb{C}, +, \cdot)$ è un campo, detto il *campo dei numeri complessi*.

Ci chiediamo ora perché il campo dei numeri complessi è considerato come estensione dei numeri reali, oppure è il campo che contiene l'unità immaginaria i oppure è il campo dove esiste $\sqrt{-1}$.

Gli elementi della forma $(a, 0) \in \mathbb{C}$ sono identificati con i numeri reali $a \in \mathbb{R}$.

L'elemento $(0, 1)$ viene detto *unità immaginaria* e viene denotato con la lettera i.

Quindi ogni numero complesso $z = (a, b)$ ammette la seguente scrittura

$$(a, b) = (a, 0) + (0, b) = a + ib = a + bi,$$

dove abbiamo identificato $(a, 0)$ con $a \in \mathbb{R}$ e $(0, b) = (0, 1) + \cdots + (0, 1) = b \cdot (0, 1) = bi$.

La scrittura $a + bi$ è detta *scrittura in forma algebrica* di un numero complesso. Il numero reale a è detto *parte reale*, il numero reale b è detto *parte immaginaria*:

$$\text{se} \qquad z = a + bi \qquad \text{allora} \qquad Re(z) = a, \qquad Im(z) = b.$$

Esempio 281. Ad esempio se sonsideriamo
$z = (4, 5) = 4 + 5i$ allora $Re(z) = 4, \qquad Im(z) = 5$.
Se $z = 2 - i$ allora $Re(z) = 2, \qquad Im(z) = -1$.

Adesso consideriamo il numero complesso i, allora abbiamo che

(1) $i = (0, 1)$;

(2) $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$;

(3) $i^3 = (-1, 0)(0, 1) = (0, -1) = -i$;

(4) $i^4 = (-1, 0)(-1, 0) = (1, 0) = 1$.

Dato che $i^2 = -1$, si può dire che che i è radice di -1.

Usando la forma algebrica dei numeri complessi, si può fare direttamente la somma:

$$\forall\ z_1 = a + ib, z_2 = (c + id) \in \mathbb{C} \qquad z_1 + z_2 = (a + ib) + (c + id) = a + c + i(b + d).$$

Notiamo che coincide con la definizione di $+$ su $\mathbb{C}$, infatti

$$a + c + i(b + d) = (a + c, b + d) = (a, b) + (c, d).$$

Usando la forma algebrica dei numeri complessi, si può fare direttamente la moltiplicazione:

$$\forall\ z_1 = a + ib,\ z_2 = (c + id) \in \mathbb{C}$$

$$(a + ib)(c + id) = ac + iad + ibc + i^2bd = ac + iad + ibc - bd = (ac - bd) + i(ad + bc).$$

Notiamo che coincide con la definizione di $\cdot$ su $\mathbb{C}$, infatti

$$(ac - bd) + i(ad + bc) = (ac - bd, ad + bc) = (a, b) \cdot (c, d).$$

Esempio 282. Siano

$$z_1 = 3 + i \qquad \text{e} \qquad z_2 = 2 + 4i,$$

allora

$$z_1 + z_2 = 5 + 5i \qquad \text{e} \qquad z_1 z_2 = (3 + i)(2 + 4i) = 6 + 12i + 2i - 4 = 2 + 14i.$$

Siano

$$z_1 = \sqrt{2} - i \qquad \text{e} \qquad z_2 = 2i - 4,$$

allora

$$z_1 + z_2 = (\sqrt{2} - 4) + i \qquad \text{e} \qquad z_1 z_2 = (\sqrt{2} - i)(2i - 4) = (-4\sqrt{2} + 2) + i(2\sqrt{2} + 4).$$

Definizione 88. (CONIUGATO) Dato un numero complesso $z = a + ib$, si definisce *coniugato* di z e si indica con $\overline{z}$ il numero complesso

$$\overline{z} = a - ib;$$

ovvero, si cambia segno alla sola parte immaginaria.

Esempio 283. Nei seguenti numeri complessi abbiamo:

$$z_1 = 3 + i \qquad \overline{z_1} = 3 - i; \qquad z_2 = 2 - 4i \qquad \overline{z_2} = 2 + 4i;$$
$$z_3 = -\sqrt{2} - i \qquad \overline{z_3} = -\sqrt{2} + i; \qquad z_4 = 2i - 4 \qquad \overline{z_4} = -2i - 4.$$

Proprietà del coniugato: $\forall\ z, z_1, z_2 \in \mathbb{C}$ abbiamo

(1) $z + \overline{z} = 2Re(z)$;

(2) $z - \overline{z} = 2iIm(z)$;

(3) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$;

(4) $\overline{z_1 z_2} = \overline{z_1 z_2}$.

Definizione 89. (MODULO) Il *modulo* di un numero complesso $z = a + ib$ si indica con $|z|$ ed è il numero reale

$$|z| = \sqrt{a^2 + b^2} = \sqrt{Re(z)^2 + Im(z)^2} \in \mathbb{R}.$$

Esempio 284. Calcolare il modulo:

$$z_1 = 3 + i, \qquad |z_1| = \sqrt{9+1}; \qquad z_2 = 2 + 4i \qquad |z_2| = \sqrt{4+16};$$
$$\overline{z_1} = 3 - i, \qquad |\overline{z_1}| = \sqrt{9+1}; \qquad \overline{z_2} = 2 - 4i \qquad |\overline{z_2}| = \sqrt{4+16};$$
$$z_3 = \sqrt{2} - i \qquad |z_3| = \sqrt{2+1}; \qquad z_4 = 2i - 4 \qquad |z_4| = \sqrt{4+16};$$
$$z_5 = 2i \quad |z_5| = \sqrt{4} = 2; \qquad z_6 = -3 \quad |z_6| = \sqrt{9} = 3.$$

Proprietà del modulo: $\forall\ z \in \mathbb{C}$ si ha

(1) $|z| = |\overline{z}|$;

(2) $|z| \geq 0$ e $|z| = 0 \Longleftrightarrow z = 0$;

(3) $z\overline{z} = |z|^2$.

Per quanto riguarda la terza proprietà, se $z = a + ib \in \mathbb{C}$ si ha che

$$z \cdot \overline{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2.$$

Infine dato $z = a + ib$ vogliamo calcolare la forma algebrica dell'inverso.

Esempio 285. Consideriamo $z = 3 + i$, allora l'inverso $z^{-1} = \dfrac{1}{z} = \dfrac{1}{3+i}$, ma questo non è in forma algebrica ovvero del tipo $a + ib$.

Proposizione 17. *(INVERSO) Sia $z \in \mathbb{C}^*$ allora la forma algebrica dell'inverso è*

$$z^{-1} = \frac{1}{z} = \frac{1}{z} \cdot 1 = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2}.$$

Il denominatore è un numero reale non nullo, quindi è ben definito. Notiamo che se $z = a + ib = (a, b)$, allora

$$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{ib}{a^2 + b^2} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right),$$

ovvero coincide con la formula data dall'Equazione (5).

Esempio 286. Sia $z = 3 + i \in \mathbb{C}^*$, allora la forma algebrica dell'inverso è

$$z^{-1} = \frac{1}{z} = \frac{1}{3 + i} = \frac{3 - i}{(3 + i)(3 - i)} = \frac{3 - i}{10} = \frac{3}{10} - \frac{1}{10}i.$$

È possibile controllare i conti:

$$z \cdot z^{-1} = (3 + i)(\frac{3}{10} - \frac{1}{10}i) = 1.$$

Esercizio 62. Siano dati i seguenti numeri complessi:

$$z_1 = \sqrt{2} - i, \ z_2 = 2i - 4.$$

(1) Determinare il modulo di z_1 e z_2.
(2) Scrivere in forma algebrica i numeri complessi $\overline{z_1}$ e $\overline{z_2}$.
(3) Scrivere in forma algebrica i numeri complessi $z_1 z_2$, $\dfrac{1}{z_2}$ e $\dfrac{z_2}{z_1}$.

Soluzione 1. Già visti:

$$\overline{z_1} = \sqrt{2} + i \qquad \overline{z_2} = -2i - 4. \qquad |z_1| = \sqrt{2 + 1} \qquad |z_2| = \sqrt{4 + 16}.$$

Inoltre,

$$\frac{1}{z_2} = \frac{1}{2i - 4} = \frac{-2i - 4}{(-2i - 4)(2i - 4)} = \frac{-4}{20} + \frac{-2}{20}i = -\frac{1}{5} - \frac{1}{10}i;$$

$$\frac{z_2}{z_1} = \frac{2i - 4}{\sqrt{2} - i} = \frac{(2i - 4)(\sqrt{2} + i)}{(\sqrt{2} - i)(\sqrt{2} + i)} = \frac{(2i - 4)(\sqrt{2} + i)}{3} = \frac{(-2 - 4\sqrt{2}) + i(2\sqrt{2} - 4)}{3};$$

$$z_1 \cdot z_2 = (\sqrt{2} - i)(2i - 4) = (2 - 4\sqrt{2}) + i(4 + 2\sqrt{2}).$$

19. Matrici

La libertà personale è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge. (....)

Questa sezione è dedicata alle matrici come esempio di anello unitario (non commutativo).

Definizione 90. (MATRICE) Una matrice a coefficienti in un campo $(\mathbb{K}, +, \cdot)$ di tipo (m, n) è una tabella di $m \times n$ elementi di $\mathbb{K}$ organizzati in m righe ed n colonne. L'insieme delle matrici di tipo (m, n) a coefficienti in $\mathbb{K}$ si indica con $M_{m\times n}(\mathbb{K})$ (oppure $M_{m,n}(\mathbb{K})$).

Osservazione 134. A volte, soprattutto in alcuni linguaggi di programmazione, al posto di$M_{m\times n}(\mathbb{K})$ si usa $M(m, n, \mathbb{K})$.

Esempio 287. Matrice 3×3 a coefficienti in $\mathbb{R}$,

$$\begin{pmatrix} 1 & 2 & 3 \\ 6 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{R}),$$

Matrice 2×5 a coefficienti in $\mathbb{Q}$,

$$\begin{pmatrix} 0 & -\frac{5}{4} & 2 & -1 & 1 \\ 3 & 1 & \frac{1}{3} & 2 & 2 \end{pmatrix} \in M_{2\times 5}(\mathbb{Q})$$

Matrice 5×2 a coefficienti in $\mathbb{Q}$,

$$\begin{pmatrix} 0 & \frac{-4}{3} \\ 1 & 0 \\ 1 & -1 \\ 1 & -1 \\ -1 & 4 \end{pmatrix} \in M_{5\times 2}(\mathbb{Q})$$

In generale un elemento $A \in M_{m\times n}(\mathbb{K})$ è una tabella

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{pmatrix}$$

di m righe e n colonne. Il termine $a_{ij} \in \mathbb{K}$ indica l'elemento al posto (i, j) ovvero riga i e colonna j.

Notazione: Possiamo indicare in modo compatto una matrice $A = (a_{ij}) \in M_{m\times n}(\mathbb{K})$, con $i = 1, \ldots, m$ e $j = 1, \ldots, n$. Alcuni testi usano la notazione a^i_j per denotare l'elemento al posto (i, j).

Esempio 288. Consideriamo

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{R});$$

allora $a_{33} = 2, a_{13} = 3$ e $a_{31} = -1$.

Definizione 91. (TRASPOSTA) Data $A = (a_{ij}) \in M_{m\times n}(\mathbb{K})$. La matrice *trasposta* di A si denota con A^t ed è la matrice $A^t = (a_{ji})$ in $M_{n\times m}(\mathbb{K})$ ottenuta scambiando le righe e le colonne di A.

Notazione: Alcuni testi usano la notazione A^T oppure ${}^tA$ o ${}^TA$.

Esempio 289. Ad esempio

$$A = \begin{pmatrix} 0 & \sqrt{2} & 2 & -1 & 1 \\ 3 & 1 & 5 & 2 & 2 \end{pmatrix} \in M_{2\times 5}(\mathbb{R}) \Longrightarrow A^t = \begin{pmatrix} 0 & 3 \\ \sqrt{2} & 1 \\ 2 & 5 \\ -1 & 2 \\ 1 & 2 \end{pmatrix} \in M_{5\times 2}(\mathbb{R});$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \end{pmatrix} \in M_{2\times 3}(\mathbb{Q}) \Longrightarrow A^t = \begin{pmatrix} 1 & 0 \\ 2 & -1 \\ 3 & -2 \end{pmatrix} \in M_{3\times 2}(\mathbb{Q});$$

$$A = \begin{pmatrix} -5 & 4 \\ \frac{1}{2} & -\frac{3}{4} \end{pmatrix} \in M_{2\times 2}(\mathbb{Q}) \Longrightarrow A^t = \begin{pmatrix} -5 & \frac{1}{2} \\ 4 & -\frac{3}{4} \end{pmatrix} \in M_{2\times 2}(\mathbb{Q}).$$

Definizione 92. (QUADRATA) Se $n = m$ allora la matrice si dice *quadrata*. L'insieme $M_{n\times n}(\mathbb{K})$ si indica con $M_n(\mathbb{K})$.

Esempio 290. Ad esempio

$$\begin{pmatrix} 1 & 2 & 3 \\ 6 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \in M_3(\mathbb{R}); \qquad \begin{pmatrix} -5 & 4 \\ \frac{1}{2} & -\frac{3}{4} \end{pmatrix} \in M_2(\mathbb{Q}).$$

Definizione 93. Sia $A \in M_n(\mathbb{K})$ una matrice quadrata. Gli elementi $a_{ii} \in \mathbb{K}$ (ovvero $i = j$) costituiscono la *diagonale principale*.

Esempio 291. Ad esempio, in

$$\begin{pmatrix} 1 & -2 & 3 \\ 6 & 0 & -1 \\ -1 & -1 & 2 \end{pmatrix} \in M_3(\mathbb{R}),$$

gli elementi 1 0 2 costituiscono la diagonale principale

Definizione 94. (IDENTITÀ) In $M_n(\mathbb{K})$, la matrice *identità* è la matrice tale che $a_{ii} = 1$ e $a_{ij} = 0$ se $i \neq j$, ovvero ha tutti 1 sulla diagonale principale e zero altrove. Si indica con $Id_n \in M_n(\mathbb{K})$.

$$Id_1 = (1) \in M_1(\mathbb{K}) \qquad Id_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{K}) \qquad Id_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{K})$$

$$Id_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in M_n(\mathbb{K}).$$

Osservazione 135. La matrice identità è una matrice quadrata.

Definizione 95. (SOMMA) Sull'insieme delle matrici $M_{m\times n}(\mathbb{K})$ è possibile definire l'operazione di *somma*:

$+ : M_{m\times n}(\mathbb{K}) \times M_{m\times n}(\mathbb{K}) \to M_{m\times n}(\mathbb{K}) \qquad \forall A, B \in M_{m\times n}(\mathbb{K}) \qquad +(A, B) = A + B :$

data $A = (a_{ij})$ e $B = (b_{ij})$ allora $A + B = (a_{ij} + b_{ij})$, ovvero sommiamo termine a termine.

Osservazione 136. Le matrici sono dello stesso tipo (m, n).

Esempio 292. Siano

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 1 & 0 \end{pmatrix} \text{ e } C = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix},$$

con $A, B \in M_{3\times 3}(\mathbb{R})$ e $C \in M_{2\times 2}(\mathbb{R})$. Allora $A + C$ e $B + C$ non esistono e

$$A + B = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 6 \\ 8 & 4 & 7 \\ 0 & 2 & 2 \end{pmatrix}.$$

Esercizio 63. Data

$$D = \begin{pmatrix} -3 & 0 & 0 \\ -2 & 3 & -1 \\ 0 & 3 & 0 \end{pmatrix} \in M_{3\times 3}(\mathbb{R})$$

Calcolare $A + D, B + D$ e $D + C$, con A, B e C le matrici dell'Esempio 292.

Proprietà della somma di matrici in $M_{m\times n}(\mathbb{K})$:

(1) $+$ è commutativa: $\forall A, B \in M_{m\times n}(\mathbb{K})$, $A + B = B + A$;

(2) $+$ è associativa $\forall A, B, C \in M_{m\times n}(\mathbb{K})$, $(A + B) + C = A + (B + C)$;

(3) esiste in $M_{m\times n}(\mathbb{K})$ l'elemento neutro che si indica con 0 ed è la matrice con tutti i coefficienti zero, tale che $\forall A \in M_{m\times n}(\mathbb{K})$ si ha $A + 0 = 0 + A$;

(4) ogni elemento ammette inverso (opposto): $\forall A = (a_{ij}) \in M_{m\times n}(\mathbb{K}), \exists -A$ tale che $A + (-A) = (-A) + A = 0$, dove $-A = (-a_{ij})$, ovvero la matrice opposta è ottenuta dalla matrice A cambiando il segno a tutti i suoi coefficienti.

Quindi $(M_{m\times n}(\mathbb{K}), +)$ è un gruppo abeliano.

Esempio 293. Consideriamo in $M_{2\times 4}(\mathbb{R})$ la matrice

$$A = \begin{pmatrix} 0 & \sqrt{2} & 2 & -1 \\ -3 & 1 & \sqrt{3} & 2 \end{pmatrix};$$

allora

$$-A = \begin{pmatrix} 0 & -\sqrt{2} & -2 & 1 \\ 3 & -1 & -\sqrt{3} & -2 \end{pmatrix} \qquad \text{e} \qquad A + (-A) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Definizione 96. Per ogni $\lambda \in \mathbb{K}$ e per ogni $A = (a_{ij}) \in M_{m\times n}(\mathbb{K})$. Si definisce il prodotto $\lambda A = (\lambda a_{ij})$, la matrice ottenuta moltiplicando per λ ogni coefficiente di A.

Esempio 294. Siano $\lambda = 2 \in \mathbb{Q}$ e

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \end{pmatrix} \in M_{2\times 3}(\mathbb{Q}).$$

Allora

$$\lambda A = 2A = \begin{pmatrix} 2 & 4 & 6 \\ 0 & -2 & -4 \end{pmatrix} \in M_{2\times 3}(\mathbb{Q}).$$

Definizione 97. (PRODOTTO) 1) Due matrici A e B sono *moltiplicabili* (ovvero $\exists A \cdot B$) se e soltanto se il numero delle colonne di A è uguale al numero delle righe di B, ovvero se e solo se

$$A \in M_{m\times n}(\mathbb{K}) \qquad e \qquad B \in M_{n\times s}(\mathbb{K}).$$

2) Date due matrici moltiplicabili $A \in M_{m\times n}(\mathbb{K})$ e $B \in M_{n\times s}(\mathbb{K})$, il *prodotto* $A \cdot B$ è la matrice $A \cdot B \in M_{m\times s}(\mathbb{K})$, ottenuta moltiplicando le righe di A per le colonne di B, ovvero al posto (i, j) si ha

$$\sum_{t=1}^{n} a_{it} b_{tj}$$

(che è il prodotto tra gli elementi della riga i di A e gli elementi della colonna j di B).

Esempio 295. Consideriamo

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \end{pmatrix} M_{2\times 3}(\mathbb{Q}) \qquad B = \begin{pmatrix} -5 & -14 & -23 \\ \frac{1}{2} & \frac{7}{4} & 3 \end{pmatrix} M_{2\times 3}(\mathbb{Q}),$$

allora $A \cdot B$ non esiste e neanche $B \cdot A$!

Esempio 296. Siano date le seguenti matrici a coefficienti in $\mathbb{R}$

$$A = \begin{pmatrix} -5 & 4 \\ \frac{1}{2} & -\frac{3}{4} \end{pmatrix} \in M_{2\times 2}(\mathbb{R}) \qquad B = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \end{pmatrix} \in M_{2\times 3}(\mathbb{R});$$

allora $A \cdot B \in M_{2\times 3}(\mathbb{R})$ è:

$$A \cdot B = \begin{pmatrix} -5 & 4 \\ \frac{1}{2} & -\frac{3}{4} \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \end{pmatrix} = \begin{pmatrix} -5 & -14 & -23 \\ \frac{1}{2} & \frac{7}{4} & 3 \end{pmatrix}.$$

Il prodotto $B \cdot A$ non esiste.

Esempio 297. Siano date le seguenti matrici a coefficienti in $\mathbb{R}$

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_{2\times 2}(\mathbb{R}) \qquad B = \begin{pmatrix} 0 & 0 \\ 4 & 0 \end{pmatrix} \in M_{2\times 2}(\mathbb{R});$$

allora $A \cdot B \in M_{2\times 2}(\mathbb{R})$ è:

$$A \cdot B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$$

e $B \cdot A \in M_{2\times 2}(\mathbb{R})$ è:

$$B \cdot A = \begin{pmatrix} 0 & 0 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix}.$$

Osserviamo che $A \cdot B \neq B \cdot A$: il prodotto non è commutativo.

Esempio 298. Siano date le seguenti matrici a coefficienti in $\mathbb{R}$

$$A = \begin{pmatrix} 0 & 1 & 2 & -1 & 1 \\ 3 & 1 & 4 & 2 & 2 \end{pmatrix} \in M_{2\times 5}(\mathbb{R}), \qquad B = \begin{pmatrix} 0 & -\frac{4}{3} \\ 1 & 0 \\ 1 & -1 \\ 1 & -1 \\ -1 & 4 \end{pmatrix} \in M_{5\times 2}(\mathbb{R}).$$

Allora

$$A \cdot B = \begin{pmatrix} 1 & 3 \\ 5 & -2 \end{pmatrix} \in M_{2\times 2}(\mathbb{R}).$$

Esempio 299. Siano date le seguenti matrici a coefficienti in $\mathbb{R}$

$$A = \begin{pmatrix} 0 & 0 & 2 & -1 \\ 3 & 1 & -2 & 2 \end{pmatrix} \in M_{2\times 4}(\mathbb{R}), \qquad B = \begin{pmatrix} 0 & \frac{-4}{3} \\ 1 & 1 \\ 1 & -1 \\ 1 & -1 \end{pmatrix} \in M_{4\times 2}(\mathbb{R}).$$

Allora

$$A \cdot B = \begin{pmatrix} 1 & -1 \\ 1 & -3 \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$$

e

$$B \cdot A = \begin{pmatrix} 0 & \frac{-4}{3} \\ 1 & 1 \\ 1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 2 & -1 \\ 3 & 1 & -2 & 2 \end{pmatrix} = \begin{pmatrix} -4 & \frac{-4}{3} & \frac{8}{3} & -\frac{8}{3} \\ 3 & 1 & 0 & 1 \\ -3 & -1 & 4 & -3 \\ -3 & -1 & 4 & -3 \end{pmatrix} \in M_{4\times 4}(\mathbb{R}).$$

Da qui capiamo che la moltiplicazione non è commutativa, può non esistere e può essere diversa.

Osservazione 137. $\forall n \geq 1$, tutte le matrici in $M_n(\mathbb{K})$ sono moltiplicabili tra loro, e il prodotto è ancora una matrice in $M_n(\mathbb{K})$, ovvero esiste un prodotto

$$\cdot : M_n(\mathbb{K}) \times M_n(\mathbb{K}) \to M_n(\mathbb{K}) \qquad \forall A, B \in M_n(\mathbb{K}) \qquad \cdot (A, B) = A \cdot B.$$

Proprietà del prodotto in $M_n(\mathbb{K})$:

(1) $\cdot$ è associativa $\forall A, B, C \in M_n(\mathbb{K})$, $(A \cdot B) \cdot C = A \cdot (B \cdot C)$;

(2) esiste la matrice Identità $Id_n \in M_n(\mathbb{K})$ tale che $\forall A \in M_n(\mathbb{K})$ si ha $A \cdot Id_n = Id_n \cdot A = A$;

(3) valgono le proprietà distributive della somma rispetto al prodotto: $\forall A, B, C \in M_n(\mathbb{K})$ si ha

$$(A + B) \cdot C = A \cdot C + B \cdot C \quad \text{e} \quad A \cdot (B + C) = A \cdot B + A \cdot C.$$

Quindi $(M_n(\mathbb{K}), +, \cdot)$ è un *anello unitario non commutativo* (per $n > 1$). In particolare, non è un campo perché non è commutativo.

Vogliamo capire se esistono divisori dello zero ed elementi invertibili.

Esempio 300. Consideriamo $M_2(\mathbb{R})$

$$\begin{pmatrix} 0 & 0 \\ 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ -3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 3 & 2 \end{pmatrix}.$$

Quindi esistono divisori dello zero.

Definizione 98. (MATRICE INVERTIBILE) Sia $A \in M_n(\mathbb{K})$ una matrice quadrata, allora A è *invertibile* se e solo se esiste $A' \in M_n(\mathbb{K})$, tale che $A'A = AA' = Id_n$. Se A è invertibile la matrice A' è unica (Proposizione 12), si denota con A^{-1} e si chiama *matrice inversa* di A.

Vogliamo risolvere due **Problemi**:

Problema 1): Capire se una matrice è inveritibile.

Problema 2): Determinare la matrice inversa.

Soluzione del **Problema 1)**:

Teorema 27. *Sia $A \in M_n(\mathbb{K})$, allora A è invertibile se e solo se il determinate di A è diverso da zero: $det(A) \neq 0$*

Allora dobbiamo capire come è definito il determinante di una matrice quadrata.
Se $n = 1$ $A = (a) \in M_1(\mathbb{K})$, allora

$$det(A) = det(a) = a \in \mathbb{K}.$$

Se $n = 2$

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{K}) \qquad \text{e} \qquad det(A) = a_{11}a_{22} - a_{12}a_{21} \in \mathbb{K}.$$

Esempio 301. Consideriamo i seguenti esempi in $M_2(\mathbb{R})$

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 6 \end{pmatrix} \qquad det(A) = a_{11}a_{22} - a_{12}a_{21} = 6 - 8 = -2;$$

$$A = \begin{pmatrix} \sqrt{2} & -2 \\ 1 & 2 \end{pmatrix} \qquad det(A) = 2\sqrt{2} - (-2)(1) = 2\sqrt{2} + 2;$$

$$A = \begin{pmatrix} 1 & 2 \\ -2 & -4 \end{pmatrix} \qquad det(A) = -4 + 4 = 0.$$

Se $n > 2$ come possiamo definire $det(A)$?

Definizione 99. (DETERMINANTE) Sia $A \in M_n(\mathbb{K})$ una matrice quadrata, con $n \geq 2$. Il *determinante* di A, si indica con $det(A)$, ed è l'elemento di $\mathbb{K}$ (ovvero $det(A) \in \mathbb{K}$), dato dalla formula: per ogni i fissato

$$det(A) = \sum_{j=1}^{n} a_{ij}(-1)^{i+j} det(B_{ij}),$$

oppure per ogni j fissato

$$det(A) = \sum_{i=1}^{n} a_{ij}(-1)^{i+j} det(B_{ij}),$$

dove $(B_{ij}) \in M_{n-1}(\mathbb{K})$ è la matrice ottenuta dalla matrice A eliminando la riga i e la colonna j. Ovvero il determinante della matrice A è ottenuto sommando su una qualsiasi riga (prima formula) o su una qualsiasi colonna (seconda formula) il prodotto di ogni elemento a_{ij} della riga (o della colonna) per $(-1)^{i+j}$ per il determinante della matrice ottenuta dalla matrice A eliminando la riga i e la colonna j. Questa formula viene chiamata *Regola di Laplace*.

Osservazione 138. Si dimostra che non dipende dalla scelta della riga o della colonna.

Esempio 302. Verifichiamo la formula per $n = 2$. Scegliendo la prima riga, otteniamo

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad det(A) = a_{11}(-1)^{1+1}a_{22} + a_{12}(-1)^{1+2}a_{21} = a_{11}a_{22} - a_{12}a_{21}.$$

Esempio 303. Sia data la seguente matrice $A \in M_2(\mathbb{R})$, scegliendo la prima riga otteniamo

$$A = \begin{pmatrix} \sqrt{2} & -2 \\ 1 & 2 \end{pmatrix} \qquad det(A) = 2\sqrt{2} - (-2) \cdot 1 = 2\sqrt{2} + 2;$$

scegliendo la prima colonna, otteniamo lo stesso risultato

$$det \begin{pmatrix} \sqrt{2} & -2 \\ 1 & 2 \end{pmatrix} = \sqrt{2}(2) - (1)(-2) = 2\sqrt{2} + 2.$$

Esempio 304. Consideriamo in $M_3(\mathbb{R})$

$$A = \begin{pmatrix} 3 & -3 & \frac{1}{3} \\ 0 & 4 & 1 \\ -1 & -1 & -1 \end{pmatrix}.$$

Scegliendo la prima riga, abbiamo

$$det \begin{pmatrix} 3 & -3 & \frac{1}{3} \\ 0 & 4 & 1 \\ -1 & -1 & -1 \end{pmatrix} =$$

$$3(-1)^{1+1} det \begin{pmatrix} 4 & 1 \\ -1 & -1 \end{pmatrix} + (-3)(-1)^{1+2} det \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} + \frac{1}{3}(-1)^{1+3} det \begin{pmatrix} 0 & 4 \\ -1 & -1 \end{pmatrix} =$$

$= 3(-3) + 3 + \frac{1}{3}4 = -9 + 3 + \frac{4}{3} = -6 + \frac{4}{3} = -\frac{14}{3}$.

Scegliendo la prima colonna, otteniamo lo stesso risultato

$$det\begin{pmatrix} 3 & -3 & \frac{1}{3} \\ 0 & 4 & 1 \\ -1 & -1 & -1 \end{pmatrix} = 3(-1)^{1+1} det\begin{pmatrix} 4 & 1 \\ -1 & -1 \end{pmatrix} + (-1)(-1)^{3+1} det\begin{pmatrix} -3 & \frac{1}{3} \\ 4 & 1 \end{pmatrix} =$$

$$= -9 - (-3 - \frac{4}{3}) = -9 + \frac{13}{3} = -\frac{14}{3}.$$

Definizione 100. (COMPLEMENTO ALGEBRICO) Sia $A \in M_n(\mathbb{K})$ una matrice quadrata, il *complemento algebrico* del suo elemento a_{ij} è il prodotto $(-1)^{i+j} det(B_{ij})$ dove la matrice B_{ij} è ottenuta da A eliminando la riga i e la colonna j.

Esempio 305. Consideriamo in $M_3(\mathbb{R})$

$$A = \begin{pmatrix} 3 & -3 & \frac{1}{3} \\ 0 & 4 & 1 \\ -1 & -1 & -1 \end{pmatrix}.$$

Allora il complemento algebrico di a_{11} è $(-1)^{1+1} det\begin{pmatrix} 4 & 1 \\ -1 & -1 \end{pmatrix} = -4 + 1 = -3$;

il complemento algebrico di a_{12} è $(-1)^{1+2} det\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = -1$;

il complemento algebrico di a_{32} è $(-1)^{3+2} det\begin{pmatrix} 3 & \frac{1}{3} \\ 0 & 1 \end{pmatrix} = -3$.

Osservazione 139. Il determinante di una matrice $A \in M_n(\mathbb{K})$ è ottenuto sommando su una qualsiasi riga (prima formula) o su una qualsiasi colonna (seconda formula) il prodotto di ogni elemento della riga (o della colonna) per il suo complemento algebrico.

Soluzione del **Problema 2)**:

Definizione 101. (MATRICE INVERSA) Sia $A \in M_{n\times n}(\mathbb{K})$ con $det(A) \neq 0$. Allora la matrice *inversa* di A è A^{-1} dove

$$A^{-1} = \frac{1}{det(A)}(trasposta\ matrice\ complementi\ algebrici) = \frac{1}{det(A)}(matrice\ complementi\ algebrici)^t,$$

dove la matrice dei complementi algebrici è ottenuta scrivendo al posto di ogni elemento(i, j) il complemento algebrico dell'elemento $a_{i,j}$.

Osservazione 140. L'inversa di una matrice esiste se e solo se :

(1) la matrice è quadrata;

(2) il determinante è diverso da zero.

Per determinare l'inversa si deve:
1) calcolare il determinante;
2) calcolare i complementi algebrici;
3) determinare la matrice dei complementi algebrici;
4) determinare la trasposta;
5) dividere per determinante.
(Possiamo anche fare prima la divisione per il determinante e poi la trasposta).

Esempio 306. Determinare, se esiste, la matrice inversa di

$$A = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix} \in M_{2\times 2}(\mathbb{R}).$$

Si ha che

$$det(A) = 3 + 4 = 7 \neq 0,$$

quindi è invertibile.

Determiniamo i complementi algebrici:
il complemento algebrico di a_{11} è 3;
il complemento algebrico di a_{12} è -2;
il complemento algebrico di a_{21} è 2;
il complemento algebrico di a_{22} è 1.
Quindi la matrice dei complementi algebrici è

$$\begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix}.$$

Applicando la trasposta e dividendo per $det(A)$, si ottiene

$$A^{-1} = \begin{pmatrix} \frac{3}{7} & \frac{2}{7} \\ \frac{-2}{7} & \frac{1}{7} \end{pmatrix}.$$

Controllo:

$$AA^{-1} = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} \frac{3}{7} & \frac{2}{7} \\ \frac{-2}{7} & \frac{1}{7} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Esempio 307. Determinare, se esiste, la matrice inversa di

$$C = \begin{pmatrix} -6 & 1 & -4 \\ 0 & 3 & 4 \\ -2 & -1 & -2 \end{pmatrix} \in M_{3\times 3}(\mathbb{R}).$$

Si ha che

$$det(C) = -6det\begin{pmatrix} 3 & 4 \\ -1 & -2 \end{pmatrix} - 2det\begin{pmatrix} 1 & -4 \\ 3 & 4 \end{pmatrix} = -6(-6+4) - 2(4+12) = +12 - 32 = -20,$$

quindi è invertibile. Determiniamo i complementi algebrici:
il complemento algebrico di a_{11} è -2
il complemento algebrico di a_{12} è -8
il complemento algebrico di a_{13} è 6
il complemento algebrico di a_{21} è 6
il complemento algebrico di a_{22} è 4
il complemento algebrico di a_{23} è -8
il complemento algebrico di a_{31} è 16
il complemento algebrico di a_{32} è 24
il complemento algebrico di a_{33} è -18
Quindi la matrice dei complementi algebrici è

$$\begin{pmatrix} -2 & -8 & 6 \\ 6 & 4 & -8 \\ 16 & 24 & -18 \end{pmatrix}.$$

Applicando la trasposta, si ottiene

$$\begin{pmatrix} -2 & 6 & 16 \\ -8 & 4 & 24 \\ 6 & -8 & -18 \end{pmatrix}.$$

Infine dividendo per $det(C) = -20$, si ottiene

$$C^{-1} = \begin{pmatrix} \frac{1}{10} & \frac{-3}{10} & \frac{-4}{5} \\ \frac{2}{5} & \frac{-1}{5} & \frac{-6}{5} \\ \frac{-3}{10} & \frac{2}{5} & \frac{9}{10} \end{pmatrix}.$$

20. Grafi

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Definizione 102. (GRAFO) Un grafo (semplice) G è una coppia (V, L) dove

(1) V è un insieme non vuoto, i cui elementi si chiamano *vertici* del grafo, o nodi o punti.

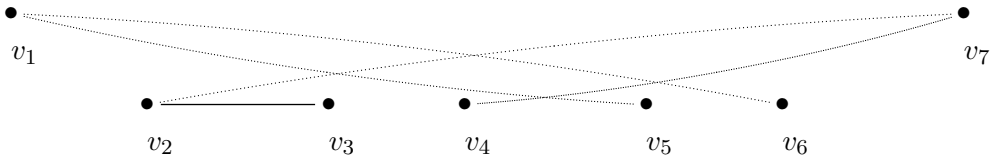
(2) L è un sottoinsieme dell'insieme costituito da due elementi di V, ovvero $L \subseteq \{$ sottoinsiemi di V con 2 elementi $\}$. Gli elementi di L sono detti *lati (o archi o spigoli)* del grafo; se $l = \{v, w\}$ allora v e w sono detti estremi del lato.

Al posto di L si usa anche la notazione E, per indicare *edges*.

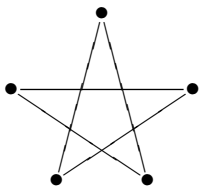
Osservazione 141. Siamo interessati ai grafi finiti ovvero V è un insieme finito. Se $|V| = 1$, allora il grafo ha un unico vertice senza alcun lato. Se $|V| = n \geq 2$ allora anche L è un insieme finito, dato che $|L| \leq \binom{n}{2}$. Infatti, $\binom{n}{2}$ è il numero di sottoinsiemi con due elementi (Sezione 8.1.2).

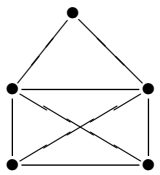
Esempio 308. Rappresentazione dei grafi: un punto per ogni vertice e una linea tra due punti (vertici) se esiste il lato.

Esempio 309. $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ e $L = \{l_1 = \{v_1, v_6\}, l_2 = \{v_1, v_5\}, l_3 = \{v_2, v_3\}, l_4 = \{v_7, v_4\}, l_5 = \{v_2, v_7\}\}$



Esempio 310. Altri esempi.





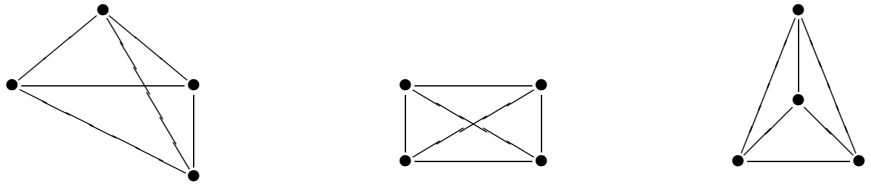
Definizione 103. (ISOMORFISMO) Un isomorfismo di grafi $G = (V, L) \to G' = (V', L')$ è una biezione di insiemi, $f : V \to V'$ tale che $\forall v, w \in V$ si ha

$$\{v, w\} \in L \iff \{f(v), f(w)\} \in L';$$

ovvero esiste un lato tra v e w in G se e solo se esiste un lato tra $f(v)$ e $f(w)$ in G'. (In particolare hanno lo stesso numeri di vertici e di lati.)

Osservazione 142. Quindi il grafo non dipende dalla rappresentazione usata.

Esempio 311. Queste sono rappresentazioni di uno stesso grafo.



Osservazione 143. Per come abbiamo dato la definizione di grafo (semplice), stiamo considerando sottoinsiemi $\{v, w\}$ di due elementi. Quindi $v \neq w$, ovvero il grafo non contiene lati della forma $\{v\} = \{v, v\}$, quelli che vengono chiamati *cappi* o *loop*.

Inoltre, $\{v, w\} = \{w, v\}$, quindi non abbiamo un verso di percorrenza del lato.

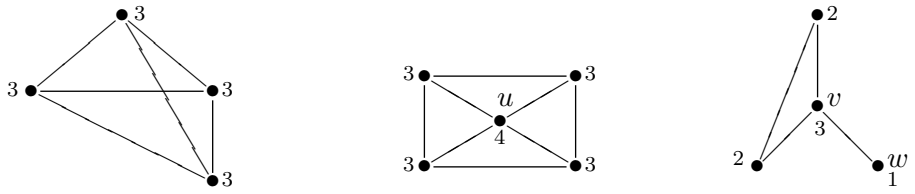
Infine, fissati due vertici in un grafo, allora esiste al più un lato tra essi, una coppia $\{v, w\}$ è presa al più una volta, ovvero non abbiamo i cosidetti lati *multipli*.

Si può generalizzare la definizione, introducendo i grafi orientati, multigrafi, etc.

Noi studiamo solo grafi semplici. Con la parola grafo intendiamo un grafo semplice e quindi senza loops e senza lati multipli.

Definizione 104. (GRADO o VALENZA) Siano $G = (V, L)$ un grafo finito e $v \in V$ vertice di G. Diremo che v ha *grado* n o v ha *valenza* n, e scriveremo $d(v) = n$ se v appartiene ad n lati. Inoltre, v si dice pari o dispari se $d(v)$ è pari o dispari, rispettivamente. Se $d(v) = 0$, allora v è detto vertice isolato.

Esempio 312. Determinare le valenze dei vertici nei seguenti grafi.

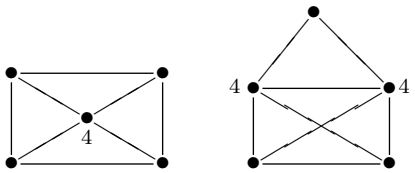


Nel primo grafo tutti i vertici hanno grado 3. Nel secondo grafo tutti i vertici hanno grado 3 tranne il vertice u che ha grado 4. Infine, nel terzo grafo il vertice v ha grado 3, il vertice w ha grado 1 e i due vertici restanti hanno grado 2.

Osservazione 144. In un grafo con n vertici, il grado di un vertice è al massimo $n - 1$.

Osservazione 145. Se due grafi sono isomorfi, allora i vertici che sono in biezione hanno lo stesso grado.

Esempio 313. I seguenti grafi non sono isomorfi in quanto nel primo grafo c'è solo un vertice di grado 4 mentre nel secondo grafo esistono 2 vertici con tale grado.



Teorema 28. *(Teorema delle strette di Mano) Il numero dei lati in un grafo finito $G = (V, L)$ è tale che:*

$$2 \mid L \mid = \sum_{v \in V} d(v).$$

Per i più curiosi:

Dimostrazione. (Non inclusa nel Programma)

Contiamo gli estremi dei lati: ogni lato ha due estremi, quindi ci sono $2 \mid L \mid$ estremi.

Contiamo ora gli estremi, contando i vertici: ogni vertice è estremo di $d(v)$ lati. Quindi, ogni estremo lo abbiamo contato $d(v)$ volte. Quindi in tutto $\sum_{v \in V} d(v)$.

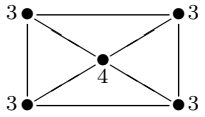
Pertanto,

$$2 \mid L \mid = \sum_{v \in V} d(v).$$

Corollario 1. *Ogni grafo finito $G = (V, L)$ ha un numero pari di vertici dispari.*

Dimostrazione. Per il Teorema delle strette di mano (Teorema 28), $\sum_{v \in V} d(v)$ deve essere un numero pari.

Esempio 314. Ad esempio, nel grafo

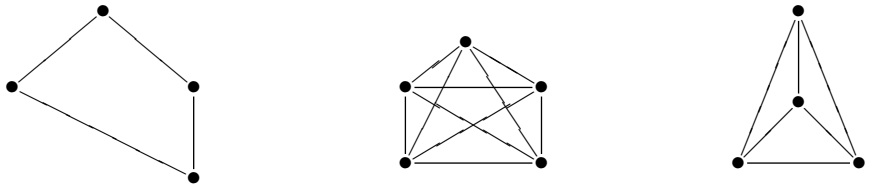


abbiamo

$$2 \mid L \mid = 2 \cdot 8 = 16 \qquad \text{e} \qquad \sum_{v \in V} d(v) = 3 + 3 + 3 + 3 + 4 = 16.$$

Esempio 315. Esiste un grafo con solo 3 vertici di grado tre? No.

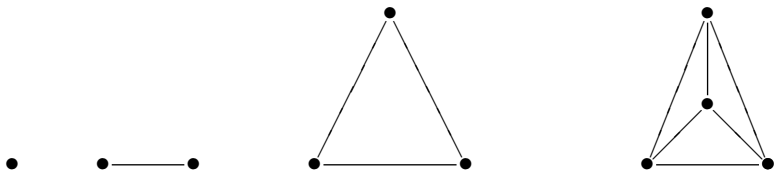
Esempio 316. Altri esempi di grafi.



Definizione 105. (COMPLETO) Un grafo si dice *completo* se per ogni coppia di vertici esiste un lato che li congiunge.

Osservazione 146. Per ogni $n \geq 1$ esiste un unico (a meno di isomorfismi) grafo completo con n vertici e si denota con K_n. Quindi K_1 è il grafo con solo un vertice e senza lati. Per ogni $n \geq 2$, K_n ha il massimo numero di lati possibile ovvero $|L| = \binom{n}{2}$: ogni vertice di K_n ha grado/valenza $n - 1$.

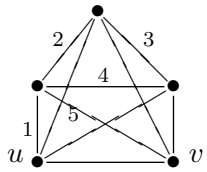
Esempio 317. Rappresentazione grafica di K_1, K_2, K_3 e K_4.



Esercizio 64. Disegnare K_5, K_6 e K_7.

Definizione 106. (CAMMINO) Sia $G = (V, L)$ un grafo. Un *cammino* di estremi v e w è una successione finita di lati a due a due distinti tra v e w: $l_1 = \{v, v_2\}, l_2 = \{v_2, v_3\}, \cdots, l_n = \{v_n, w\}$. In tal caso diremo che n è la *lunghezza del cammino* tra v e w e i vertici v e w sono detti *vertici* o *estremi del cammino*.

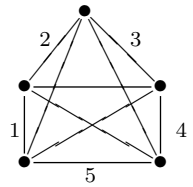
Esempio 318. Cammino da u a v, percorrendo i lati $1, 2, 3, 4$ e 5.



Osservazione 147. Se i lati non sono distinti si chiama *percorso*.

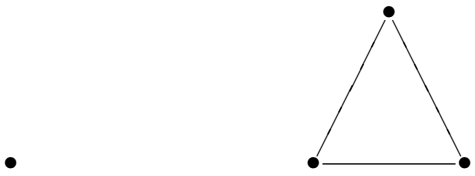
Definizione 107. (CIRCUITO) Un *circuito* è un cammino di lunghezza $n > 0$, i cui estremi coincidono.

Esempio 319. Esempio di circuto, percorrendo i lati $1, 2, 3, 4$ e 5.



Definizione 108. (CONNESSO) Un grafo si dice *connesso* se per ogni v e w esiste un cammino tra v e w. Altrimenti il grafo si dice *sconnesso*.

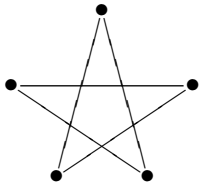
Esempio 320. Esempio di grafo sconnesso

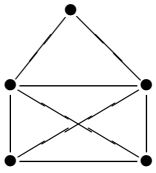


Definizione 109. (CAMMINO EULERIANO) Sia $G = (V, L)$ un grafo. Un *cammino Euleriano* è un cammino $l_1, l_2, \ldots, l_n$ che passa per tutti i lati del grafo, una unica volta.

Definizione 110. (CIRCUITO EULERIANO) Sia $G = (V, L)$ un grafo. Un *circuito Euleriano* è un circuito che passa per tutti i lati del grafo una unica volta (ovvero è un cammino euleriano con gli estremi che coincidono).

Esempio 321. Esistono cammini euleriani nei seguenti grafi? Esistono circuiti euleriani?





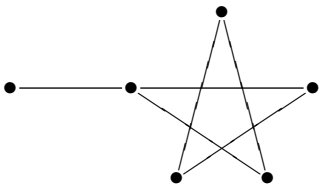
Come facciamo a capire se esistono?

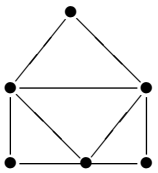
Teorema 29. *(di Eulero) Un grafo finito connesso con almeno due vertici ammette un circuito euleriano se e solo se tutti i suoi vertici sono pari.*

Corollario 2. *(di Eulero) Un grafo finito connesso con almeno due vertici ammette un cammino euleriano se e solo se ha al più due vertici dispari (quindi o 0 o 2).*

Infatti, se non ci sono vertici dispari allora esiste circuito euleriano, che è un particolare cammino euleriano. Se ci sono due vertici dispari, allora sono obbligatoriamente gli estremi del cammino euleriano.

Esempio 322. Stabilire se esistono cammini euleriani e circuiti euleriani nei seguenti grafi.

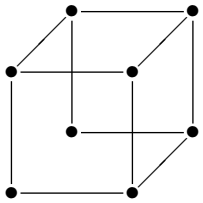


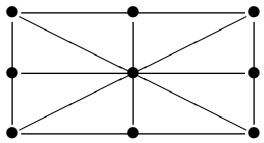


Esempio 323. Esempio dei Ponti di Königsberg di Eulero.[21]

Definizione 111. (CAMMINO HAMILTONIANO) Sia $G = (V, L)$ un grafo. Un *cammino Hamiltoniano*[22]è un cammino $l_1, l_2, \ldots, l_n$ che passa esattamente una volta per ogni vertice del grafo.

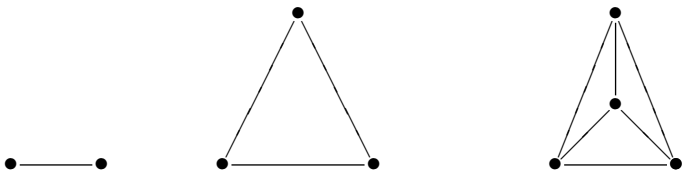
Esempio 324. Esistono cammini euleriani o hamiltoniani nei seguenti grafi?





Definizione 112. (BIPARTITO) Un grafo $G = (V, L)$ si dice *bipartito* se esiste una partizione (V_1, V_2) di V tale che ogni lato di G ha un estremo in V_1 e l'altro in V_2. Quindi, $V_1, V_2 \subseteq V$ non vuoti, $V_1 \cap V_2 = \emptyset$, $V_1 \cup V_2 = V$ (Definizione 45) e tra due vertici di V_1 o di V_2 non esistono lati.

Esempio 325. Consideriamo K_2, K_3 e K_4.



Il primo grafo è bipartito, negli altri due grafi non riusciamo a trovare una partizione.

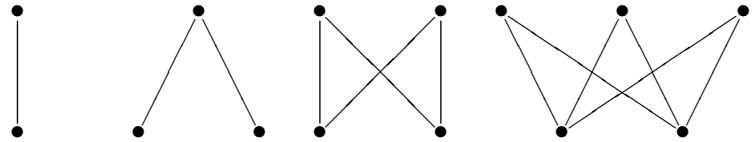
[21] Nel 1736, L. Eulero (1707-1783) ha affrontato e risolto il problema dei 7 ponti dando origine alla teoria dei grafi.

[22]W.R.Hamilton, 1805-1865, scienziato Irlandese.

Teorema 30. *Un grafo è bipartito se e solo se non ammette circuiti di lunghezza dispari.*

Osservazione 148. Per ogni $n, m \geq 1$, esistono i grafi $K_{n,m}$ che sono grafi bipartiti (completi) di $n+m$ vertici, con $|V_1| = n$ e $|V_2| = m$, ovvero per ogni vertice di V_1 e per ogni vertice di V_2 esiste un lato tra loro.

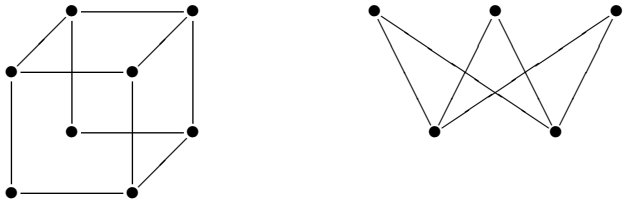
Esempio 326. I grafi $K_{1,1}$, $K_{1,2}$, $K_{2,2}$, $K_{3,2}$.



Esercizio 65. Disegnare $K_{3,3}$, $K_{4,3}$.

Definizione 113. (PLANARE) Un grafo si dice *planare* se può essere disegnato su un piano senza incroci, ovvero se i lati si incontrano al più nei vertici in comune. Quindi un grafo è planare se è isomorfo ad un grafo i cui lati distinti si intersecano al più nel loro estremi.

Esempio 327. Stabilire se i seguenti grafi sono planari.



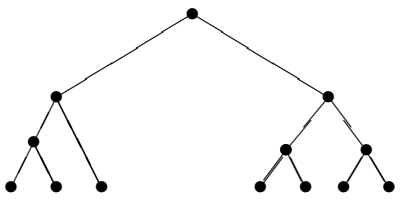
Osservazione 149. Per capire se un grafo è planare, dobbiamo capire se può essere rappresentato da un "disegno senza incroci". La rappresentazione scelta potrebbe non essere quella giusta. Quindi abbiamo bisogno di alcuni risultati che ci aiutino nella scelta.

Teorema 31. *(Teorema di Kuratowski[23]) Un grafo $G = (V, L)$ finito è planare se e solo se non contiene come sottografi K_5 o $K_{3,3}$ (o una loro espansione/suddivisione).*

Osservazione 150. Il precedente Teorema di Kuratowski si può enunciare equivalentemente: un grafo G non è planare se è K_5 o di $K_{3,3}$ o è ottenuto a partire da K_5 o da $K_{3,3}$, aggiungendo nuovi vertici e nuovi lati o aggiungendo uno o più vertici (su un unico lato alla volta) di K_5 o di $K_{3,3}$.

Definizione 114. (ALBERO) Un'*albero* è un grafo connesso privo di circuiti.

Esempio 328. Esempio di un albero.



[23] K. Kuratowski 1896-1980, matematico Polacco, il Teorema è del 1930.

Osservazione 151. Il nome deriva dalla rappresentazione. Possiamo fissare un qualsiasi vertice (detto anche radice). Poi si dispongono tutti gli altri vertici ad un livello più alto (risp. più basso).

Esempio 329. Esempio dei numeri di Fibonacci (Sezione 6.1).

Teorema 32. *Sia $G = (V, L)$ un grafo con $\mid V \mid = n$. Le seguenti affermazioni sono equivalenti tra loro:*

(1) *G è un albero.*

(2) *$\forall v, w \in V$, esiste ed unico il cammino tra v e w.*

(3) *G è privo di circuiti ed ha $n-1$ lati, ovvero $\mid L \mid = \mid V \mid -1$.*

(4) *G è un grafo connesso ed ha $n-1$ lati.*

Osservazione 152. Ogni albero è bipartito, dato che non ha circuiti (Teorema 30).

Vogliamo ora concentrarci sull'esistenza di alberi e grafi. In particolare, data una sequenza di numeri positivi esiste un albero o un grafo con queste determinate valenze. Per gli alberi il problema si risolve in maniera abbastanza semplice.

Teorema 33. *Siano n in $\mathbb{N}$ con $n \geq 2$ e $d_1, d_2, \ldots, d_n$ una sequenza di numeri naturali, tali che $1 \leq d_i \leq n-1$, per ogni $i = 1, \ldots, n$. Allora esiste un albero con n vertici di grado $d_1, d_2, \ldots, d_n$ se e solo se $\sum_{i=1}^{n} d_i = 2(n-1)$.*

Osservazione 153. Sappiamo che in un grafo con n vertici il grado di un vertice è al massimo $n-1$, per questo si richiede che $d_i \leq n-1$, per ogni $i = 1, \ldots, n$. Inoltre essendo un albero connesso, richiediamo $1 \leq d_i$.

Esempio 330. Esiste un albero avente 9 vertici, con solo 3 vertici di grado 3 e solo 3 vertici di grado 2 e nessuno di ordine maggiore?

Abbiamo $|V| = 9$, quindi $|L| = 8$; inoltre

$$16 = 2 \mid L \mid = \sum_{v \in V} d(v) = 3 \cdot 3 + 3 \cdot 2 + d(v) + d(w) + d(z),$$

ovvero $16 = 15 + d(v) + d(w) + d(z)$. Ma un albero è connesso quindi gli altri vertici devono avere grado 1. Allora 16=18 e questo è impossibile.

Esempio 331. Esiste un albero avente 9 vertici, con solo 2 vertici di grado 3 e solo 3 vertici di grado 2 e nessuno di ordine maggiore?

Abbiamo $|V| = 9$, quindi $|L| = 8$. Inoltre,

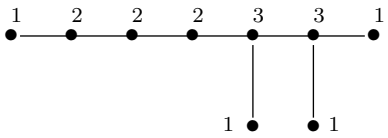
$$16 = 2 \mid L \mid = \sum_{v \in V} d(v) = 2 \cdot 3 + 3 \cdot 2 + d(v_1) + d(v_2) + d(v_3) + d(v_4).$$

Quindi, $16 = 12 + d(v_1) + d(v_2) + d(v_3) + d(v_4)$. Un albero è connesso, ne segue che $d(v_i)$ è maggiore o uguale ad 1, ovvero 1.

Quindi è un albero con 9 vertici: con solo 2 vertici di grado 3, solo 3 vertici di grado 2 e gli altri 4 vertici di grado 1. Non abbiamo contraddizioni, quindi tale albero esiste. Ad esempio



oppure, un altro albero, non isomorfo a quello precedente è



In generale, capire se esiste un grafo (semplice) con determinate valenze è un problema più complicato. Un algoritmo utile è basato sul seguente teorema.

Teorema 34. *(Hakimi-Havel) Sia $d_1, d_2, \ldots, d_n$ una successione di numeri naturali, tali che $d_1 > 0$ e $d_2 \geq d_3 \ldots \geq d_n > 0$. Allora esiste un grafo con n vertici di grado $d_1, d_2, \ldots, d_n$ se e solo se ne esiste uno con $n-1$ vertici di grado $d_2 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$.*

Dimostrazione. Idea della dimostrazione:

Considerare il grafo con $n-1$ vertici, ottenuto togliendo il vertice di grado d_1 e sottraendo 1 al grado di tanti vertici quanti è d_1.

Per Saperne di più. In Informatica, i grafi hanno numerose applicazioni. Ad esempio, intervengono per rappresentare una computer network, communication network, per studiare percorsi di logistica, per i circuiti stampati, per studiare mappe, nel design software, per capire come differenti moduli interagiscono tra loro.

Il problema dei grafi planari è di fondamentale importanza nella progettazione dei circuiti elettrici.

Check list. In questo capitolo abbiamo introdotto i grafi, abbiamo definito il grado di un vertice, i cammini, i circuiti, grafi conessi, completi, cammini Elureiani, circuiti euleriani, cammini hamiltoniani, grafi bipartiti, planari e alberi.

Index

∩ intersezione, 7
∪ unione, 7
∃ esiste, 6
∀ per ogni, 6
∑ sommatoria, 37

Algoritmo di Euclide, 59
Anelli, 97, 100
  Campo, 99, 101
  Commutativo unitario, 97, 100
  Divisore dello zero, 97
  Invertibile, 98, 100
  Unitario, 97, 100

Campo dei numeri complessi, 102
  Coniugato, 104
  forma algebrica, 103
  Inverso, 104
  Modulo, 104
  Parte Immaginaria, 103
  Parte reale, 103
  unità immaginaria, 103
Cardinalità di un Insieme
  Principio di Inclusione-Esclusione, 39
  Regola del Prodotto, 41
  Regola della Somma, 39
Cardinalità di un insieme, 26
Classe di equivalenza, 52
Coefficiente Binomiale, 43
  Proprietà, 44
Combinatoria, 42
  Combinazioni con ripetizioni, 47
  Combinazioni semplici, 43
  Disposizioni con ripetizioni, 46
  Disposizioni semplici, 42
Congruenza modulo n, 68
Congruenze, 68
  Classe di congruenza, 68
  Classe resto, 68
  Congruenza lineare, 72
  Esistenza soluzioni congruenza lineare, 72
  Proprietà delle congruenze, 69
  Sistema di congruenze, 74
  Soluzioni congruenza lineare, 72
  Teorema Cinese dei Resti, 75

Equazioni Diofantee, 62
  Esistenza Soluzione, 62
  Soluzioni, 63

Formula di Newton, 44
Funzione di Eulero, 70
  Proprietà, 70
Funzioni, 16
  Biettiva, 21
  Composizione, 22
  Controimmagine, 17
  Costante, 18
  Grafico, 19
  hash, 25
  Identica, 18
  Imamgine, 17
  Iniettiva, 19
  Inversa, 24
  Numero funzioni biettive tra insiemi finiti, 43
  Numero funzioni iniettive tra insiemi finiti, 43
  Numero funzioni tra insiemi finiti, 46
  Suriettiva, 20

Grafo, 114
  Albero, 119
  Bipartito, 118
  Cammino, 116
  Cammino Euleriano, 117
  Cammino Hamiltoniano, 118
  cappio, 115
  Circuito, 117
  Circuito Euleriano, 117
  Completo, 116
  Connesso, 117
  Grado, 115
  Isomorfismo, 114
  Loop, 115
  Percorso, 117
  Planare, 119
  Teorema delle strette di Mano, 115
  Valenza, 115
Gruppi, 82
  Abeliano, 82
  Ciclici, 85, 89
  Finito, 84
  Gruppo di permutazioni, 91
  Gruppo Simmetrico, 91
  Infinito, 84
  Ordine, 84
  Ordine di un elemento, 85, 88
  Sottogruppo, 85, 86
  Sottogruppo Ciclico, 85, 87
Gruppo di permutazioni, 91
  Ciclo, 93
  Composizione, 92
  Inverso, 93
  Ordine di una permutazione, 94
  Permutazione pari, 95
  Trasposizioni, 93

Identità di Bézout, 59
Insieme, 4
  Cardinalità insieme della parti, dim.1, 28
  Cardinalità insieme della parti, dim.2, 45
  Cardinalità, 26
  Complementare, 8
  Diagrammi di Venn, 5
  Differenza, 9
  Disgiunti, 7
  Equipotenti, 26
  Finito, 26
  Inclusione, 5
  Inclusione propria, 6
  Infinito, 27

Insieme delle Parti, 9
Insieme quoziente, 54
Intersezione, 7
Leggi di De Morgan, 8
Numerabile, 27
Partizione di un insieme, 54
Parzialmente ordinato, 51
Potenza del continuo, 27
Prodotto Cartesiano, 9
Totalmente ordinato, 51
Unione, 7
Vuoto, 4
Insieme Parzialmente Ordinato, 51

Matrici, 106
Complemento Algebrico, 112
Determinante, 111
Diagonale Principale, 107
Identità, 107
Inversa, 112
Invertibile, 110
Moltiplicabili, 108
Prodotto, 108
Quadrate, 107
Somma, 107
Trasposta, 107
Monoide, 78

Numeri di Fibonacci, 35
Numeri Fattoriali, 34
Numeri interi
Algoritmo di Euclide, 59
combinazione lineare, 57
Crivello di Eratostene, 67
divisione con resto, 57
divisore, 56
divisori di 1, 56
Fattorizzazione di Eratostene, 67
fattorizzazione in primi, 65
Identità di Bézout, 59
massimo comun divisore, 58
minimo comune multiplo, 61
multiplo, 56
numeri associati, 56
numeri coprimi, 59
numero dei divisori, 66
numero primo, 65
Numero primo, 65

Operazione, 77
Associativa, 77
Commutativa, 79

Partizione di un insieme, 54
Permutazione, 43
Principio di Induzione, 28
Generalizzato, 30
Proposizioni, 10
Congiunzione, 11
Connettivi logici, 10
Disgiunzione, 11
Doppia Implicazione, 13
Equivalenza, 13
Implicazione, 12
negazione, 10

Relazioni su un insieme, 49
Classe di equivalenza, 52
Elementi equivalenti, 51
Insieme quoziente, 54
Proprietà antisimmetrica, 50
Proprietà riflessiva, 49
Proprietà simmetrica, 51
Proprietà transitiva, 50
Relazione d'equivalenza, 51
Relazione d'ordine, 49
Relazione identica su un insieme, 49
Relazione totale su insieme, 49
Relazione vuota su un insieme, 49
Relazioni compatibili con operazioni, 82

Simbolo di Sommatoria, 37
Strutture Algebriche, 77
Anelli, 97, 100
Associativa, 77
Campo, 99, 101
Commutativa, 79
Elemento Neutro, 78
Gruppo, 82
Gruppo Abeliano, 82
Invertibili, 79
Monoide, 78
Monoide commutativo, 79
Monoide delle Parole, 78
Operazione, 77
Sottogruppo, 85, 86
Successione, 32
definita per ricorrenza, 33
formula chiusa, 33
Numeri di Fibonacci, 35
Torre di Hanoi, 36

Teorema
Piccolo Teorema di Fermat, 70
Teorema Cinese dei Resti, 75
Teorema dei numeri primi, 66
Teorema di Eulero Fermat, 71
Teorema di Fermat, 70
Teorema di Lagrange, 86
Teorema fondamentale dell'aritmetica, 65
Torre di Hanoi, 36
Triangolo di Tartaglia, 45