

TEORIA DEGLI INSIEMI

DEF - Un insieme è una collezione di oggetti, detti elementi.

Rappresentazione per elencazione $A = \{1, 2, a, n\}$

o per enumerazione della proprietà

$A = \{\text{lettere della parola casa}\} = \{e, a, s\} = \{s, e, a\}$

OSS - Non devono esserci ripetizioni, non importa l'ordine

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{-\dots, -1, 0, 1, \dots\}$$

$$\mathbb{Q} = \{m/n \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$$

$$\mathbb{R} = \{\text{numeri reali}\}$$

DEF - Chiamiamo singoletto di $a \in A$ l'insieme formato dal solo elemento a , $\{a\}$

DEF - Dato A insieme, un sottoinsieme di A è un insieme B tale che ogni elemento di B è anche elemento di A

$$B \subseteq A \quad \forall a \in B \Rightarrow a \in A$$

$$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

$B \not\subseteq A$ significa $\exists b \in B : b \notin A$

Se $A \subseteq B$ e $B \subseteq C \Rightarrow A \subseteq C$ l'inclusione è transitiva

PROP - $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

DEF - Inclusione stretta $A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$

$$(\forall a \in A \Rightarrow a \in B) \wedge (\exists b \in B : b \notin A)$$

$A \neq B \Leftrightarrow (\exists b \in B : b \notin A) \vee (\exists a \in A : a \notin B)$

DEF - Dato S insieme, si chiama insieme delle parti di S l'insieme dei sottoinsiemi di S

$$P(S) = \{X \text{ insieme} \mid X \subseteq S\}$$

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

$$P(S) = \{\emptyset, S, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$$

PROP- $S \subseteq T \Leftrightarrow P(S) \subseteq P(T)$

DIM- Ipotesi: $S \subseteq T$

Tesi: $\forall X \in P(S) \Rightarrow X \in P(T)$

$$\forall X \subseteq S \Rightarrow X \subseteq T ?$$

Se $X \subseteq S \wedge S \subseteq T$ allora $\underbrace{X \subseteq T}$

equivalente a $X \in P(T)$ \hookrightarrow

(\Leftarrow) Ipotesi: $P(S) \subseteq P(T)$

Tesi: $S \subseteq T$

per ipotesi $\forall X \in P(S) \Rightarrow X \in P(T)$

$$\forall X \subseteq S \Rightarrow X \subseteq T$$

allora $X = S$, ottengo $S \subseteq T$ \hookrightarrow

Relazione di divisibilità

$a | b$ (a divide b) $\Leftrightarrow \exists c : b = c \cdot a$

$a | 0$ $\forall a \in \mathbb{Z} \setminus \{0\}$ perché $0 = 0 \cdot a$

il divide è transitivo

DIM- $a | b \Leftrightarrow \begin{cases} \exists m : b = m \cdot a \\ b | c \Leftrightarrow \exists m : c = m \cdot b \end{cases} \left. \begin{array}{l} c = m(m \cdot a) = (m \cdot m)a \\ \Rightarrow a | c \end{array} \right\}$

\hookrightarrow

$\forall a, b \in \mathbb{N}_0 \quad a | b \wedge b | a \Rightarrow a = b$

DIM. $a | b \Leftrightarrow \begin{cases} \exists m : b = m \cdot a \\ b | a \Leftrightarrow \exists m : a = m \cdot b \end{cases} \left. \begin{array}{l} b = m \cdot m \cdot a \\ \Rightarrow m \cdot m = 1 \Rightarrow m = m = 1 \\ \text{da cui } b = 1 \cdot a = a \end{array} \right\}$

\hookrightarrow

Se $a | b \wedge a | c \Rightarrow a | b+c$

DIM- $a | b \Leftrightarrow \begin{cases} \exists m : b = m \cdot a \\ a | c \Leftrightarrow \exists m : c = m \cdot a \end{cases} \left. \begin{array}{l} b+c = m \cdot a + m \cdot a = (\underbrace{m+m)}_{\in \mathbb{Z}} a \Rightarrow a | b+c \end{array} \right\}$

\hookrightarrow

DEF - Un intervallo chiuso è un sottoinsieme di \mathbb{R} della forma

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\} \subseteq \mathbb{R}$$

è ben definito se $a \leq b$

$$\text{se } a = b \Rightarrow [a, b] = \{a\}$$

$$\text{se } a > b \Rightarrow [a, b] = \emptyset$$

OPERAZIONI TRA INSIEMI

UNIONE

Dati A, B insiemi $A \cup B := \{x \mid x \in A \vee x \in B\}$ per definizione

INTERSEZIONE

Dati A, B $A \cap B := \{x \mid x \in A \wedge x \in B\}$

• \cap e \cup sono COMMUTATIVE

• \cap e \cup sono ASSOCIATIVE $(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$

• $A \subseteq B \Rightarrow A \cap B = A$ e $A \cup B = B$

• $A \cap B \subseteq A$ $A \cap B \subseteq B$

• $A \subseteq A \cup B$ $B \subseteq A \cup B$

• Dato A insieme, consideriamo $P(A)$

$$\forall X \in P(A)$$

$$\left. \begin{array}{l} X \cap \emptyset = \emptyset \\ X \cup A = A \end{array} \right\} \text{ in } P(A), \emptyset \text{ è l'elemento neutro per } \cup$$

$$\left. \begin{array}{l} X \cup \emptyset = X \\ X \cap A = X \end{array} \right\} A \text{ è } // \text{ per } \cap$$

ES. $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\} = \text{multipli di } 3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$

$6\mathbb{Z} = \{6z \mid z \in \mathbb{Z}\} = \text{multipli di } 6 = \{\dots, -12, -6, 0, 6, 12, \dots\}$

$$\left. \begin{array}{l} 3\mathbb{Z} \cap 6\mathbb{Z} = 6\mathbb{Z} \\ 6\mathbb{Z} \subseteq 3\mathbb{Z} \end{array} \right\}$$

$$3 \in 3\mathbb{Z} \text{ ma } 3 \notin 6\mathbb{Z}$$

$$\forall m \in 6\mathbb{Z}, m = 6 \cdot z = 2 \cdot (3z) \in 3\mathbb{Z}$$

DIFFERENZA DI INSIEMI

Dati A, B insiemi

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

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

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

$$A \setminus B = \{b, c\}$$

$$B = \{a, f, g\}$$

$$B \setminus A = \{f, g\}$$

$$A \setminus \emptyset = A$$

$$\emptyset \setminus A = \emptyset$$

- In $P(A)$, $X \in P(A)$ $A \setminus X$ è detto complemento di X \bar{X}

$$(A \setminus X) \cup X = A$$

$$(A \setminus X) \cap X = \emptyset$$

Due insiemi S, T si dicono disgiunti se $S \cap T = \emptyset$

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

Dim.

$$\text{se } x \in A \cap (B \cup C) \Leftrightarrow x \in A \text{ e } x \in B \cup C \Leftrightarrow$$

$$\Leftrightarrow x \in A \text{ e } x \in B \text{ o } x \in C \Leftrightarrow x \in A \text{ e } x \in B \text{ o } x \in A \text{ e } x \in C \Leftrightarrow$$

$$\Leftrightarrow x \in (A \cap B) \text{ o } x \in (A \cap C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$$

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

Dim.

$$\text{se } x \in A \cup (B \cap C) \Leftrightarrow x \in A \text{ o } x \in B \cap C \Leftrightarrow$$

$$\Leftrightarrow x \in A \text{ o } x \in B \text{ e } x \in C \Leftrightarrow x \in A \text{ o } x \in B \text{ e } x \in A \text{ o } x \in C \Leftrightarrow$$

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

PRODOTTO CARTESIANO DI INSIEMI

A, B insiemi - il prodotto cartesiano è l'insieme

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

$$\text{se } |A|=m \text{ e } |B|=n \quad |A \times B|=m \cdot n$$

$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 \Rightarrow$ il piano cartesiano

DEF. - Una relazione è un sottoinsieme del prodotto cartesiano
di due insiemi S, T $R \subseteq S \times T$

DEF - Dato A insieme, ΔA diagonale di A = $\{(x,y) \in A \times A \mid x=y\} \subseteq A \times A$

Dato $R \subseteq A \times B$, questa è detta

- Vuota $\Rightarrow R = \emptyset$
- Totale $\Rightarrow R = A \times B$
- Bimaria $\Rightarrow A = B$
- Identità $\text{id}_A \subseteq A \times A$, $\text{id}_A = \Delta_A$
- Opposta $R^{\text{opp.}} = \{(y,x) \in A \times B \mid (x,y) \in R\}$

Proprietà del prodotto cartesiano

$$S \subseteq A \wedge T \subseteq B \Leftrightarrow S \times T \subseteq A \times B$$

DIM -

$$\begin{aligned} (\Rightarrow) \quad (x,y) \in S \times T &\Rightarrow x \in S \wedge y \in T \Rightarrow \text{per ipotesi } \left. \begin{array}{l} S \subseteq A \\ T \subseteq B \end{array} \right\} \Rightarrow \left. \begin{array}{l} x \in A \\ y \in B \end{array} \right\} \\ &\Rightarrow (x,y) \in A \times B \quad \text{allora } S \times T \subseteq A \times B \end{aligned}$$

$$(\Leftarrow) \quad \text{Per ipotesi } S \times T \subseteq A \times B$$

$$\text{Sia } x \in S \text{ e } y \in T \Rightarrow (x,y) \in S \times T \Rightarrow (x,y) \in A \times B \Rightarrow$$

$$\Rightarrow x \in A \wedge y \in B \Rightarrow \text{allora } S \subseteq A \wedge T \subseteq B$$

↳

TEOREMA

Dati A, B, C insiemi si ha:

$$1) (A \cup B) \times C = (A \times C) \cup (B \times C)$$

$$2) (A \cap B) \times C = (A \times C) \cap (B \times C)$$

$$3) (A \cdot B) \times C = (A \times C) \cdot (B \times C)$$

DIM -

$$① (x,y) \in (A \cup B) \times C \Leftrightarrow x \in A \cup B \wedge y \in C \Leftrightarrow$$

$$\Leftrightarrow x \in A \vee x \in B \wedge y \in C \Leftrightarrow (x,y) \in A \times C \cup (x,y) \in B \times C$$

$$\Leftrightarrow (x,y) \in (A \times C) \cup (B \times C) \quad \text{↳}$$

OSS - $R \subseteq A \times B$ $(x,y) \in R$ si scrive anche $x R y$

Ese. $N_0 \times \mathbb{Z}$

$$x R y \Leftrightarrow x+y=3 \quad \text{Fissato } x \exists ! y : x R y \quad (y=3-x)$$

In $N \times N$ non è una applicazione

$$(7) - 4 \in R$$

DEF -

1) $R \subseteq A \times B$ è detta **APPPLICAZIONE** (o funzione) se

$$\forall x \in A \exists ! y \in B : x R y$$

Si scrive come $R: A \rightarrow B$ $x R y$ chiamata $R(x) = y$

A è detto dominio di R

B è detto codominio di R

2) Data R binaria $R \subseteq A \times A$

R è detta **RIFLESSIVA** se $(x, x) \in R \quad \forall x \in A$

$$x R x \quad \forall x \in A$$

$$\lambda A \in R$$

3) Data $R \subseteq A \times B$

R è detta **SIMMETRICA** se $(x, y) \in R \Rightarrow (y, x) \in R$

$$\text{se } x R y \Rightarrow y R x$$

4) Data $R \subseteq A \times A$

R è detta **ASIMMETRICA** se $(x R y \wedge y R x) \Rightarrow x = y$

$$\text{Es. I "divise" } \subseteq \mathbb{N}_0 \times \mathbb{N}_0 \quad a/b \wedge b/a \Rightarrow a = b$$

5) Data $R \subseteq A \times A$

R è detta **TRANSITIVA** se $((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$

$$x R y \wedge y R z \Rightarrow x R z$$

$$\text{Es. } A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$$

6) R è detta **RELAZIONE DI EQUIVALENZA** se è refl. + simm. + tr.

7) R è detta **RELAZIONE DI ORDINE** se è refl. + assimm. + tr.

ES.

$$A = \{x \in \mathbb{Z} \mid -6 \leq x \leq 6\}$$

$$2\mathbb{Z} \cup 3\mathbb{Z} = \{x \in \mathbb{Z} \mid 2/x \text{ oppure } 3/x\}$$

$$(2\mathbb{Z} \cup 3\mathbb{Z}) \cap A = \{-6, -4, -2, -3, 0, 2, 3, 4, 6\}$$

$$(2\mathbb{Z} \cap 3\mathbb{Z}) \cap A = \{-6, 0, 6\} \quad \text{multipli di 3 e di 2}$$

$$(2\mathbb{Z} \setminus 3\mathbb{Z}) \cap A = \{-4, -2, 2, 4\}$$

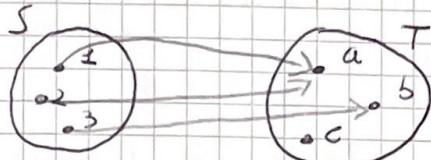
$$(2\mathbb{Z} \cup 3\mathbb{Z}) \cap A = \{-4, -3, -2, 2, 3, 4\}$$

DEF - Dati A, B insiemmi: $A \cup B = \{x \mid x \in A \cup B \wedge x \notin A \cap B\}$

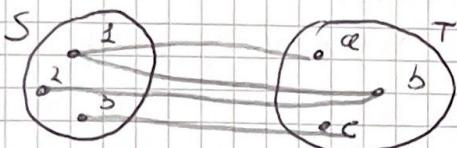
$$A \cup B = (A \cup B) \setminus (A \cap B) \quad \circ \quad (A \setminus B) \cup (B \setminus A)$$

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

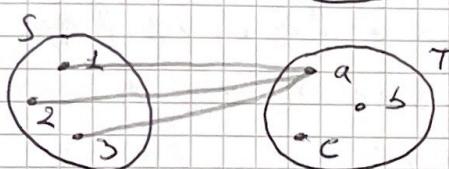
ES - $S = \{1, 2, 3\} \quad T = \{a, b, c\}$



$$\begin{aligned} & 1 \mapsto a \quad f(1) = a \\ & f(1) = a \quad f(2) = a \\ & f(3) = b \end{aligned} \quad \text{Im}(f) = \{a, b\}$$



$$f(1) = ? \in \begin{matrix} a \\ b \end{matrix}$$

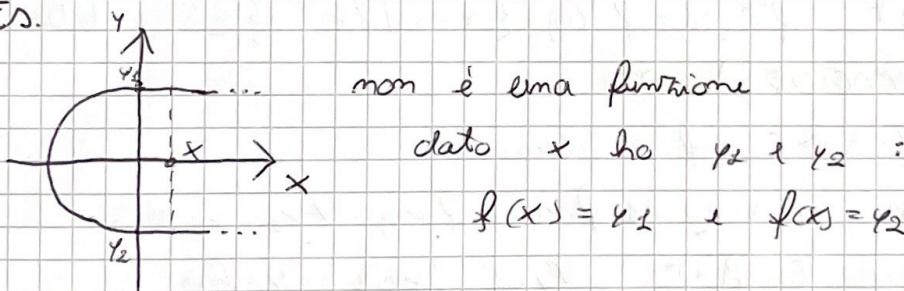


$$\begin{aligned} & f(1) = f(2) = f(3) = a \\ & f \text{ è "costante"} \quad \text{Im}(f) = \{a\} \end{aligned}$$

DEF - $\text{Im}(f) \subseteq T$ è definito come

$$\text{Im}(f) = \{y \in T \mid \exists x \in S : f(x) = y\} \subseteq T$$

Es.



dato x ho y_1 e y_2 :

$$f(x) = y_1 \quad \text{e} \quad f(x) = y_2$$

PROPRIETÀ $f: S \rightarrow T, A \subseteq S$ Definito $f(A) = \{f(x) \mid x \in A\} \subseteq T$

Dati $A_1, A_2 \subseteq S$, si ha

$$\text{1)} A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$$

DIM -

ma $y \in f(A_1)$ - Per def. $\exists x \in A_1 : y = f(x)$, poiché $x \in A_1 \Rightarrow x \in A_2$
 $\Rightarrow x \in A_1 \subseteq A_2 \Rightarrow x \in A_2$ Quindi $f(x) \in f(A_2) \Rightarrow$
 \Rightarrow poiché $f(x) = y$ si ha $y \in f(A_2)$ Allora $f(A_1) \subseteq f(A_2)$



$$2) f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$$

DIM - $y \in f(A_1 \cap A_2) \Leftrightarrow \exists x \in A_1 \cap A_2 : y = f(x) \Leftrightarrow$

\Leftrightarrow poiché $x \in A_1 \cap A_2$ si ha $x \in A_1$ e $x \in A_2 \Leftrightarrow$

$\Leftrightarrow y = f(x)$ con $x \in A_1 \Rightarrow y \in f(A_1) \cap f(A_2)$

$y = f(x)$ con $x \in A_2$

↪

$$3) f(A_1) \cup f(A_2) = f(A_1 \cup A_2)$$

DIM - $y \in f(A_1) \cup f(A_2) \Leftrightarrow \exists x \in A_1 : y = f(x) \text{ o } \exists x \in A_2 : y = f(x) \Leftrightarrow$

$\Leftrightarrow \exists x \in (A_1 \cup A_2) : y = f(x) \Rightarrow y \in f(A_1 \cup A_2)$ ↪

$$4) f(A_1) \cdot f(A_2) \subseteq f(A_1 \setminus A_2)$$

DIM - $y \in f(A_1) \cdot f(A_2) \quad \exists x_1 \in A_1 : y = f(x_1) \text{ e } y \notin f(A_2)$

$\Rightarrow \exists x_2 \in A_2 : y = f(x_2) \Rightarrow \exists x \in A_1 \setminus A_2 \Rightarrow$

$\Rightarrow y = f(x_1) \in f(A_1 \setminus A_2)$ ↪

DEF - Data $A \subseteq S$, $f[A] = f(A) = \{f(x) \in T \mid x \in A\} \subseteq T$ è detto

IMMAGINE DI A

Data $B \subseteq T$ $f^{-1}[B] = f^{-1}(B) = \{x \in S \mid f(x) \in B\} \subseteq S$ è detto

CONTROIMMAGINE DI B

DEF - Data $f: S \rightarrow T$, f si dirà

- **INIETTIVA** se $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \quad \forall x_1, x_2 \in S$

- **SURIETTIVA** se $\text{Im}(f) = T \quad \forall y \in T \exists x \in S : y = f(x)$

- **BIETTIVA** = iniettiva + suriettiva $\forall y \in T \exists ! x \in S : f(x) = y$

- **COSTANTE** se $f(x) = c \quad \forall x \in S$ con $c \in T$ è finito

Proprietà della controimmagine

$f: S \rightarrow T$ - Dati $B_1, B_2 \subseteq T$

$$1) B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$$

$$2) f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$$

$$3) f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$$

$$4) f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$$

$$5) \forall A \subseteq S \quad A \subseteq f^{-1}(f(A))$$

$$6) \forall B \subseteq T \quad f(f^{-1}(B)) \subseteq B$$

DIM -

⑤ $\forall a \in A \Rightarrow f(a) \in f(A)$

$$f^{-1}(f(A)) = \{x \in S \mid f(x) \in f(A)\} \Rightarrow \text{def.}$$

$$\Rightarrow x \in f^{-1}(f(A)) \Rightarrow A \subseteq f^{-1}(f(A)) \quad \checkmark$$

DEF - $f \subseteq S \times T$ e $g \subseteq T \times W$

$$f: S \rightarrow T \quad g: T \rightarrow W$$

Si chiama **composta** di $f \circ g$ l'applicazione

$$(g \circ f): S \rightarrow W \quad (g \circ f)(x) = g(f(x))$$

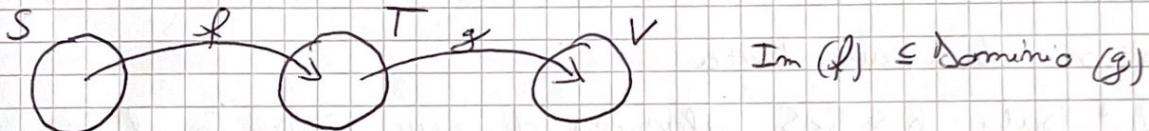
$$\text{es. } f(x) = x+3$$

$$(g \circ f)(x) = g(x+3) = (x+3)^2$$

$$g(x) = x^2$$

$$(f \circ g)(x) = f(x^2) = x^2 + 3$$

La composizione non è commutativa - è associativa



$$\text{es. } f(x) = -x \quad f: \mathbb{R} \rightarrow \mathbb{R}$$

$$g(x) = \sqrt{x} \quad g: \mathbb{R}^+ \rightarrow \mathbb{R}$$

$(g \circ f)(x)$ ha senso solo se $f(x) \geq 0$

TEOREMI

1) f, g sono iniettive $\Rightarrow g \circ f$ è iniettiva

2) $\text{\"{u}} \text{\"{u}}$ suriettive $\Rightarrow g \circ f$ è suriettiva

3) $\text{\"{u}} \text{\"{u}}$ biiettive $\Rightarrow g \circ f$ è biiettiva

4) $g \circ f$ è iniettiva $\Rightarrow f$ è iniettiva

5) $g \circ f$ è suriettiva $\Rightarrow g$ è suriettiva

6) $g \circ f$ è biiettiva $\Rightarrow f$ è iniettiva e g è suriettiva



DEF - $f: S \rightarrow T$, $g: T \rightarrow V$ $g \circ f: S \rightarrow V$

Definiamo **INVERSA** di f la funzione

$f^{-1}: T \rightarrow S$ f^{-1} è funzione $\Leftrightarrow f$ è biettiva

OSS - f^{-1} è la Relazione opposta di f

Ese - $f: S \rightarrow T$

$$f = \{(a, 1), (b, 1), (c, 3)\} \subseteq S \times T$$

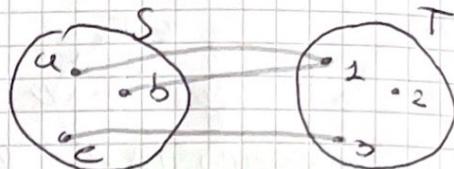
$$f^{op} = \{(1, a), (1, b), (3, c)\} \subseteq T \times S$$

f^{op} non è funzione: non è né iniettiva né suriettiva

DEF - Data f biiettiva, f^{-1} è l'unica funzione tale che

$$f: S \rightarrow T \quad \forall s \in S \quad (f^{-1} \circ f)(s) = s$$

$$f^{-1}: T \rightarrow S \quad \forall t \in T \quad (f \circ f^{-1})(t) = t$$



Relazioni di equivalenza

DEF - Data $R \subseteq S \times S$ relazione di equivalenza, si chiama

CLASSE DI EQUIVALENZA di $x \in S$ rispetto ad R

definita da $[x]_R = \{y \in S \mid x R y\} \subseteq S$

L'INSIEME QUOTIENTE S/R è l'insieme delle classi di equivalenza rispetto a R

$$S/R = \{[x]_R \mid x \in S\} \subseteq P(S)$$

Data $R \subseteq S \times S$ rel. di equi., la funzione $\pi: S \rightarrow S/R$

$\pi(x) = [x]_R$ è detta **PROIEZIONE CANONICA** di S sul quoziente.

Proposizione

Sia $R \subseteq S \times S$ r.e. Allora:

$$\text{1)} x \in [x]_R \quad \forall x \in S$$

DIM. - Se $x \in S$, per definizione di R.e., si ha $x R x$. Allora per definizione di classe di equivalenza si ha $x \in [x]_R$

$$2) x R y \Leftrightarrow [x]_R = [y]_R$$

DIM -

$$\begin{aligned} (\Rightarrow) \text{ Sia } z \in [x]_R &\Leftrightarrow x R z \Leftrightarrow z R x \Leftrightarrow (z R x) \wedge (x R y) \Leftrightarrow \\ &\Leftrightarrow z R y \Leftrightarrow y R z \Leftrightarrow z \in [y]_R \end{aligned}$$

$$(\Leftarrow) \text{ Se } [x]_R = [y]_R \Rightarrow x \in [x]_R = [y]_R \Rightarrow x \in [y]_R \Rightarrow y R x \Rightarrow x R y \quad \hookrightarrow$$

$$3) x R y \Leftrightarrow [x]_R \cap [y]_R = \emptyset$$

DIM -

$$\begin{aligned} \Rightarrow \text{ Se } x R y \text{ se } [x]_R \cap [y]_R \neq \emptyset \Rightarrow \exists z \in [x]_R \cap [y]_R \Rightarrow \\ \Rightarrow z \in [x]_R \Rightarrow x R z \Rightarrow x R z \wedge z R y \Rightarrow x R y \text{ che contr.} \\ z \in [y]_R \Rightarrow y R z \text{ l'ipotesi} \end{aligned}$$

$$\Leftarrow \text{ Sia per assurdo } x R y \Rightarrow x \in [x]_R \cup x \in [y]_R \Rightarrow$$

$$\Rightarrow x \in [x]_R \cap [y]_R \text{ che contraddice l'ipotesi} \quad \hookrightarrow$$

OSS - Date $R_1, R_2 \subseteq S \times S$, si ha che

$$R_1 = R_2 \Leftrightarrow [x]_{R_1} = [x]_{R_2} \quad \forall x \in S \Leftrightarrow \frac{S}{R_1} = \frac{S}{R_2}$$

DEF - Una **PARTIZIONE** di un insieme S è una famiglia di sottointersiemi $\mathcal{F} \subseteq P(S)$ tale che:

$$1) \forall F \in \mathcal{F}, F \neq \emptyset$$

$$2) \forall F, G \in \mathcal{F}, F \cap G = \emptyset \text{ se } F \neq G$$

$$3) \bigcup \mathcal{F} = S \quad \text{unione degli insiemi } F \in \mathcal{F}$$

$$\text{Ese - } A = \{a, b, c\}$$

$$\mathcal{F}_1 = \{\{a\}, \{b\}, \{c\}\} \quad \text{V l'unione di tutti restituisce } A \text{ e tutte le inters. sono vuote}$$

$$\mathcal{F}_2 = \{\{a, b\}, \emptyset, \{c\}\} \quad \times$$

$$\mathcal{F}_3 = \{\{A\}\} \quad \checkmark$$

Teorema fondamentale sulle relazioni di equivalenza

1) Se R è relaz. d'eq. su S , allora $\frac{S}{R}$ è partizione di S

2) Se \mathcal{F} è partizione di S , allora $x R_{\mathcal{F}} y \Leftrightarrow \exists F \in \mathcal{F} \text{ t.c. } x, y \in F$

la relazione $R_{\mathcal{F}}$ è una relaz. d'eq. e l'unica tale che $\mathcal{F} = \frac{S}{R_{\mathcal{F}}}$

Esercizio -

$A \subseteq \mathbb{N}_0$ definito da $A = \{2^m 3^n \mid m, n \in \mathbb{N}\}$. Si definisce $R \subseteq A \times A$

$$2^m 3^n R 2^t 3^r \Leftrightarrow m+n=t+r$$

Dimostra che R è di equivalenza

1) Riflessività?

$$2^m 3^n R 2^m 3^n \Leftrightarrow m+n=m+n \quad \text{VERO}$$

2) Simmetria?

$$\text{Se } 2^m 3^n R 2^t 3^r \Leftrightarrow m+n=t+r \Leftrightarrow t+r=m+n \Leftrightarrow 2^t 3^r R 2^m 3^n \quad \text{VERO}$$

3) Transitività?

$$\begin{aligned} 2^m 3^n R 2^t 3^r &\Leftrightarrow m+n=t+r \\ 2^t 3^r R 2^h 3^k &\Leftrightarrow t+r=h+k \end{aligned} \quad \left\{ \begin{array}{l} m+n=h+k \\ m+n=t+r \end{array} \right. \Rightarrow 2^m 3^n R 2^h 3^k \quad \text{VERO}$$

$$\{12\}_{2,2} = \{2^0 3^3, 2^2 3^3, 2^3 3^2, 2^3 3^0\} = \{27, 18, 12, 8\}$$

$$12 = 2^3 \cdot 3^1 \quad 2^m 3^n R 12 \Leftrightarrow m+n=3$$

NOTAZIONE - Indichiamo ogni relazione d'ordine R con \leq

DEF - Un **insieme ordinato** è una coppia (S, \leq) dove \leq è una relazione d'ordine su S

Esercizio - $(\mathbb{N}_0, \leq), (\mathbb{N}, \leq), (P(X), \subseteq)$

DEF - Data (S, \leq) insieme ordinato chiamiamo

1) $x, y \in S$ si dicono confrontabili (rispetto a \leq) se vale una tra

$$x \leq y \quad o \quad y \leq x$$

2) Se $\forall x, y \in S$ si ha che $x \neq y$ sono confrontabili \Rightarrow

S è detto totalmente ordinato o catena



3) Definiamo < minore stretto : $x < y \Leftrightarrow x \leq y \quad e \quad x \neq y$

\geq maggiore uguali : $x \geq y \Leftrightarrow y \leq x$

4) Dati $(S, \leq), (S^*, \leq^*)$ due insiemni ordinati - Definiamo

$f: S \rightarrow S^*$ **funzione crescente** se $\forall x, y \in S$ tali che $x \leq y \Rightarrow f(x) \leq^* f(y)$

omomorfismo di insiemni ordinati

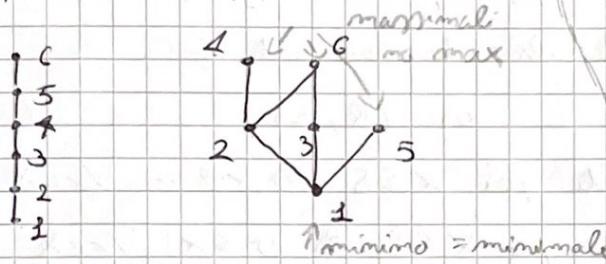
DEF - Diagrammi di Hasse (per insiemi finiti)

Si rappresenta ogni elemento dell'insieme come vertice e si traccia una linea che va da x a y se $x \leq y$ e non esiste z tale che $x < z < y$; nel primo caso si dice che y copre x o che y è un successore immediato di x

$$\text{es - } A = \{1, 2, 3, 4, 5, c\}$$

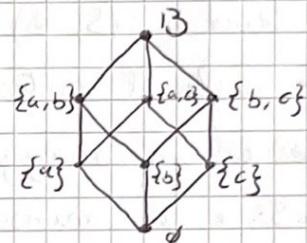
$$(A, \leq)$$

$$(A, 1)$$



$$B = \{a, b, c\} \quad (\text{es } (P(B), \subseteq))$$

$$P(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$



DEF - Dato (S, \leq)

Un elemento $a \in S$ è detto massimo per S se $\forall x \in S, x \leq a$

$\Leftrightarrow b \in S \Rightarrow$ minimo per S se $\forall x \in S, b \leq x$

Se $X \subseteq S$, definisco massimo e minimo dentro X :

1) $a = \max_S(x)$ se $a \in X$ e $\forall x \in X$ si ha $x \leq a$

2) $b = \min_S(x)$ se $b \in X$ e $\forall x \in X$ si ha $b \leq x$

OSS - Su (S, \leq) ha un massimo, questo è unico - same per min

DIM. - Siano a e b due massimi per S

Poiché $a = \max(S) \Rightarrow \forall x \in S, x \leq a \Rightarrow$ in part. $b \leq a \} \quad a = b$

Poiché $b = \max(S) \Rightarrow \forall x \in S, x \leq b \Rightarrow \quad a \leq b \} \quad a = b$

DEF - Dato (S, \leq)

un elemento $\overset{c \in S}{\underset{x \in S}{\forall}}$ detto massimale se $\forall x \in S$ t.c. $c \leq x$

$\Leftrightarrow d \in S$ detto minimale se $\forall x \in S$: $x \leq d$

OSS - ogni minimo è anche minimale - ogni max è anche massimale

OSS - In un insieme totalmente ordinato e finito esistono sempre massimo e minimo. — Se un insieme è totalmente ordinato e ha un massimale \Rightarrow questo è max - same per min

DEF - Dato (S, \leq) insieme ordinato, questo è detto **BENE ORDINATO**

se $\forall X \subseteq S, X \neq \emptyset, \exists \min_S(X)$

"ogni suo sottinsieme non vuoto ha un minimo"

Eg: (\mathbb{N}_0, \leq) è bene ordinato

PROP - Se (S, \leq) è bene ordinato \Rightarrow è totalmente ordinato.

DIM - Per ipotesi, $\forall x, y \in S$ si ha $\{x, y\} \subseteq S$ che un minimo.

Se $\min\{x, y\} = x \Rightarrow x \leq y$, se $\min\{x, y\} = y \Rightarrow y \leq x$.

Quindi (S, \leq) è totalmente ordinato \hookrightarrow

OSS - Non vale il contrario es. (\mathbb{R}, \leq)

DEF - w è un maggiorante per $X \subseteq S \Leftrightarrow w \geq x \quad \forall x \in X$

$v \in S$ è un minorante per $X \subseteq S \Leftrightarrow v \leq x \quad \forall x \in X$

Eg. - $A = \{n \in \mathbb{N}_0 : n \mid 36\}$ ($A; 1$)

$$A = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

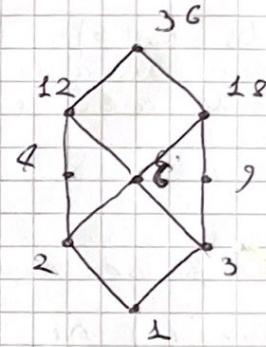
$$X = \{12, 4, 6, 2\}$$

$$\max(X) = 12$$

$$\min(X) = 2$$

maggioranti di $X = \{12, 36\}$

minoranti di $X = \{2, 1\}$



DEF - Sia $N = \{\text{insieme dei maggioranti di } X \subseteq S\}$ (S, \leq) ordinato

chiamiamo estremo superiore di X in S il $\min(N)$ e lo indichiamo con $\sup_S(X)$

$$w = \sup_S(X) \Leftrightarrow \begin{cases} x \leq w \quad \forall x \in X & (\text{è maggiorante}) \\ \forall y \in N, w \leq y & (\text{è il più piccolo di essi}) \end{cases}$$

DEF - Sia $M = \{\text{insieme dei minoranti di } X \subseteq S\}$

chiamiamo estremo inferiore di X in S il $\max_S(N)$ e lo indichiamo con $\inf_S(X)$

$$v = \inf_S(X) \Leftrightarrow \begin{cases} v \leq x \quad \forall x \in X \\ \forall y \in M, y \leq v \end{cases}$$

DEF - Un insieme ordinato (S, \leq) è detto RETICOLO se

$\forall x, y \in S$ esistono $\inf(\{x, y\})$ e $\sup(\{x, y\})$

Se S è un reticolo: $\inf(\{x, y\}) := x \wedge y$

$$\sup(\{x, y\}) := x \vee y$$

Se S è un reticolo con un massimo a ed un minimo b ,

chiamiamo complemento di $x \in S$ un elemento y t.c. $\begin{cases} x \vee y = a \\ x \wedge y = b \end{cases}$

In $P(A)$, il complemento di $X \subseteq A$ è $A \setminus X$

TEOREMA

$\forall A \neq \emptyset, (P(A), \subseteq)$ è un reticolo t.c. ogni elemento ha un complemento

DIM -

Vogliamo dim. che $\forall X, Y \subseteq A, X \cup Y = \sup(X, Y) \wedge X \cap Y = \inf(X, Y)$

$X \cup Y$ è un maggiorante per la def. di unione:

$$X \subseteq X \cup Y \wedge Y \subseteq X \cup Y$$

Sia Z tale che Z è un altro maggiorante. Allora $X \subseteq Z \wedge Y \subseteq Z$

$\left. \begin{array}{l} \forall x \in X \Rightarrow x \in Z \\ \forall y \in Y \Rightarrow y \in Z \end{array} \right\} \Rightarrow$ ogni elemento che appartiene a X oppure Y appartiene a Z $\Rightarrow X \cup Y \subseteq Z$

\vdash

$X \cap Y$ è un minorante perché $X \cap Y \subseteq X \wedge X \cap Y \subseteq Y$

Sia Z un altro minorante. Allora per definizione

$Z \subseteq X \wedge Z \subseteq Y \Rightarrow \forall z \in Z \Rightarrow z \in X$
 $\qquad \qquad \qquad \qquad \qquad \qquad \qquad \Rightarrow z \in Y \Rightarrow z$ appartiene ad entrambi

$$\Rightarrow Z \subseteq X \cap Y \Rightarrow Z \subseteq X \cap Y \quad \hookrightarrow$$

$\forall X \subseteq A, A \setminus X$ è il complemento di X perché

$$\bullet (A \setminus X) \cup X = A \quad A \text{ è il max } (P(A))$$

$$\bullet (A \setminus X) \cap X = \emptyset \quad \emptyset \text{ è il min } (P(A))$$

TEOREMA DI EUCLIDE Esistono infiniti numeri primi

DIM - Per assurdo, supponiamo che $P = \{\text{insieme dei numeri primi}\}$ sia finito e supponiamo che $|P| = t$, $P = \{p_1, \dots, p_t\}$

(VEDI DORO) Sia $m = p_1 \cdot \dots \cdot p_t$ e $m+1 = p_1 \cdot \dots \cdot p_t + 1$

Dato $q \in P$, $q | m$. Per come ho definito $m+1$, questo non è primo perché $p_i < m+1 \quad \forall i = 1, \dots, t$ e dunque si può scomporre in fattori primi. Esiste quindi $z \in P$ tale che $z | m+1$ ma vale anche $z | m$ da cui

$$1 = (m+1) - m \quad m+1 = zh \quad m = zk \Rightarrow 1 = zh - zk = (h-k)z$$

e ciò implica $z | 1$ che è assurdo perché 1 non è da diverso da niente



CRIVELLO DI ERATOSTENE

Sia $n \geq 2$; allora n è primo se non ammette divisori primi

P tali che $p^2 \leq n$

Ese: 151 è primo, verifica:

$$2 \Rightarrow 2^2 = 4 \leq 151 \text{ ma } 2 \nmid 151$$

$$3 \Rightarrow 3^2 = 9 \leq 151 \text{ ma } 3 \nmid 151$$

~~$$4 \Rightarrow 4^2 = 16 \leq 151 \text{ ma } 4 \nmid 151$$~~

~~$$5 \Rightarrow 5^2 = 25 \leq 151 \text{ ma } 5 \nmid 151$$~~

$\Rightarrow 151$ è primo perché tutti i primi con un quadrato ≤ 151 non dividono 151

PRINCIPIO DI INDUZIONE

(Vedi prima induzione e divisione)

Si caratterizza dalla seguente proprietà:

Se parto da 0 e definisco un insieme S aggiungendo per ogni $m \in S$ il suo successivo $m+1 \Rightarrow S = \mathbb{N}$

Prima forma

Sia $m \in \mathbb{N}$ e sia $P(m)$ una proprietà dei numeri naturali che dipende da m - Allora si:

(1) P è vera per m base di induzione

② ogni volta che P è vera per $m \geq \bar{m}$ allora posso dimostrare che P è vera per $m+1$ $P(m)$ ipotesi di induzione allora P è vera $\forall m \geq \bar{m}$ $P(m) \Rightarrow P(m+1)$ il passo induttivo

N.B. Il passo può essere anche $P(m-1) \Rightarrow P(m)$

E.S. - $\forall m \in \mathbb{N}$ " $1 + 2 + \dots + m = \frac{m(m+1)}{2}$ " = $P(m)$
 $\stackrel{\downarrow}{\bar{m}=1}$ "l'ugualanza è vera"

$$P(1) \Rightarrow 1 = \frac{1(1+1)}{2} \Rightarrow 1=1 \text{ vero} \leftarrow \text{base di ind.}$$

$$P(m) \Rightarrow P(m+1)$$

$$\underbrace{1+2+\dots+m}_{\frac{m(m+1)}{2}} + m+1 = \frac{(m+1)((m+1)+1)}{2}$$

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

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

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

Seconda forma

Sia $\bar{m} \in \mathbb{N}$, sia $P(m)$ una proprietà dei numeri naturali $m \geq \bar{m}$

Si (3) $P(\bar{m})$ è vera

(2) dato $t \geq \bar{m}$, se da $P(k)$ vera $\forall \bar{m} \leq k \leq t$ segue che $P(t)$ è vera
 allora $P(t)$ vera $\forall t \geq \bar{m}$

$P(k)$ vera $\forall k < t \Rightarrow P(t)$ passo

TEOREMA FONDAMENTALE DELL'ARITMÉTICA (in \mathbb{N}_0)

Sia $m \in \mathbb{N}$, allora esistono $t \geq 1$ e $p_1 \dots p_t$ numeri primi tali che $m = p_1 \cdot \dots \cdot p_t$. La scomposizione è unica a meno dell'ordine dei fattori.

DIM -

Base: $\bar{m} = 2$ si ha $t=1$ e $p_1 = 2$

Passo: $m \in \mathbb{N}$, $m \geq 2$ e supponiamo al teorema vero per ogni $k < m$

(1) Se m è primo, si ha $t=1$ e $p_1 = 2$

(2) Se m non è primo, esistono $a, b \in \mathbb{N}$ t.c. $m = ab$ e per ipotesi di induzione anche $t, r \in \mathbb{N}$

$$\left. \begin{array}{l} p_1, \dots, p_c \\ q_1, \dots, q_s \end{array} \right\} \text{numeri primi t.c. } a = p_1 \dots, p_c \\ b = q_1, \dots, q_s$$

Allora $m = ab = p_1 \dots p_c \cdot q_1 \dots q_s \Rightarrow$ ho trovato $C+S$ numeri primi dunque dimostrata

Algoritmo della divisione euclidea (in \mathbb{N}_0)

Sia $b \neq 0$. $\forall m \in \mathbb{N}_0$ $\exists q, r \in \mathbb{N}_0 : m = qb + r$ e $r < b$ P(m)

DIM-

$m=0$ Si ha $0 = 0 \cdot b + 0$

Passo ind. $(m-1) \rightarrow m$

\vdash forma

Per ipotesi $P(m-1)$ è vera cioè esistono $q, r \in \mathbb{N}_0$ t.c.

$$m-1 = qb + r \quad e \quad r < b$$

Da cui ricaviamo $m = qb + r + 1$

Se $r+1 < b$ ho finito

Se invece $r+1 \geq b \Rightarrow r+1 = b+k \quad - k = r+1-b$

$$\text{da cui } m = qb + r + 1 = qb + b + k = (q+1)b + k \quad e \quad k < b$$

e quindi ho scritto m come somma multiplo di b + k \Rightarrow

(ora vengono T. di Euclide e Caccetta)

Rappresentazione di un numero naturale in una base fissata

Sia $b \geq 2$. Ogni numero $m \in \mathbb{N}$ ha una scrittura

$$m = c_0 + c_1 b + c_2 b^2 + \dots + c_s b^s$$

con $s \geq 0$, $c_0, c_1, c_2, \dots, c_s \in \{0, 1, 2, \dots, b-1\}$ e $c_s \neq 0$

$$\text{scriveremo } m = (c_s c_{s-1} \dots c_0)_b$$

DIM

Dati $m \in \mathbb{N}$ e $b \geq 2$, esistono q_0 e c_0 tali che

$$m = q_0 b + c_0 \quad / \quad q_0 \in \mathbb{N}_0 \quad 0 \leq c_0 \leq b-1 \quad (c_0 < b)$$

$$q_0 = q_1 b + c_1 \quad / \quad q_1 \in \mathbb{N}_0 \quad 0 \leq c_1 \leq b-1$$

$$q_1 = \dots$$

:

$$q_{s-1} = q_s b + c_s \quad \text{ti fermo quando } q_{s-1} < b - \text{Questa ha } q_s = 0 \quad e \quad q_{s-1} = c_s$$

Ciò succede perché $q_0 > q_1 > q_2 > \dots > q_s$ e quindi invertibilmente il quoziente q_s sarà minore di b

$$m = q_0 b + c_0 =$$

$$= (q_1 b + c_1) b + c_0 = q_1 b^2 + c_1 b + c_0 =$$

$$= (q_2 b + c_2) b^2 + c_1 b + c_0 = q_2 b^3 + c_2 b^2 + c_1 b + c_0$$

$$= (q_3 b + c_3) b^4 + \dots + c_2 b^2 + c_1 b + c_0$$

$$= c_s b^s + \dots + c_1 b + c_0$$



Algoritmo della divisione euclidea (in \mathbb{Z})

Dati $a, b \in \mathbb{Z}$ con $b \neq 0$ sì $q, r \in \mathbb{Z}$: $m = qb + r$ con $0 \leq r < |b|$

Proprietà

$$\text{rest}(a, b) = \text{rest}(a, -b)$$

$$a = qb + r \Rightarrow a = (-q)(-b) + r$$

$$\text{rest}(-a, b) = 0 \quad \text{o} \quad \text{rest}(a, b) = 0$$

$$b - \text{rest}(a, b) \quad \text{se} \quad \text{rest}(a, b) \neq 0$$

$$\text{Se } a = qb \Rightarrow -a = (-q) \cdot b$$

$$\text{Se } a = qb + r \Rightarrow -a = (-q) \cdot b - r$$

$$-a = (-q) \cdot b - r + b - b$$

$$-a = (-q-1) \cdot b + (b-r) \Rightarrow 0 \leq b-r < |b|$$

$$\text{Se } x|y \Rightarrow \text{rest}(x, y) = 0$$

$$\text{Es.} - \quad \text{rest}(19, 3) = 1 \quad 19 = 6 \cdot 3 + 1$$

$$\text{rest}(19, 3) = 3 - 1 = 2$$

$$-19 = (-6) \cdot 3 - 1 = (-6)3 - 3 + 3 - 1 = (-7)3 + 2$$

$$\text{Es.} - \quad \forall n \in \mathbb{N}, \quad "2+4+6+\dots+2n = n(n+2)" \quad P(m)$$

$$\text{Base: } m=1 \quad 2 \cdot 1 = 1(1+1) \Rightarrow 2=2 \quad \checkmark$$

$$\text{Passo: } m \rightarrow m+1 \quad P(m+1) \Rightarrow 2+4+\dots+2m+2(m+1) = (m+1)(m+2)+2$$

Per ipotesi di induzione $P(m+1)$ diventa

$$m(m+2) + 2(m+1) = (m+1)(m+2)$$

$$(m+1)(m+2) = (m+1)(m+2)$$

DEF- Dato $a \in \mathbb{Z}$, denotiamo con $D(a) = \{x \in \mathbb{Z} \mid x \mid a\}$ l'insieme dei suoi divisori

$$D(a) \subseteq \mathbb{Z}$$

Sia $a=0$, $D(a) = \mathbb{Z}$

Sia $a \neq 0$ e $a \neq -1, 1$ allora $|D(a)| \geq 4$ e $D(a)$ è finito.

LEMMA

$\forall x, y, k, z \in \mathbb{Z}$ tali che $x = ky + z$, allora $D(x) \cap D(y) = D(y) \cap D_z$

$$\text{DIM. } D(x) \cap D(y) \subseteq D(y) \cap D_z$$

Sia $m \in D(x) \cap D(y) \Rightarrow m/x \wedge m/y \Rightarrow \exists h, l : x = hm$
 allora dalle ipotesi $z = ky + x = hm - khm \Rightarrow (l-kh)m \Rightarrow m/z$

$$\Rightarrow m \in D(y) \cap D_z$$

Vediamo $D(y) \cap D_z \subseteq D(x) \cap D_y$

Per definizione, se $m \in D(y) \cap D_z \Rightarrow m/y \wedge m/z \Rightarrow m/ky$
 $\Rightarrow m/k_y + z$ che è uguale ad $x \Rightarrow m \in D(x) \cap D_y \subseteq$

DEF- Sia $p \in \mathbb{Z} \setminus \{-1, 1\}$. p è detto primo se $D(p) = \{-p, p, -1, 1\}$

DEF- Dati $a, b \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{Z}$ è Massimo Comune Divisore di a e b

$$\textcircled{1} \quad d \in D(a) \cap D(b) \quad (d/a \wedge d/b)$$

$$\textcircled{2} \quad \forall t \in \mathbb{Z} : t/a \wedge t/b \Rightarrow t/d$$

PROPOSIZIONE-

Dati $a, b \in \mathbb{Z} \setminus \{0\}$, si ha

$$\textcircled{1} \quad d \text{ è un MCD per } a \text{ e } b \Leftrightarrow -d \text{ è un MCD per } a \text{ e } b$$

$\textcircled{2}$ Se d è un MCD per a e b , gli unici MCD di a e b sono d e $-d$

DIM.-

$\textcircled{3} \Rightarrow$ Ipotesi: d è un MCD per a e b Tesi: $-d$ è MCD per a e b

$$\textcircled{i} \quad \text{Se } d \text{ è un MCD per } a \text{ e } b \Rightarrow \exists h, k : a = hd \wedge b = kd \Rightarrow a = (-h)d \wedge b = (-k)d \Rightarrow -d/a \wedge -d/b \Rightarrow -d \in D(a) \cap D(b)$$

\textcircled{ii} Sia t tale che $t/a \wedge t/b$. Per ipotesi d è un MCD

$$\Rightarrow t/d \text{ e } \exists k : d = k \cdot c. \text{ Allora } -d = (-k)c \Rightarrow -t/d$$

Per " \Leftarrow " si ragiona per ragione identica invertendo d e $-d$

(2) Supponiamo d un MCD e per contraddizione sia t un altro MCD per a, b . Deve essere $t = d$ o $t = -d$

Se t è un altro MCD ho $t/a = t/b = t/d = d/t$
quindi $\exists k, h$ tali che $d = t \cdot k$ e $t = d \cdot h \Rightarrow d = d \cdot kh$
poiché siamo in \mathbb{Z} , si ha $kh = 1 \Rightarrow h = 1$ e $k = 1 \Rightarrow t = d$
 $h = -1 \Rightarrow k = -1 \Rightarrow t = -d$

CONVENZIONE

$\forall a, b \in \mathbb{Z} - \{0\}$, $\text{MCD}(a, b) = d \geq 0$

$$\text{MCD}(6, 3) = \{-3, 3\} = 3$$

Oss. - $d = \text{MCD}(a, b) = \text{MCD}(-a, b) = \text{MCD}(a, -b) = \text{MCD}(a, -b)$

LEMMA

$\forall a, b, d \in \mathbb{Z}$ con $d \geq 0$

$$d = \text{MCD}(a, b) \Leftrightarrow D(d) = D(a) \cap D(b)$$

DIM. -

\Rightarrow Sia $mld \Rightarrow d = m \cdot a$

d è MCD $d(a, b) \Rightarrow d/a = d/b \Rightarrow a = kd$ e $b = hd \Rightarrow$

$\Rightarrow a = kdm$ e $b = hdm \Rightarrow m/a = m/b \Rightarrow m \in D(a) \cap D(b)$

Se $m \in D(a) \cap D(b)$ allora per definizione di MCD $mld = m \in D(d)$

\Leftarrow Se $D(a) \cap D(b) = D(d) \Rightarrow$ poiché $d \in D(d)$, si ha $d \in D(a) \cap D(b) \Rightarrow$
 $\Rightarrow d/a = d/b$

Sia $t \in D(a) \cap D(b) \Rightarrow t/a = t/b \Rightarrow t \in D(d) \Rightarrow t/d$

Dunque $d = \text{MCD}(a, b)$

S

PROPOSIZIONE

$\forall a, b \in \mathbb{Z}$ $\text{MCD}(a, b)$ esiste sempre

Nom Algoritmo delle divisioni successive

Sia $b > 0$ ($b = 0 \Rightarrow \text{MCD}(a, 0) = a$)

$\exists q_1, r_1 \in \mathbb{Z}$ t.c.

$$a = q_1 \cdot b + r_1$$

$$0 \leq r_1 < b$$

$\exists q_2, r_2 \in \mathbb{Z}$ t.c.

$$b = q_2 \cdot r_1 + r_2$$

$$0 \leq r_2 < r_1 < b$$

$\exists q_3, r_3 \in \mathbb{Z}$ t.c.

$$r_1 = q_3 \cdot r_2 + r_3$$

$$0 \leq r_3 < r_2 < r_1 < b$$

Ad un certo punto il $c_{t+1} = a_{t+1} \cdot c_t + c_{t-1}$ resterà zero

Ho quindi $b > c_1 > c_2 > \dots > c_t > c_{t+1} = 0$

$$\Delta(a) \cap \Delta(b) = \Delta(b) \cap \Delta(c_1) = \dots \supseteq \Delta(c_t) \cap \Delta(c_{t+1}) = \Delta(c_t)$$

\downarrow
 $\Delta(0) = \mathbb{Z}$

E quindi dall'ultimo lemma si ha $c_t = \text{MCD}(a, b)$ ↗

ES. - $\text{MCD}(1218, 132)$

$$1218 = 132 \cdot 9 + 30$$

$$132 = 30 \cdot 4 + 12$$

$$30 = 12 \cdot 2 + 0$$

$$12 = 6 \cdot 2 + 0 \quad \Rightarrow \text{MCD}(\dots) = 6$$

DEF- $a, b \in \mathbb{Z}$ sono detti coprimi se $\text{MCD}(a, b) = 1$

LEMMA -

① $a, p \in \mathbb{Z}$ con p primo. Se p divide allora $\text{MCD}(p, a) = 1$

DIM. - $\Delta(p) = \{-p, p, -1, 1\} \Rightarrow$ se p divide $p \in \Delta(a) \Rightarrow -p \in \Delta(a)$

$$\Delta(p) \cap \Delta(a) = \{-1, 1\} = \Delta(1) \quad \text{↗}$$

② Se $a, b \in \mathbb{Z} \setminus \{0\}$ e $d = \text{MCD}(a, b)$, allora $\exists a', b' \in \mathbb{Z}$ tali che
 $a = d \cdot a'$, $b = d \cdot b'$ con $\text{MCD}(a', b') = 1$

Teorema di Bezout

$\forall a, b \in \mathbb{Z}$, se $d = \text{MCD}(a, b)$ $\exists u, v \in \mathbb{Z}$: $d = ua + vb$

$$\text{ES. } 1218 = 132 \cdot 9 + 30$$

$$132 = 30 \cdot 4 + 12$$

$$30 = 12 \cdot 2 + 0 \quad \Rightarrow \quad 6 = 30 - 2 \cdot 12 = 30 + (-2) \cdot 12 =$$

$$= 30 + (-2)(132 + (-4)30) =$$

$$= 30 + (-2)(132) + (8)(30) =$$

$$= 9 \cdot 30 + (-2) \cdot 132 =$$

$$= 9 \cdot (1218 + (-2)(132)) + (-2)(132) =$$

$$= 9 \cdot 1218 + (-8)(132) + (-2)(132) =$$

$$= 9 \cdot 1218 + (-88)(132)$$

$$\begin{matrix} 1 \\ u \\ \hline a \end{matrix} \quad \begin{matrix} 1 \\ v \\ \hline b \end{matrix}$$

Teorema fondamentale dell'aritmetica (in \mathbb{Z})

Sia $\tau \in \mathbb{Z} \setminus \{-1, 0, \pm 1\}$. $\exists k \in \mathbb{N}$ ed esistono $p_1 \dots p_k$ numeri primi tali che $\tau = p_1 \cdot \dots \cdot p_k$.

Inoltre la rappresentazione è unica a meno del segno dei fattori e del loro ordine.

Conseguenza del teorema di Bezout

① $\forall a, b, c \in \mathbb{Z}$, se a/bc e $\text{mcd}(a, b) = 1 \Rightarrow a/c$

DIM. - Per ipotesi $\text{mcd}(a, b) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ t.c. $1 = ua + vb$

Moltiplico ambo i membri per $c \Rightarrow c = uac + vbc$

Per ipotesi a/bc quindi $\exists k \in \mathbb{Z}$ t.c. $bc = k \cdot a$ dunque

$c = uac + vka = (uc + vk)a \Rightarrow c$ è multiplo di a e a/c

② $\forall a, b \in \mathbb{Z}$, p numero primo in \mathbb{Z} . Se $p/a b \Rightarrow p/a$ oppure p/b

DIM. - Per ipotesi sappiamo che p è un numero primo,

dunque $\Delta(p) = \{-p, p, -1, 1\}$ e sappiamo che $p/a b$,

dunque $a b = p \cdot k$. Se $p/k \Rightarrow \text{mcd}(p, k) = 1$ e

per la prima conseguenza del teorema di Bezout

si ha che b è multiplo di p e quindi p/b

DEF - Dati $a, b \in \mathbb{Z}$, m si detto minimo comune multiplo di a e b se:

① a/m e b/m m è multiplo di entrambi ($a, b \in \Delta(m)$)

② $\forall \epsilon \in \mathbb{Z} : a/\epsilon$ e $b/\epsilon \Rightarrow m/\epsilon$ (è il minimo dei multipli)

PROPOSIZIONE

Dati $a, b \in \mathbb{Z}$, $d = \text{mcd}(a, b)$ e siamo $a' = a/d$ e $b' = b/d$ e $\text{mcd}(a', b') = 1$. Si ha:

① $m_i = a' b' d$ è un m.c.m. per a e b

② m' è mcm per a e b ($\Leftrightarrow m' = \pm m$)

DM-

① Vediamo che $m_1 = a'b'd$ soddisfa le due condizioni della definizione di mcm.

Per la ①, si ha $m = (a'd) \cdot b' = a'b' \Rightarrow m$ è multiplo di a
 $m = a' \cdot (b'd) = a'b' \Rightarrow m$ è multiplo di b'

Per la ②, sia t t.c. $a|t$ e $b|t$. Per definizione di l ,

$\exists h, k \in \mathbb{Z} : t = h \cdot a$ e $t = k \cdot b \Rightarrow t = h \cdot a'd$ e $t = k \cdot b'd$
 $\Rightarrow h \cdot a = k \cdot b'$ dunque $b'|h \cdot a'$. Per ipotesi $\text{mcd}(a', b') = 1$
quindi $b'|h$ per la 2^a conseg. del t. d. Bezout \Rightarrow
 $\exists l : h = b'l$. Di conseguenza $t = h \cdot a'd = b'l \cdot a'd =$
 $= (a'b'd) \cdot l = m \cdot l \Rightarrow m/t$ c.v.d.

② Supponiamo m un mcm e per contraddizione sia m'
un altro mcm per a e b . Dovrà essere $m' = +m$ o $m' = -m$

Se m' è un altro mcm si ha $a/m' \in b/m'$ da cui
 $m'/m \in m/m'$ e quindi esistono $\exists K, h$ tali che se
 $m = m' \cdot K$ e $m' = m \cdot h \Rightarrow m = m \cdot h \cdot K$. Poiché siamo in
 \mathbb{Z} , si ha $K \cdot h = \pm 1 \Rightarrow h = \pm 1$ e $K = \pm 1 \Rightarrow m' = m^{\pm}$
 \Downarrow
 $h = -1$ e $K = -1 \Rightarrow m' = -m$

NOTAZIONE - $\text{mcm}(a, b)$ sarà il positivo tra i due m e $-m$

OSS- $\text{mcm}(a, b) = a' \cdot b' \cdot \text{mcd}(a, b)$

$$\begin{aligned} \text{mcm}(a, b) \cdot \text{mcd}(a, b) &= a' \cdot b' \cdot \text{mcd}(a, b) \cdot \text{mcd}(a, b) \\ &= a \cdot b \end{aligned}$$

$$|ab| = \text{mcm}(a, b) \cdot \text{mcd}(a, b)$$

ES- $\text{mcm}(494, 214)$ prima trova $\text{mcd}(a, b)$

$$494 = 214 \cdot 2 + 16$$

$$214 = 16 \cdot 13 + 6$$

$$16 = 6 \cdot 2 + 4$$

$$6 = 4 \cdot 1 + 2$$

$$\text{mcd}(a, b) = 2 \Rightarrow \text{mcm}(494, 214) = \frac{494 \cdot 214}{2} = 52858$$

DEF - Sia $m \in \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$ la relazione definita da :

$a \equiv b \pmod{m} \Leftrightarrow a-b$ è multiplo di m

$$\exists k \in \mathbb{Z} : a-b = m \cdot k$$

$$\exists k \in \mathbb{Z} : a = b + m \cdot k$$

$$m | a-b$$

$m \in \mathbb{Z}$ si chiama congruenza modulo m .

TEOREMA

$m \in \mathbb{Z}$ è una relazione di equivalenza compatibile con $+$ e \cdot ,

cioè se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ allora $a+c \equiv b+d \pmod{m}$ e $a \cdot c \equiv b \cdot d \pmod{m}$.

DIM.-

(i) Riflessiva: $\forall a \in \mathbb{Z}, a \equiv a \pmod{m}$?

Vero perché $a-a=0=0 \cdot m \Rightarrow m | 0$

(ii) Simmetrica: $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$?

Se $a \equiv b \pmod{m}$ allora $\exists k \in \mathbb{Z} : a-b=m \cdot k$ da cui

riconosciamo $b-a=(-k) \cdot m \Rightarrow m | b-a$ e $b \equiv a \pmod{m}$

(iii) Transitiva: $\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$?

Per ipotesi $\exists h, k \in \mathbb{Z} : a-b=mh \wedge b-c=mk$

Ricaviamo b e sostituiamo $a-(c+mh)=mh \Rightarrow$

$\Rightarrow a-c=mh+mk=m(h+k) \Rightarrow m | a-c$ e $a \equiv c \pmod{m}$

② Per $\exists l, r \in \mathbb{Z} : a-b=ml \wedge c-d=mr$

Tesi: $\exists s, t \in \mathbb{Z} : (a+b)-(c+d)=sm \wedge ac-bd=tm$

Dalla ipotesi ho $(a-b)+(c-d)=ml+mr=m(l+r)$ da $(a+b)-(c+d)=m(l+r)$

$\Rightarrow (a+b) \equiv (c+d) \pmod{m}$

Dalle ipotesi, moltiplico ambo i termini per c (1°) e b (2°)

$(a-b)c=mc \cdot l \wedge (c-d)b=mc \cdot r$ e ora sommo

$(ac-bc)+(cb-bd)=mc(l+r) \Rightarrow ac-bd=mc(l+r)$

$\Rightarrow ac \equiv bd \pmod{m}$

ES.-

$$\begin{array}{r} 2 \quad 4 \in \mathbb{Z} \quad 6 \\ 2 \quad 4 \in \mathbb{Z} \quad 10 \end{array} \left\{ \text{stesso resto se dividono per } 2 \right.$$

ottenuti sommando + (o sottr.)

$$6=2 \cdot 2+2$$

$$10=2 \cdot 4+2$$

$$2=2 \cdot 0+2$$

NOTAZIONE $a \in \mathbb{Z}$ $b \in \mathbb{Z}$ $a \equiv_m b$ $a \equiv b \pmod{m}$

DEF - L'insieme quoziente ~~$\mathbb{Z}/m\mathbb{Z}$~~ $\mathbb{Z}/m\mathbb{Z}$ verrà denotato con \mathbb{Z}_m e chiamato insieme degli interi modulo m ed i suoi elementi sono denotati con $[x]_m$ opp. \bar{x}

OSS-

① Dato $m \in \mathbb{Z}$ e $x \in \mathbb{Z}$, $[x]_m = \{x + mk \mid k \in \mathbb{Z}\}$

$$[\bar{1}]_m = \{1 + 4k \mid k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

② $\forall x \in \mathbb{Z}$, $[x]_0 = \{x\}$ ($x + mk = x \pmod{m=0}$)

③ Se $m \neq 0$ \mathbb{Z}_m è infinito

④ $\forall x \in \mathbb{Z}$, se $m \neq 0$ $[x]_m = [\text{rest}(x, m)]_m$

$$x = mq + r \quad x - r = mq \Rightarrow x \equiv_m \text{rest}(x, m)$$

⑤ Se $m > 0$ e $0 < a, b < m$, $a \equiv_m b \Leftrightarrow a = b$

DIM.-

(\Leftarrow) Se $a = b \Rightarrow a$ è in relazione con b per la proprietà riflessiva di \mathbb{Z}

(\Rightarrow) Se $a \equiv_m b$, supponendo che $a \geq b$ si ha $a = b + mk$ con $k \geq 0$.
Ma deriva $a - b \leq a < m$ ma questo implica $k \leq 0$ da cui deriva $k = 0$ e quindi $a = b$.

TEOREMA

Sia $m > 0$, $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$. Quindi $|\mathbb{Z}_m| = m$

DIM-

$\forall x \in \mathbb{Z}$, $[x]_m = [\text{rest}(x, m)]$ e $0 \leq \text{rest}(x, m) \leq m-1$ e dal punto 5 della precedente osservazione sappiamo che a rest. diversi corrispondono classi diverse.

LEMMA

① $a \equiv b \pmod{m} \Leftrightarrow \forall c \in \mathbb{Z} \quad a + c \equiv b + c \pmod{m}$

② $a \equiv b \pmod{m} \Rightarrow \forall t \in \mathbb{Z} \quad at \equiv bt \pmod{m}$

③ Se $at \equiv bt \pmod{m}$ e $\text{gcd}(m, t) = 1 \Rightarrow a \equiv b \pmod{m}$

DEF - $\forall m \in \mathbb{Z}$, $\mathbb{Z}_m^* = \{[a]_m \mid \text{MCD}(a, m) = 1\} \subseteq \mathbb{Z}_m$

ES. - $\mathbb{Z}_3^* = \{[1]_3, [2]_3\}$ $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5\}$

$|\mathbb{Z}_m^*| = \text{Indicatore di Gauss-Eulero } \varphi(m)$

$$\varphi : \mathbb{Z} \rightarrow \mathbb{N}$$

$m \mapsto |\mathbb{Z}_m^*|$ il numero di interi positivi che sono coprimi con m - tra 0 e $m-1$ compresi

OSS - $\varphi(p) = |\mathbb{Z}_p^*| = |\{[1]_p, \dots, [p-1]_p\}| = p-1$

$\varphi(p^m) = p^m - p^{m-1}$ i multipli di p e le eventuali potenze non sono coprimi con p^2

Primo teorema di Fermat

Se $p \in \mathbb{N}$ è primo, allora $\forall a \in \mathbb{Z}$ si ha $a^p \equiv a \pmod{p}$

$$\text{Eg. } 4^3 \equiv 4 \pmod{3}$$

Teorema di Fermat-Eulero

Se $m > 1$ e $a \in \mathbb{Z}$, $\text{MCD}(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

$$\text{Eg. } 7^4 \equiv 1 \pmod{5} \quad [\bar{a}^{\varphi(m)} \equiv 1 \pmod{m}]$$

DEF - Dato $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, l'equazione $ax \equiv b \pmod{m}$

è detta equazione congruenziale lineare.

TEOREMA

Dato $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, l'equazione $ax \equiv b \pmod{m}$ ha soluzione

$\Leftrightarrow \text{MCD}(a, m) = 1$. Se \bar{x} è soluzione, l'insieme di tutte le soluzioni sarà $S = [\bar{x}]_m$ cioè $[\bar{x}]_m = \{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\}$

DIM-

Sia $\text{MCD}(a, m) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : 1 = au + mv$ da cui $mv = 1 - au \Rightarrow$

$\Rightarrow au \equiv 1 \pmod{m}$ [la loro diff. è un multiplo di m] da cui ricava

$bau \equiv b \pmod{m}$ e quindi bu è soluzione \bar{x} dell'equazione

• Se $t \in [\bar{x}]_m \Rightarrow \exists k \in \mathbb{Z} : t = \bar{x} + mk \Rightarrow t \equiv \bar{x} \pmod{m} \Rightarrow$

$\Rightarrow at \equiv a\bar{x} \pmod{m}$ e per ipotesi $a\bar{x} \equiv b \pmod{m} \Rightarrow at \equiv b \pmod{m}$

[per transitività] $\Rightarrow t \in \{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\}$

- Se $\exists \in \{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\} \Rightarrow z$ è soluzione e
 $az \equiv b \pmod{m}$ ma se s è soluzione $\Rightarrow as \equiv b \pmod{m}$ da cui ricavo $b \equiv as \pmod{m} \Rightarrow az \equiv as \pmod{m}$. Poiché per ipotesi $\text{MCD}(a, m) = 1$, posso dividere per $a \Rightarrow z \equiv s \pmod{m}$
 $\Rightarrow z \in \mathbb{Z}_m$

TEOREMA

Sia $m > 0$, $a, b \in \mathbb{Z}$ e $\alpha a \in \mathbb{Z}$ t.c. $t \in \mathbb{Z} : t|a$, $t|b$ e $t|m$.

Allora l'equazione $ax \equiv b \pmod{m}$ ha soluzione $\Leftrightarrow \left(\frac{a}{t}\right)x \equiv \left(\frac{b}{t}\right) \pmod{\frac{m}{t}}$
 ha soluzione $\Leftrightarrow \exists z \in \mathbb{Z}$

N.B. L'insieme delle soluzioni sarà

$$S = \mathbb{Z}_{\frac{m}{d}} = \mathbb{Z}_m \cup \left[\frac{b+m}{d}\right]_m \cup \left[\frac{b+2m}{d}\right]_m \cup \dots \cup \left[\frac{b+(k-1)m}{d}\right]_m$$

N.B. $ax \equiv b \pmod{m}$ ha sol. $\Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ha soluzione

con $d = \text{MCD}(a, m) \neq d|b$

COROLLARIO

Se $\text{MCD}(a, m) \nmid b \Rightarrow ax \equiv b \pmod{m}$ ha soluzione e la trovo risolvendo $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{m}{d}}$; con $d = \text{MCD}(a, m)$

ES. - $84x \equiv 108 \pmod{500}$

$$500 = 84 \cdot 5 + 80$$

$$125 = 21 \cdot 5 + 20$$

Ricavati dividendo per 4

$$84 = 80 \cdot 1 + 4$$

$$21 = 20 \cdot 1 + 1$$

$$80 = 4 \cdot 20 + 0$$

$$20 = 1 \cdot 20 + 0$$

$$\text{MCD}(500, 84) = 4 \quad \text{e} \quad 4|108 \quad \text{dunque}$$

$$21x \equiv 27 \pmod{125}$$

$$1 = 21 + (-1)(20) = 21 + (-1)(125 + (-5) \cdot 21) = (-1)125 + (6) \cdot 21$$

$$6 = 6 \cdot 21 = 126$$

$$S = \left[126\right]_{125} \rightarrow \left[37\right]_{125} = \left[37\right]_{500} \cup \left[37 + \frac{125}{4} \cdot 500\right]_{500} \cup \left[37 + \frac{1000}{4} \cdot 500\right]_{500} \\ \cup \left[37 + \frac{1500}{4} \cdot 500\right]_{500}$$

$$z \in [s]_m \Leftrightarrow z = s + m k$$

$$z \in \bigcup_{n=0}^{t-1} [s + \frac{nm}{c}]_m \Leftrightarrow \exists i \in \{0, \dots, t-1\} \text{ } \exists h \in \mathbb{Z} : z = s + ih + \frac{nm}{c}$$

TEOREMA CHINÉSE DEL RESTO

Sia $m_1, \dots, m_k \in \mathbb{Z}$, $b_1, \dots, b_k \in \mathbb{Z}$ con m_1, \dots, m_k a due a due coprimi. Il sistema $\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$ ha soluzione se e solo se l'insieme di tutte le

soluzioni è $S = [s]_{m_1 \cdot \dots \cdot m_k}$

Generalizzazione:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_j \pmod{m_j} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \text{ ha soluzione} \Leftrightarrow \operatorname{med}_{i \neq j} (m_i, m_j) \mid b_i - b_j$$

Nel caso le equazioni del sistema si presentino nella forma

$a_i : x \equiv b_i \pmod{m_i}$ basterà risolvere singolarmente trasformandole in $x \equiv s_i \pmod{m_i}$ con s_i soluzione della precedente ^{suddetta} eq.

Esempio:

$$\text{I} \quad \begin{cases} x \equiv 4 \pmod{5} \\ \text{II} \quad x \equiv 3 \pmod{4} \end{cases} \quad \operatorname{med}(5, 4) = 1 \quad \text{dunque possiamo cercare la soluzione}$$

Risolvendo I: $x = 4 + 5k \text{ con } k \in \mathbb{Z}$

Sostituendo nella II: $4 + 5k \equiv 3 \pmod{4}$ da cui

$$5k \equiv -1 \pmod{4}$$

Poiché $5 \equiv 1 \pmod{4}$ e $-1 \equiv 3 \pmod{4}$ si ha

$$1 \equiv 3 \pmod{4}$$

Sostituendo $k = 3$ nella I:

$$x = 4 + 5 \cdot 3 = 19$$

$$S = [19]_{4 \cdot 5} = [19]_{20}$$

Ex. -

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases} \quad \text{mcd}(5, 7) = \text{mcd}(7, 11) = \text{mcd}(5, 11) = 1$$

$$① m = m_1 \cdot m_2 \cdot m_3 = 385$$

$$② a_1 = m/m_1 = 77$$

$$a_2 = m/m_2 = 55$$

$$a_3 = m/m_3 = 35$$

③ Let's the equations in form $a_i x \equiv 1 \pmod{m_i}$ we have

$$i) 77x \equiv 1 \pmod{5}$$

$$ii) 55x \equiv 1 \pmod{7}$$

$$iii) 35x \equiv 1 \pmod{11}$$

$$77x \equiv 1 \pmod{5}$$

$$77 = 5 \cdot 15 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\text{mcd}(77, 5) = 1$$

$$1 = 5 + (-2) \cdot 2 = 5 + (-2)(77 + (-15) \cdot 5) = 5 + (-2) \cdot 77 + (30) \cdot 5$$

$$\text{thus } \gamma = -2 \cdot 1 = -2 \quad S = [-2]_5 = [3]_5$$

$$55x \equiv 1 \pmod{7}$$

$$55 = 7 \cdot 7 + 6$$

$$7 = 6 \cdot 1 + 1$$

$$6 = 1 \cdot 6 + 0$$

$$1 = 7 + (-1) \cdot 6 = 7 + (-1)(55 + (-7) \cdot 7) = 7 + (-1) \cdot 55 + (7) \cdot 7$$

$$\gamma = -1 \cdot 1 = -1 \quad S = [-1]_7 = [6]_7$$

$$35x \equiv 1 \pmod{11}$$

$$35 = 11 \cdot 3 + 2$$

$$2 = 2 \cdot 1 + 0$$

$$2 = 1 \cdot 2 + 0$$

$$l = l_1 + (-5) \cdot 2 = l_1 + (-5)(35 + (-3) \cdot 11) = l_1 + (-5)35 + (15)11$$

$$\gamma = -5 \cdot 1 = -5 \Rightarrow S = [-5]_{11} = [6]_{11}$$

La soluzione S del sistema è

$$S = \frac{a_1}{m_1} b_1 n_1 + \frac{a_2}{m_2} b_2 n_2 + \frac{a_3}{m_3} b_3 n_3 = 3573$$

$$S = [3573]_{385} = [108]_{385}$$

Esercizio -

$$\text{rest}(a, 3) = 2 \quad \text{rest}(a, 4) = 3 \quad \text{rest}(a, 7) = 6$$

$$\begin{cases} a \equiv 2 \pmod{3} \\ a \equiv 3 \pmod{4} \\ a \equiv 6 \pmod{7} \end{cases} \quad \text{med}(3, 4) = \text{nco}(3, 7) = \text{med}(3, 7) = 1$$

$$(i) \quad a = 2 + 3k \quad \text{con } k \in \mathbb{Z}$$

$$(ii) \quad 2 + 3k \equiv 3 \pmod{4} \rightarrow 3k \equiv +1 \pmod{4}$$

$$l = 4 + (-1) \cdot 3$$

$$k = -1 \equiv 3 \pmod{4} \quad \text{sostituendo in i}$$

$$a = 2 + 3 \cdot 3 = 11 \rightarrow [11]_{12} = 11 + 12k \quad \text{con } k \in \mathbb{Z}$$

$$(iii) \quad 11 + 12k \equiv 6 \pmod{7}$$

$$12k \equiv -5 \pmod{7} \Rightarrow 5k \equiv \underline{2} \pmod{7}$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1 \rightarrow l = 5 + (-2) \cdot 2 = 5 + (-2)(7 + (-1) \cdot 5) =$$

$$2 = l \cdot 2 + 0 \quad \Rightarrow \quad = \underline{(3)} 5 + (-2) \cdot 7$$

$$k = 2 \cdot 3 = 6$$

$$\Rightarrow \Delta = l_1 + l_2 \cdot 6 = 83, \quad S = [83]_{85}$$

Esercizio (7.2)

$S = \{a, b, c, d\}$ è sotto $P(S)$ insieme delle parti

$$|P(S)| = 2^{st} = 2^4 \quad \text{numero elementi}$$

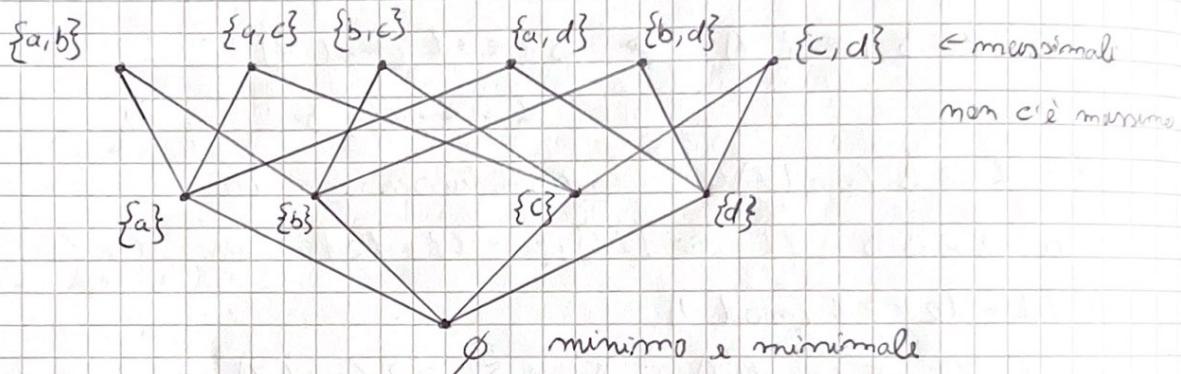
Si calcola $\sup P(S) (\{a, c\}, \{a, d\})$ e $\inf P(S) (\{a, c\}, \{a, d\})$

$$A, B \subseteq S \quad \inf(A, B) = A \cap B \quad \sup(A, B) = A \cup B$$

$$\inf(\cdot, \cdot) = \{a\} \quad \sup(\cdot, \cdot) = \{a, c, d\}$$

Sia $A = \{X \in P(S) : |X| \leq 2\}$ quanti e quali elementi lo compongono?

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



Osserviamo che $\{b, a\} \not\subseteq \{b, c\}$ e $\{b, c\} \not\subseteq \{b, a\}$

(7.3)

$$A = \{2, 3, 4\} \quad B = A \times A$$

$$(a, b) \sqsubseteq (c, d) \iff a \leq c \quad \& \quad b \leq d$$

① \sqsubseteq è d'ordine:

$$(a) (a, b) \sqsubseteq (a, b) \quad \text{verg} \quad a \leq a \quad \& \quad b \leq b$$

$$(b) (a, b) \sqsubseteq (c, d) \quad \& \quad (c, d) \sqsubseteq (a, b) \Rightarrow (a, b) = (c, d)$$

$$a \leq c \quad \& \quad b \leq d \quad c \leq a \quad \& \quad d \leq b \Rightarrow a = c \quad \& \quad b = d$$

$$(c) (a, b) \sqsubseteq (e, d) \quad \& \quad (e, d) \sqsubseteq (e, f) \Rightarrow (a, b) \sqsubseteq (e, f)$$

$$a \leq e \quad \& \quad b \leq d \quad e \leq e \quad \& \quad d \leq f \Rightarrow a \leq e \quad \& \quad b \leq f$$

(a)

$$B = \{(2, 2); (2, 3); (2, 4); (3, 2); (3, 3); (3, 4); (4, 2); (4, 3); (4, 4)\}$$

(B, \leq)

$(2, 2) \nleq (2, 3)$

$(2, 2) \leq (2, 4)$

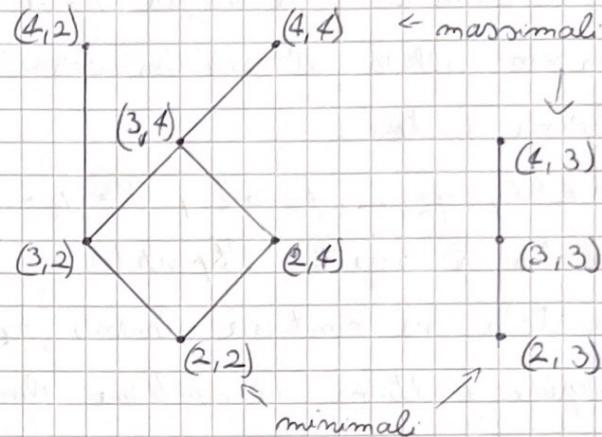
$(2, 2) \leq (3, 2) \leq (3, 4)$

$(2, 2) \leq (4, 2) \leq (4, 4)$

$(3, 2) \leq (3, 4) \leq (4, 4)$

$(3, 2) \leq (4, 2)$

$(2, 3) \leq (3, 3) \leq (4, 3)$



(iii) $(2, 2) \nleq (2, 3)$ non sono confrontabili, quindi (B, \leq) non è un reticolo

CALCOLO COMBINATORIO

• Princípio di addizione

Dati A, B insiemi finiti con $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$

• Princípio di inclusione - esclusione

Dati A, B finiti, $|A \cup B| = |A| + |B| - |A \cap B|$

$$|A \cdot B| = |A| \cdot |B|$$

$$A \cup B = (A \cdot B) \cup B$$

• Princípio di moltiplicazione

$$S = \{x_1, \dots, x_m\}, T = \{y_1, \dots, y_n\} \quad |S \times T| = |S| \cdot |T| = m \cdot n$$

• S, T insiemi finiti, $T^S := \{f : S \rightarrow T \mid f \text{ funzione}\} \quad |T^S| = |T|^{|\mathbb{S}|}$

[DIM.]

$$f \in T^S, T = \{y_1, \dots, y_n\} \cup S = \{x_1, \dots, x_m\}$$

$$\forall x_i \in S, f(x_i) \in T$$

$$f(x_1) \rightarrow m \text{ scelte} \quad (f(x_1) = y_1 \circ f(x_1) = y_2 \circ \dots)$$

duque ho m^n funzioni, cioè $|T|^{\mathbb{S}}$

• Principio della piccionaia (o dei cassetti)

Dati $n, m \in \mathbb{N}$, se voglio porre n oggetti in m cassetti e $n > m$, allora almeno un cassetto deve contenere 2 oggetti.

Forma forte:

$$n \in \mathbb{N}, q_1, \dots, q_m > 1, K = q_1 + \dots + q_m - m + 1$$

Se ho K oggetti ~~separati~~ partiti in m scatole, allora la prima scatola ne contiene almeno q_1 , oppure la seconda almeno q_2 , ..., oppure l'ultima ne contiene almeno q_m .

[Es.]

25 persone fanno lezione di MD e ottengono 28, 29 e 30.

Ciò significa che almeno 9 hanno lo stesso voto:

:::	:::	:::
..

3 0 2, 2 8

Distribuendo uno studente alla volta per cassetto, ottengo 8 studenti per cassetto. L'ultimo da aggiungere porterà il totale di uno di essi a 9

$$9 + 9 + 9 - 3 + 1 = 25 \\ (q_1 + q_2 + q_3 + \dots + q_9)$$

[DEF.] Dato $n \in \mathbb{N}_0$, chiamiamo fattoriale di n il numero

$$n(n-1)(n-2) \dots \cdot 2 \cdot 1$$

$$n! = n \cdot (n-1)!$$

$$0! := 1$$

[DEF.] $X \neq \emptyset$, $F_X = \{f: X \rightarrow X \mid f \text{ è biettiva}\}$

[PROPOSIZIONE]

Se $|X| = m \Rightarrow |F_X| = m!$

[DIM.] $X = \{x_1, \dots, x_m\}$

$f(x_1) = 1$ scelta

$f(x_2) = m-1$ scelta poiché f deve essere iniettiva

\vdots

$f(x_m) = 1$ scelta

$$\Rightarrow m \cdot (m-1) \cdot \dots \cdot 1 = m!$$

[DEF.] Le funzioni biettive di X in se stessa si chiamano

permutazioni

[ES]

Anagrammi di PERA

$$\overline{\quad \quad \quad \quad} \\ \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ 4 \quad 3 \quad 2 \quad 1 \quad 4! = 24$$

Anagramma di CASA

$$\overline{\quad \quad \quad \quad} \\ - \quad - \quad - \quad - \quad \frac{4!}{2!} = 12$$

Permutazioni con ripetizione

$$\frac{m!}{m_1! \cdot m_2! \cdots m_n!}$$

← permutazioni delle lettere rip.

Disposizioni di m oggetti su h posti

$$\overline{\quad \quad \quad \quad} \\ \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ 6 \quad 5 \quad 4 \quad 3 \quad \frac{6!}{2!} = 6 \cdot 5 \cdot 4 \cdot 3 = 360$$

$$\frac{m!}{(m-h)!} = d_{m,h}$$

PROPOSIZIONE

Sia $|X|=h$ e $|Y|=m$, $h \leq m$. Allora, detto $F = \{f: X \rightarrow Y \mid f \text{ è iniettiva}\}$

$$|F| = \frac{m!}{(m-h)!}$$

DIM.

Se $h > m$, non ci sono funzioni iniettive da X a Y

Se $h \leq m$, $X = \{x_1, \dots, x_h\} \subset Y = \{y_1, \dots, y_m\}$

$f(x_1) \rightarrow m$ scelti

$f(x_2) \rightarrow m-1$ scelti

\vdots
 $f(x_h) \rightarrow m-(h-1)$ scelti

~~$m(m-1) \cdots (m-(h-1))$~~ $\underbrace{(m-h)(m-(h+1)) \cdots \frac{1}{(m-h)!}}_{(m-h)!} = m!$

$$m(m-1) \cdots (m-(h-1)) = \frac{m!}{(m-h)!}$$

Disposizioni con ripetizione

$$N = \{0, \dots, 9\}, |N| = 10$$

$$\overline{\quad \quad \quad \quad \quad \quad} \\ \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ 10 \quad 10 \quad 10 \quad 10 \quad 10$$

h posti

m oggetti su h posti con ripetizione $\Rightarrow m^h$

Combinazioni semplice

Estraggo h oggetti da un insieme di m , senza ordine

$$\frac{m!}{(m-h)! \cdot h!}$$

L'espressione equivale a $\binom{m}{h}$ detto coefficiente binomiale

PROPOSIZIONE

Dato X insieme con $|X|=m$, il numero dei sottoinsiemi di cardinalità h è proprio $\binom{m}{h}$

D.M.

Un sottoinsieme $Y \subseteq X$ di cardinalità h si ottiene scegliendo h elementi da X . Poiché Y è un insieme, non conta l'ordine.

E.S.

$$Y \subseteq X \text{ t.c. } |Y| \leq 2$$

$$\binom{4}{0} + \binom{4}{1} + \binom{4}{2} = \frac{4!}{4! \cdot 0!} + \frac{4!}{3! \cdot 1!} + \frac{4!}{2! \cdot 2!} = 1 + 4 + 6 = 11$$

Proprietà del coefficiente binomiale

$$-(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i} = \binom{n}{0} b^n + \binom{n}{1} a b^{n-1} + \dots + \binom{n}{n} a^n$$

$$-2^4 = \binom{4}{0} + \binom{4}{1} + \dots + \binom{4}{4}$$

- Se p è primo, $p \mid \binom{p}{i} \quad \forall i < p$

Combinazioni con ripetizioni

Scegliere m oggetti tra K possibilità

Ese. numero di modi per disporre m sassolini in K scatole

$$\frac{(m+K-1)!}{(K-1)! \cdot m!} = \binom{m+K-1}{K-1} = \binom{m+K-1}{m}$$

E.S.

Scegliere 3 gusti per il gelato tra 5 possibili

$$m=3 \rightarrow K=5$$

$$\frac{(3+5-1)!}{(5-1)! \cdot 3!} = \frac{7!}{4! \cdot 3!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35$$

(4.1)

Anagrammi (anche senza senso compiuto) della parola INFORMATICA

$$21 \text{ lett. con } 2A + 2I \Rightarrow \frac{21!}{2! \cdot 2!}$$

(4.2)

Classe di 10 alunni da distribuire in due gruppi senza ripeterli

1 - 9

2 - 8

3 - 7

4 - 6

5 - 5

$$\binom{10}{1} + \binom{10}{2} + \binom{10}{3} + \binom{10}{4} + \binom{10}{5}$$

(4.3)

Modi di disporre 10 penne in 4 astucci

$$n = 10 \text{ e } k = 4$$

$$\frac{(10+4-1)!}{10! \cdot (4-1)!} = \frac{13!}{10! \cdot 3!}$$

(4.4)

Modi di disporre, in 3 astucci, 15 penne, di cui 9 blu e 6 rosse

distrib. blu



$$m_1 = 9 \quad m_2 = 6 \quad k = 3$$

$$\frac{(9+3-1)!}{9! \cdot (3-1)!} \cdot \frac{(6+3-1)!}{6! \cdot (3-1)!} = \\ = \frac{11!}{9! \cdot 2!} \cdot \frac{8!}{6! \cdot 2!}$$

distrib. rosse

(4.5)

Sottoinsiemi di cardinalità 3 inclusi in uno di cardinalità 7

$$\binom{7}{3}$$

(4.6)

Modi in cui 10 persone possono sedersi su una fila di 4 sedili

$$\frac{m!}{(m-k)!} = \frac{10!}{6!}$$

4.7

Confezione da 7 bottiglie di vino variegato. Sapendo che deve essere presente almeno uno dei 3 tipi di vino, quanti confezioni diverse?

$$3 = k$$

$$m = 7 - 3 = 4$$

$$\frac{(4+3-1)!}{4! \cdot (3-1)!} = \frac{6!}{4! \cdot 2!}$$

4.8

Invito 8 persone a una festa. Sapendo che si può rifiutare o accettare, quante combinazioni di invitati?

$$2 \cdot 2 \cdot \dots \cdot 2 = 2^8$$

4.9

Chiamo le cifre 2, 3, 7, 5, quanti m. naturali a 5 cifre?

$$\begin{array}{ccccc} \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 4 & 4 & 4 & 4 \end{array} \quad 4^5$$

DEF.

Dato un insieme S , una applicazione $L: S \times S \rightarrow S$ si detta **OPERAZIONE** (binaria) interna di S

L'insieme (S, L) è detto **STRUTTURA ALGEBRICA**

Notazione: $L(x, y) = z \iff x \perp y = z$

ES.

- $(\mathbb{N}, +)$

$+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$(2, 3) \mapsto 2 + 3 = 5$

$(x, y) \mapsto x + y$

- $(\mathbb{N}, *)$

$* : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$x * y = x^y$

$m \mapsto 3^m$

$(m, n) \mapsto m^n$

- $(\mathbb{R}, *)$

$* : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$

$(x, y) \mapsto 3x + 2y + 4$

$(x, y) \mapsto x^2 \cdot \log|y|$

- $X \neq \emptyset, (P(X), \cap)$

$\cap : P(X) \times P(X) \rightarrow P(X)$

$(A, B) \mapsto A \cap B$

- L insieme ordinato, (L, \vee)

$\vee : L \times L \rightarrow L$

è operazione se L rettangolo

$(a, b) \mapsto a \vee b = \sup(a, b)$

(L, \wedge) è struttura algebrica

DEF. Data (S, \perp) , \perp è detta:

Associativa $\forall x, y, z \in S, x \perp (y \perp z) = (x \perp y) \perp z$

Commutativa $\forall x, y \in S, x \perp y = y \perp x$

ES $(\mathbb{N}, *)$

i) $m * m = m^m$ non commutativa $\Rightarrow 2 * 3 = 2^3$ mentre $3 * 2 = 3^2$

ii) $m * (m * l) = (m * m) * l$

$m * (m^l) = (m^m) * l$

$m^{(m^l)} = (m^m)^l \Rightarrow m^{(m^l)} = m^{ml}$ che è falso

$V^V = \{f: V \rightarrow V \mid f \text{ è funzione}\}$

$f, g \in V^V, (g \circ f)(x) = g(f(x)) \quad \forall x \in V$

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

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

$h(g(f(x))) = h(g(f(x))) \quad \forall x \in V$

ii) non è commutativa $g \circ f \neq f \circ g$

DEF. Data (S, \perp) , un elemento $e \in S$ è detto elemento neutro per \perp :

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

\uparrow \uparrow
neutro a sx neutro a dx

DEF. Data (S, \perp) con e elemento neutro, un elemento $x \in S$ è detto simmetrico se $\exists x' \in S$ t.c.

$x \perp x' = e = x' \perp x$ e x' è detto simmetrico di x

ES

$(\mathbb{N}_0, +)$ nessun simmetrico

$(\mathbb{Z}, +)$ tutti gli elementi sono simmetrici

(\mathbb{Z}, \cdot) solo -1 e $+1$

(V^V, \circ) $f^{-1} \circ f = id = f \circ f^{-1}$

$X \rightarrow V \quad x \mapsto x$

e cioè le funzioni bigettive

[LEMMA] Data (S, \perp) con elemento neutro \perp , \perp associativa.

Se $x \perp y$ sono simmetrici rispetto a \perp , lo è anche $x \perp y$ e

$$(x \perp y)^\perp = y^\perp \perp x^\perp$$

[DIM.]

i) $(x \perp y) \perp (y^\perp \perp x^\perp) = \perp$

ii) $(y^\perp \perp x^\perp) \perp (x \perp y) = \perp$

i) $(x \perp y) \perp (y^\perp \perp x^\perp) = x \perp (y \perp y^\perp) \perp x^\perp = x \perp \perp \perp x^\perp = x \perp x^\perp = \perp$

ii) $(y^\perp \perp x^\perp) \perp (x \perp y) = y^\perp \perp (x^\perp \perp x) \perp y = y^\perp \perp \perp \perp y = y^\perp \perp y = \perp$

[N.B.] $(g \circ f)^\perp = f^\perp \circ g^\perp$

[DEF] Dato $a \in S$, con (S, \perp) , diremo che:

- a è cancellabile a sx se $\forall x, y \in S \quad a \perp x = a \perp y \Rightarrow x = y$
- a è cancellabile a dx se $\forall x, y \in S \quad x \perp a = y \perp a \Rightarrow x = y$
- a è cancellabile se lo è sia a sx che a dx

[N.B.] Se \perp è associativa, ogni elem. simmetr. è cancellabile

[DEF] (S, \perp, T) con due operazioni, diremo che T è distributiva su \perp

$$\text{se } \forall x, y, z \in S \quad x \perp (y \top z) = (x \perp y) \top (x \perp z) \quad (\text{dist a sx})$$

$$x \perp (y \top z) \perp x = (y \perp x) \top (z \perp x) \quad (\text{dist a dx})$$

[CS] $(P(S), \cap, \cup)$ $\forall A, B, C \in P(S)$

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

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

[DEF] Dati S, T insiemi, $f: T \times S \rightarrow S$ funzione si detta operazione esterna su S

$$\star: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$$

$$(\alpha, a) \mapsto \alpha a$$

$$\star: \mathbb{R} \times (\mathbb{R} \times \mathbb{R}) \rightarrow \mathbb{R}$$

$$(\alpha, (a, b)) \mapsto (\alpha a, \alpha b) \quad (3, (2, 2)) \mapsto (3, 6)$$

$$\star: \mathbb{R} \times \mathbb{R}^{\mathbb{R}} \rightarrow \mathbb{R}^{\mathbb{R}}$$

$$(a, f) \mapsto \alpha f$$

$$f(x) = e^x \quad (2f)(x) = 2 \cdot f(x) = 2e^x$$

STRUUTURE ALGEBRICHE NOTEVOLI

(S, \sqcup)

① SEMIGRUPPO se \sqcup è associativa

$(\mathbb{N}, +)$

② MONOIDE se \sqcup è associativa e c'è elemento neutro

$(\mathbb{N}_0, +)$

③ GRUPPO se \sqcup è associativa, c'è elem neutro e ogni elem è simmetrico.

$(\mathbb{Z}, +)$ $(\mathbb{F}, \circ) \leftarrow$ funz. biett. da X in \mathbb{X}

④ GRUPPO ABELIANO se (S, \sqcup) è gruppo e \sqcup è commutativa

$(\mathbb{Q}, +)$

(S, \sqcup, \sqcap)

⑤ ANELLO se (S, \sqcup) è gruppo abeliano, \sqcap distributiva su \sqcup e

\sqcap associativa $(\mathbb{Z}, +, \cdot)$ Matrici

⑥ ANELLO COMMUTATIVO se è anello e \sqcap è commutativa

⑦ ANELLO UNITARIO se è anello ed esiste neutro per \sqcap

⑧ CAMPO anello commutativo e unitario e ogni elemento

eccetto il neutro per \sqcup è simmetrizzabile rispetto a \sqcap

$(\mathbb{Q}, +, \cdot)$

⑨ DOMINIO DI INTEGRITÀ se è anello e c'è l'elemento

neutro e rispetto a \sqcup : $a \sqcap b = e \Leftrightarrow a = e$ opp. $b = e$

$(\mathbb{Z}, +, \cdot)$ $a \cdot b = 0 \Leftrightarrow a = 0$ opp. $b = 0$

[ES]

A insieme, chiamato alfabeto; A^+ insieme delle stringhe di lunghezza finita formate dagli elementi di A , dette parole

$w \in A^+$ è a_1, \dots, a_m ; $a_1, \dots, a_m \in A$

Consideriamo l'operazione $\cdot : A^+ \times A^+ \rightarrow A^+$

$$(a_1, \dots, a_m) \cdot (b_1, \dots, b_n) = a_1 a_2 \dots a_m b_1 \dots b_n$$

• detta concatenazione e (A^+, \cdot) semigruppo

Ha senso aggiungere $\mu :=$ parola vuota $A_\mu^+ = A^+ \cup \{\mu\}$

(A_μ^+, \cdot) è un monoide detto MONOIDE DELLE PAROLE

(DEF) (S, \perp) struttura algebrica. $X \subseteq S$ è detto parte stabile per \perp se $\forall x, y \in X, x \perp y \in X$ (X, \perp) sottostruutura di (S, \perp)

E.S.

$$(R - \{0\}, \frac{x}{y}) \Rightarrow (R - \{0\}, \frac{\cdot}{\cdot}) \text{ è sottostruatura} \quad \frac{a}{b} = \frac{ad}{bc} \in R$$

$(\mathbb{N}, \rightarrow)$ non è sottostr. es. $\frac{2}{7} \notin \mathbb{N}$

(\mathbb{R}, \cdot)

$([2, 0], \cdot)$ non è sottostr., perché $2 \cdot 2 = 4 \notin [2, 0]$

$([0, 1], \cdot)$ è parte stabile ($a \leq 1$ e $b \leq 1 \Rightarrow ab \leq 1$)

PROPOSIZIONE

Siano (S, \perp) struttura algebrica e $X \subseteq S$ parte stabile. Allora:

① Se \perp è associativa in $S \Rightarrow \perp$ è associativa in X

DIM.

Presto $x, y, z \in X$, sapendo che $x \perp y \in X$ e $y \perp z \in X$ ho $x \perp (y \perp z) \in X$ e $(x \perp y) \perp z \in X$. Poiché $X \subseteq S$ e \perp è associativa in S , abbiamo $x \perp (y \perp z) = (x \perp y) \perp z$, che è valida anche in X

② Se \perp è commutativa in $S \Rightarrow \perp$ è commutativa in X

③ Se S ha elem. neutro per \perp , i.e. $\exists e \in S$ l'è elem. neutro in X

④ Se S ha el. neutro per \perp , x è simmetricabile in S e $x' \in X \Rightarrow x'$ è simmetrico per x in X

E.S.

(\mathbb{N}, \cdot) è monoido

$$X = \{m \in \mathbb{N} \mid m \geq 5\}$$

$$a, b \in X \Rightarrow ab \in X$$

$$\downarrow \\ a \geq 5 \wedge b \geq 5 \Rightarrow ab \geq 25 > 5$$

Non è monoido perché $2 \notin X$

PROPOSIZIONE

Sia (S, \perp) un monoido. $\cup(S) = \{x \in S \mid x \text{ è simmetricabile}\} \subseteq S$

Allora $\cup(S)$ è un gruppo rispetto a \perp

DIM

① $e \in \cup(S)$ ($e = \text{elem. neutro}$) ?

e è simmetricabile, con $e' = e$ ($e \perp e = e$) $\Rightarrow e \in \cup(S)$

② $a, b \in \cup(S) \Rightarrow a \perp b \in \cup(S)$?

$(a \perp b)$ è simmetricabile $\wedge (a \perp b)' = b' \perp a' \Rightarrow a \perp b \in \cup(S)$

③ $\forall a \in \cup(S)$, il suo simmetrico $a' \in \cup(S)$?

Se a è simmetrica, $a' \perp a = e = a \perp a' \Rightarrow a'$ è simmetricabile
con simmetrico $a \Rightarrow a' \in \cup(S)$

E.S. (\mathbb{Z}, \cdot) $\cup(\mathbb{Z}) = \{z, -z\}$

DEF. Data (S, \perp) s.a., una congruenza è una relazione
di equivalenza compatibile con \perp

$R \subseteq S \times S$ è congruenza \Leftrightarrow (i) R è R. di equivalenza

(ii) $a_1 R a_2 \wedge b_1 R b_2$

$\Rightarrow (a_1 \perp b_2) R (a_2 \perp b_2)$

E.S. Congruenza modulo m è congruenza di $(\mathbb{Z}, +, \cdot)$ conello

DEF. Data (S, \perp) e $R \subseteq S \times S$ congruenza, l'insieme quoziente S/R
è una s.a. con operazione I definita da:

$$[x]_R I [y]_R = [x \perp y]_R \quad \text{Struttura quoziente}$$

PROPOSIZIONE

Sia (S, \perp) s.a. e $(S/R, I)$ s. quoziente

④ Se \perp è associativa $\Rightarrow I$ è associativa

DIM

$$\forall [x]_R, [y]_R, [z]_R$$

$$([x]_R I [y]_R) I [z]_R = [x \perp y]_R I [z]_R = [(x \perp y) \perp z]_R =$$

$$= [x \perp (y \perp z)]_R = [x]_R I [y \perp z]_R = \underline{[x]_R I ([y]_R I [z]_R)}$$



(2) Se \mathbb{I} è commutativa $\Rightarrow \mathbb{I}$ è commutativa

[DIM.]

$$[x]_R \mathbb{I} [y]_R = [x \perp y]_R = [y \perp x]_R = [y]_R \mathbb{I} [x]_R \quad \checkmark$$

(3) Se esiste el. neutro $e \in S \Rightarrow [e]_R$ è el. neutro per \mathbb{I}

(4) Se $x' \in S$ è il simmetrco di $x \in S \Rightarrow [x']_R$ è simmetrico di $[x]_R$

(5) Se ho (S, \perp, T) e T distribuisce su $\perp \Rightarrow T$ distribuisce su \mathbb{I} .

[ES.]

$$\mathbb{Z}_m = \mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

anello
quoziente

$$[a]_m + [b]_m = [a+b]_m$$

$$[a]_m \cdot [b]_m = [ab]_m$$

$[0]_m$ è neutro per $+$

$[1]_m$ è neutro per \cdot

[TEOREMA]

$$\mathbb{Z}_m^* = \cup(\mathbb{Z}_m) = \{[a]_m \mid \text{med}(a, m) = 1\}$$

$[a]_m$ è invertibile in $\mathbb{Z}_m \Leftrightarrow \text{med}(a, m) = 1$

[DIM.]

(\Rightarrow) Sia $[a]_m$ invertibile $\Rightarrow \exists [b]_m \in \mathbb{Z}_m$ t.c.:

$$[a]_m \cdot [b]_m = [1]_m \Rightarrow [ab]_m = [1]_m \Rightarrow ab \equiv 1 \pmod{m}$$

$$\Rightarrow \exists k \in \mathbb{Z} : ab - 1 = km \Rightarrow 1 = ab + km$$

$$\Rightarrow 1 = \text{med}(a, m)$$

perché $\forall t : t/a \in t/m$, ho $t/1 \Rightarrow t = 1$

(\Leftarrow) Sia $\text{med}(a, m) = 1$, allora $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\} =$

$$= \{[0]_m, [a]_m, \dots, [(m-1)a]_m\}$$

$$\Rightarrow \exists k = 1, \dots, m : [ka]_m = [1]_m$$

$$[k]_m \cdot [a]_m = [1]_m \quad \checkmark$$

[COROLARIO]

\mathbb{Z}_m campo $\Leftrightarrow m$ è primo

[DEF.] Siamo (S, \sqcup) e $(T, *)$ due s. a. Il prod. cartesiano $S \times T$ è una s. a. con operazione così definita:

$$(s_1, t_1) \sqcup (s_2, t_2) = (s_1 \sqcup s_2, t_1 * t_2)$$

[PROPOSIZIONE] $S \times T$ è un s. a.

- ① Se $\sqcup, *$ sono associative $\Rightarrow \sqcup$ è associativa
- ② Se $\sqcup, *$ sono commutative $\Rightarrow \sqcup$ è commutativa
- ③ Se e_S è el. n. im S e e_T è el. n. im T $\Rightarrow (e_S, e_T)$ è elem. neutro im $S \times T$
- ④ $\forall (s, t) \in S \times T$, se \sqcup è simmetrico di \sqcap
 $s \sqcap t = t \sqcap s \quad \Rightarrow \quad (s', t') \in \text{simm per } \sqcap$

[ES]

$$(\mathbb{R}, +) \quad (\mathbb{R} \times \mathbb{R}, \sqcup)$$

$$(a, b) \sqcup (c, d) = (a + c, b + d)$$

$$(a, b) \sqcup (0, 0) = (a + 0, b + 0) = (a, b)$$

$$-(a, b) = (-a, -b)$$

$$(\mathbb{R}, +) \times (\mathbb{R}, \cdot)$$

$$(a, b) \sqcup (c, d) = (a + c, b \cdot d)$$

$(0, 1)$ è neutro

$$\left(-a, \frac{1}{b}\right) \quad b \neq 0 \quad (a, 0) \text{ non è simmetr.} \quad \forall a \in \mathbb{R}$$

[DEF.] Siamo (S, \sqcup) e $(T, *)$ s. a. $f: S \rightarrow T$ si detta

omomorfismo se $\forall a, b \in S \quad f(a \sqcup b) = f(a) * f(b)$

• Monomorfismo se la funzione è iniettiva

• Epimorfismo \Leftrightarrow è suriettiva

• Isomorfismo \Leftrightarrow è biiettiva

[ES.] $f: (\mathbb{N}, +) \rightarrow (\mathbb{N}, \cdot)$ $m \mapsto 2^m$

$$\forall m, n \in \mathbb{N} \quad f(m+n) = f(m) \cdot f(n)$$

$$2^{m+n} = 2^m \cdot 2^n \quad \checkmark$$

$$f(m+n) = f(m) + f(n)$$

$$2^{m+n} \neq 2^m + 2^n \quad \text{Falso}$$

ESERCIZIO

$$(\mathbb{Z}, \perp) \quad a \perp b = a + b - 5$$

$$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, \perp)$$

$$x \mapsto 5-x$$

Verifichiamo che f sia isomorfismo

1) $\forall a, b, c \in \mathbb{Z}, \quad a \perp (b \perp c) = (a \perp b) \perp c$

$$a \perp (b + c - 5) = a + (b + c - 5) - 5 = a + b + c - 10$$

$$\begin{aligned} (a \perp b) \perp c &= (a + b - 5) \perp c = ((a + b - 5) + c) - 5 = \\ &= a + b - 5 + c - 5 = \underline{\underline{a + b + c - 10}} \end{aligned}$$

2) Esiste $e \in \mathbb{Z}: a \perp e = e \perp a \quad \forall a \in \mathbb{Z}$

$$\begin{cases} a + e - 5 = a \\ e + a - 5 = a \end{cases} \Rightarrow \begin{cases} e - 5 = 0 \\ e - 5 = 0 \end{cases} \Rightarrow e = 5$$

3) $\forall a \in \mathbb{Z}$ esiste $a' \in \mathbb{Z}: a \perp a' = 5 = a' \perp a$

$$\Rightarrow a + a' - 5 = 5 \Rightarrow a' = 10 - a \in \mathbb{Z}$$

$a' = 10 - a$ è il simm. di a

4) $\forall a, b \in \mathbb{Z}, \quad a \perp b = b \perp a$

$$a + b - 5 = b + a - 5 \Rightarrow (\mathbb{Z}, +) \text{ è gruppo commutativo}$$

5) $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, \perp) \quad f$ è biettiva

$$x \mapsto 5 - x \quad f \text{ è omomorfismo}$$

$$\forall a, b \in \mathbb{Z}, \quad f(a+b) = f(a) \perp f(b)$$

$$5 - (a+b) \mid (5-a) \perp (5-b)$$

$$= 5 - a - b \mid \underline{\underline{(5-a)+(5-b)-5}} =$$

$$= 5 - a + 5 - b - 5 =$$

$$= \underline{\underline{5 - a - b}}$$

6) f è iniettiva
 $a \neq b \Rightarrow f(a) \neq f(b)$

$$f(a) = f(b) \Rightarrow a = b$$

$$f(a) = f(b) \Rightarrow 5 - a = 5 - b \Rightarrow -a = -b \Rightarrow a = b$$

7) f è suriettiva $\forall b \in \mathbb{Z}$ (codominio) esiste $a \in \mathbb{Z}$ (dominio)

t.c. $f(a) = b$ svol

$$5 - a = b \Rightarrow a = 5 - b \quad \underline{\underline{\text{Vero}}}$$

ESEMPIO DI STRUTTURA ALGEBRICA

① (\mathbb{Q}, \perp) , $x \perp y = \frac{3}{2}xy$ si dimostri che l'applicazione

$f: \mathbb{Q} \rightarrow \mathbb{Q}$ $f(x) = \frac{2}{3}x$ è isomorfismo di (\mathbb{Q}, \cdot) in (\mathbb{Q}, \perp)

1) $x \perp y = y \perp x$?

$$\frac{3}{2}xy = \frac{3}{2}yx \quad \checkmark$$

2) $x \perp (y \perp z) = (x \perp y) \perp z$

$$x \perp \left(\frac{3}{2}yz\right) = \left(\frac{3}{2}xy\right) \perp z$$

$$\frac{3}{2}x \cdot \frac{3}{2}yz = \frac{3}{2}xy \cdot \frac{3}{2}z \Rightarrow \frac{9}{4}xyz = \frac{9}{4}xyz \quad \checkmark$$

3) $\forall x \in \mathbb{Q}$, $x \perp x = x$

$$\frac{3}{2}x \cdot x = x \Rightarrow x = \frac{2}{3} \quad \text{se } x \neq 0$$

$$\text{se } x = 0 \Rightarrow 0 \perp \frac{2}{3} = 0$$

4) $(\mathbb{Q} - \{0\}, \perp)$

$$\forall x \in \mathbb{Q} - \{0\} \exists x' \in \mathbb{Q} - \{0\} : x \perp x' = x$$

$$\Rightarrow \frac{3}{2}x \cdot x' = \frac{2}{3} \Rightarrow x \cdot x' = \frac{4}{9} \quad x \neq 0, x' = \frac{4}{9} \cdot \frac{1}{x}$$

$x = 0 \Rightarrow$ non ha
simm.

(\mathbb{Q}, \perp) non è un gruppo $(\mathbb{Q} - \{0\}, \perp)$ è un gruppo

$f: (\mathbb{Q}, \cdot) \rightarrow (\mathbb{Q}, \perp)$

$x \mapsto \frac{2}{3}x$ è isomorfismo

5) $f(x \cdot y) = f(x) \perp f(y)$

$$\frac{2}{3}xy = \frac{2}{3}x \perp \frac{2}{3}y$$

$$= \frac{3}{2} \left(\frac{2}{3}x \right) \left(\frac{2}{3}y \right) = \frac{2}{3}xy \quad \checkmark$$

$$2) f \text{ è iniettiva: } \frac{2}{3}x = \frac{2}{3}y \Rightarrow x=y$$

$$f \text{ è suriettiva: } \forall y \in \mathbb{Q} \exists x \in \mathbb{Q} : y = \frac{2}{3}x$$

$$\Rightarrow x = \frac{3}{2}y \text{ perché } f\left(\frac{3}{2}y\right) = \frac{2}{3} \cdot \frac{3}{2}y = y$$

[DEF] Dato $(A, +, \cdot)$ anello, un elemento a è detto divisore dello zero se esiste $b \in A$: $a \neq 0, b \neq 0$, $ab = 0$ (\mathbb{Z}_m con m non primo li ha)

$$\boxed{\text{ES}} \quad \mathbb{Z}_{\leq 1} = \{2\}_{\leq 1} \cdot \{2\}_{\leq 1} = \{4\}_{\leq 1} = \{0\}_{\leq 1}$$

$$(2) \quad W = \{3h+1 \mid h \in \mathbb{N}_0\} \subseteq \mathbb{N}_0$$

a) si dim che W è parte stabile di $(\mathbb{N}_0, +)$ e non di (\mathbb{N}_0, \cdot)

b) $R \subseteq W \times W$, $(3h+1) R (3k+1) \Leftrightarrow h+k \in 2\mathbb{N}_0$ i congruenze in $(W, +)$

c) Studiare $(W/R, \cdot)$ stu. quoziente

$$W = \{1, 4, 7, 10, \dots\}$$

$$\bullet \quad \forall (3h+1), (3k+1) \in W, (3h+1)(3k+1) \in W$$

$$3h+k+3h+3k+1 \in W$$

$$3(3h+k+h+k)+1 \in W \quad \checkmark$$

$$\bullet \quad \forall (3h+1), (3k+1) \in W, (3h+1)+(3k+1) \in W$$

$$3(h+k)+2 \stackrel{?}{=} \in W \quad \text{Falso!}$$

(b)

$$(3h+1) R (3k+1) ?$$

è vero perché $h+k \in 2\mathbb{N}_0$

$$(3h+1) R (3l+1) \Rightarrow (3k+1) R (3l+1)$$

per ipotesi $h+k \in 2\mathbb{N}_0$, ma allora anche $k+l \in 2\mathbb{N}_0$. Vero

$$(3h+1) R (3l+1) ?$$

$$(3k+1) R (3l+1) \quad \left\{ \Rightarrow (3h+1) R (3l+1) \right.$$

per ipotesi $h+k \in 2\mathbb{N}_0 \Rightarrow h, k \text{ pari} \Rightarrow K, l \text{ pari} \Rightarrow h+l \text{ pari}$

$K+l \in 2\mathbb{N}_0 \Rightarrow h, k \text{ dispari} \Rightarrow K, l \text{ dispari} \Rightarrow h+l \text{ pari}$

$$R \text{ è congruenza se } \begin{cases} (3h+1) R (3k+1) \\ (3s+1) R (3t+1) \end{cases} \quad \left\{ \begin{array}{l} h+k \text{ è pari} \\ s+t \text{ è pari} \end{array} \right.$$

$$\Rightarrow (3h+1)(3s+1) R (3k+1)(3t+1)$$

$$3hs + 3h + 3s + 1 + 3ke + 3k + 3t + 1 \text{ è pari?}$$

$$3(hs + ke) + 3(h+k) + 3(s+t) + 2$$

$\downarrow \quad \uparrow \quad \downarrow \quad \uparrow$
pari pari pari pari

pari se $hs + kt$ è pari

$$h, k \text{ pari} \Rightarrow \begin{cases} s, t \text{ pari} \Rightarrow hs \text{ pari} \\ kt \text{ pari} \end{cases} \quad \left\{ \begin{array}{l} \text{somma pari} \\ hs \text{ pari} \end{array} \right.$$

$$h, k \text{ pari} \Rightarrow \begin{cases} s, t \text{ dispari} \Rightarrow hs \text{ dispari} \\ s, t \text{ pari} \Rightarrow hs \text{ dispari} \end{cases} \quad \left\{ \begin{array}{l} \text{somma pari} \\ hs \text{ dispari} \end{array} \right.$$

$$h, k \text{ dispari} \Rightarrow \begin{cases} s, t \text{ dispari} \Rightarrow hs \text{ dispari} \\ kt \text{ dispari} \end{cases} \quad \left\{ \begin{array}{l} \text{somma pari} \\ hs \text{ dispari} \end{array} \right.$$

$\Rightarrow hs + kt$ è sempre pari e quindi R è congruenza

c) Sapendo che (\mathbb{N}_0, \cdot) è un monoido commutativo, basta dimostrare che l'elemento neutro della moltiplicazione appartiene a $(W/R, \cdot)$

In W quando ha $h=0 \Rightarrow 3h+1 = 0+1 = 1$

$$③ W = \{3^n \cdot 7^m \mid n, m \in \mathbb{N}_0\} \subseteq \mathbb{N}$$

a) dim che W è parte stabile di (\mathbb{N}_0, \cdot) e non di $(\mathbb{N}_0, +)$

$$b) R \subseteq W \times W, 3^n 7^m R 3^s 7^t \Leftrightarrow |n-m| = |s-t|$$

④ verifica che sia di equivalenza ma non congr. in (W, \cdot)

$$\circ (3^n 7^m) \cdot (3^s 7^t) = 3^{n+s} 7^{m+t} \in W$$

$$\circ (3^n 7^m) + (3^s 7^t) \Rightarrow \text{es. } 3^0 7^0 + 3^0 7^0 = 1+1=2 \notin W$$

⑤

$$\circ 3^n 7^m R 3^s 7^t \Leftrightarrow |n-m| = |s-t| \quad \underline{\text{vera}}$$

$$\circ 3^n 7^m R 3^s 7^t \Leftrightarrow 3^n 7^m R 3^s 7^t$$

$$|n-m| = |s-t| \Rightarrow |s-t| = |n-m| \quad \underline{\text{vera}}$$

$$\left. \begin{array}{l} \bullet 3^m 7^m R 3^n 7^k \\ \quad 3^o 7^e R 3^l 7^k \end{array} \right\} \Rightarrow 3^m 7^m R 3^l 7^k$$

$$|m-m| = |n-t| \Rightarrow |m-m| = |h-k| \text{ vero}$$

$$|n-t| = |h-k|$$

$$\bullet \exists 3^2 7^2 R 3^2 7^1 \quad |2-2| = |2-2|$$

$$3^0 7^2 R 3^2 7^4 \quad |0-2| = |2-4|$$

$$3^2 7^2 \cdot 3^0 7^2 R 3^2 7^4 3^2 7^4$$

$$3^2 7^4 R 3^4 7^5$$

$$|2-4| = |4-5|$$

$3=2$ falso R non è congruenza

④ $S \neq \emptyset$ $g: P(S) \rightarrow P(S)$, $g(X) = S \setminus X$ applicazione
è isomorfismo di $(P(S), \cup)$ in $(P(S), \cap)$?

• g è iniettiva $g(X) = g(Y) \Rightarrow S \setminus X = S \setminus Y \Rightarrow S \setminus (S \setminus X) = S \setminus (S \setminus Y)$

$$=X =Y$$

• g è suriettiva. $\forall X \subseteq S$, $X = S \setminus (S \setminus X)$

$$g(S \setminus X) = X$$

• g è omomorfismo: $g(X \cup Y) = g(X) \cap g(Y)$

$$S \setminus (X \cup Y) = (S \setminus X) \cap (S \setminus Y)$$

$$a \in S \setminus (X \cup Y) \Leftrightarrow a \notin X \cup Y \Leftrightarrow a \notin X \wedge a \notin Y$$

$$\Leftrightarrow a \in S \setminus X \wedge a \in S \setminus Y \Leftrightarrow a \in (S \setminus X) \cap (S \setminus Y)$$

$$⑤ (\mathbb{Z}_2, +, \cdot), (\mathbb{Z}_6, +, \cdot)^{\text{anello}}, G = (\mathbb{Z}_2 \times \mathbb{Z}_6, +, \cdot)$$

a) Scrivere gli elem. dell'anello prodotto G

b) Ridurre le seguenti somme (vedi dopo)

c) Trovare almeno una coppia di divisori dello zero di G

d) Dim. che $T = \{(a, 2b) \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_6\}$ è sottogruppo di $(G, +)$

$$a) \quad \mathbb{Z}_2 \times \mathbb{Z}_6 = \{ ([0]_2, [0]_6), ([0]_2, [1]_6), ([0]_2, [2]_6), ([0]_2, [3]_6), \\ ([0]_2, [4]_6), ([0]_2, [5]_6), ([1]_2, [0]_6), ([1]_2, [1]_6), \\ ([1]_2, [2]_6), ([1]_2, [3]_6), ([1]_2, [4]_6), ([1]_2, [5]_6) \}$$

$$b) \quad [0]_6 + [2]_6 + [5]_6 = [7]_6 = [1]_6$$

$$[1]_2 + [2]_2 + [3]_2 = [0]_2 = [1]_2$$

$$[2]_6 \cdot [5]_6 = [10]_6 = [4]_6$$

$$[3]_6 \cdot [0]_6 = [0]_6 = [3]_6$$

$$([0]_2, [0]_6) + ([1]_2, [2]_6) = ([1]_2, [5]_6)$$

$$([1]_2, [1]_6) + ([0]_2, [4]_6) = ([1]_2, [5]_6)$$

$$([1]_2, [2]_6) + ([1]_2, [1]_6) = ([2]_2, [2]_6) = ([0]_2, [2]_6)$$

$$([0]_2, [3]_6) + ([0]_2, [3]_6) = ([0]_2, [6]_6) = ([0]_2, [0]_6)$$

$$c) \quad a \in \mathbb{R} : \exists b \quad ab = 0 \text{ con } a \neq 0 \text{ e } b \neq 0$$

$$([0]_2, [2]_6) \cdot ([0]_2, [3]_6) = ([0]_2, [6]_6) = ([0]_2, [0]_6)$$

d) 1) è parte stabile

$$(a_1, 2b_1) + (a_2, 2b_2) = (a_1 + a_2, 2(b_1 + b_2)) \quad \checkmark$$

2) $([0]_2, [0]_6)$ è della forma $(a, 2b)$ con $a \in \mathbb{Z}_2$ e $b \in \mathbb{Z}_6$

$$\downarrow \quad \downarrow$$

$$a \in \mathbb{Z}_2 \quad 2 \cdot [0]_6 = [0+0]_6 = [0]_6 \in \mathbb{Z}_6$$

3) Cerchiamo l'opposto

$$(a, 2b) = ([c]_2, 2[d]_6) = ([c]_2, [2d]_6)$$

\Rightarrow in G l'opposto è $([-c]_2, 2[-d]_6)$

$$\downarrow \quad \downarrow$$

$c \in \mathbb{Z}_2 \quad d \in \mathbb{Z}_6 \quad$ dunque ogni elem.
è simmetrico risalente

MATRICI

tabelle ordinate di elementi appartenenti
allo stesso insieme

Dati $m, n \in \mathbb{N}$ $m, n > 0$ si chiama matrice $m \times n$ su \mathbb{R}
una tabella di numeri reali disposti in m righe e n colonne.

$A = \begin{pmatrix} \sqrt{2} & -4 & 0 & \frac{1}{2} \\ 3 & 0 & 2 & -5 \\ x & 1 & 0 & 9 \end{pmatrix}$ è una matrice 3×4 i cui elementi
vengono indicati con a_{ij} : $1 \leq i \leq m$
 i indica la riga, $1 \leq j \leq n$ la colonna.

Per indicare un'intera riga si usa un apice: $A^{(i)}$ riga
 i -esima; $A^{(j)}$ indica invece la colonna j -esima

Matrice riga: matrice formata da 1 riga ed n colonne ($1, n$)

Matrice colonna: mat. formata da 1 colonna ed m righe ($m, 1$)

Matrice quadrata: mat. in cui $m = n$. Vi indroduciamo una
diagonale principale (\nearrow) fatta di elem. i cui indici di riga e
colonna sono uguali ed una secondaria (\nwarrow).

In una matrice quadrata:

- se $a_{ij} = a_{ji}$, la matrice è simmetrica
- se $a_{ij} = -a_{ji}$, la matrice è antisimmetrica
- se gli elem. al di sotto della diag. principale sono uguali
a 0, la matrice è triangolare superiore
- se gli elem. al di sotto sopra della diag. princ. sono nulli,
la matrice è triangolare inferiore
- se gli elem. al di fuori della diag. princ. sono nulli,
la matrice è diagonale
- se gli elem. al di fuori della diag. secund. sono nulli,
la matrice è antidiagonale
- se la cosa è anche diagonale e gli elem. lungo la diag.
sono tutti uguali, la matrice è reale: in particolare
se questi sono 1, la matrice è detta identità

Matrice nulla: ~~nessuna~~ matrice di dim. qualsiasi costituita da 0.

Matrice a scala: matrice $m \times n$ in cui il primo elem. non nullo della i -esima riga è più a dx del primo elem. non nullo della riga precedente.

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 4 \\ 0 & 0 & 5 \end{pmatrix} \checkmark \quad \begin{pmatrix} 1 & 2 & 1 \\ 3 & 4 & 5 \\ 0 & 0 & 8 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \checkmark \quad \leftarrow \text{se c'è una riga nulla, anche le restanti devono essere nulle}$$

Il 1° elem. $\neq 0$ è detto pivot

Data una matrice A, chiamiamo trasposta di A la matrice ottenuta scambiando le righe con le colonne

$$A = \begin{pmatrix} 1 & 2 & 7 & 0 \\ 5 & 9 & 3 & 8 \end{pmatrix} \rightarrow A^T = \begin{pmatrix} 1 & 5 \\ 2 & 9 \\ 7 & 3 \\ 0 & 8 \end{pmatrix} \quad (A^T)^T = A$$

vale la relazione $a_{ij} = b_{ji}$

Nota: la trasposta di una mat. quadrata è ancora una mat. quadrata dello stesso ordine

date 2 matrici $A, B \in M_{m \times n}(\mathbb{R})$ di uguale grandezza definiamo la somma $A + B = C \in M_{m \times n}(\mathbb{R})$

$$c_{ij} = a_{ij} + b_{ij} \quad i \in \{1, \dots, m\}, j \in \{1, \dots, n\}$$

$$A = \begin{pmatrix} 1 & 5 & 7 \\ -8 & 2 & 9 \end{pmatrix} \quad B = \begin{pmatrix} 0 & -5 & 8 \\ 3 & 1 & -2 \end{pmatrix} \quad A + B = \begin{pmatrix} 1 & 5 & 7 \\ -8 & 2 & 9 \end{pmatrix} + \begin{pmatrix} 0 & -5 & 8 \\ 3 & 1 & -2 \end{pmatrix} =$$

$$= \begin{pmatrix} 1+0 & 5+(-5) & 7+8 \\ -8+3 & 2+1 & 9+(-2) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 15 \\ -5 & 3 & 7 \end{pmatrix}$$

Data una matrice A qualsiasi, si dice opposta di A la matrice i cui elementi sono gli opposti dei rispett. elem. di A

Per come è definita la somma tra matrici è banale dimostrare sia la proprietà commutativa che quella distributiva, inoltre esistono sia elem. neutro (mat. nulla) che l'opposto, pertanto la somma è una operazione binaria interna a $(M_{m \times n}(\mathbb{R}), +)$ è gruppo abeliano

Data una matrice $A_{m \times m}$ ed un $\lambda \in \mathbb{R}$, definiamo il prodotto di una matrice per uno scalare

$$P_{i,j} = \lambda a_{i,j}, \text{ con } i \in \{1, 2, \dots, m\}, j \in \{1, 2, \dots, m\}$$

$$A = \begin{pmatrix} 3 & -6 \\ 2 & 0 \end{pmatrix} \quad \lambda = 3 \quad \lambda A = P = \begin{pmatrix} 3 \cdot 3 & -6 \cdot 3 \\ 2 \cdot 3 & 0 \cdot 3 \end{pmatrix} = \begin{pmatrix} 9 & -18 \\ 6 & 0 \end{pmatrix}$$

$$\lambda(A+B) = \lambda A + \lambda B$$

$$(\lambda + \mu) A = \lambda A + \mu A$$

$$\lambda I = A$$

Il prodotto tra matrici o prodotto righe per colonne è:

$$c_{i,j} = \sum_{k=1}^n a_{i,k} \cdot b_{k,j}$$

ed è applicabile solo se le mat.
sono compatibili (Col. della 1^a =
righe della 2^a)

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \end{pmatrix} \quad B = \begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix} \quad \text{Il risultato avrà il num. d. righe
della 1^a e il num. d. colonne della 2^a}$$

$$AB = \begin{pmatrix} (1 \cdot 4) + (0 \cdot -2) + (2 \cdot 0) & (1 \cdot 1) + (0 \cdot 2) + (2 \cdot 3) \\ (0 \cdot 4) + (3 \cdot -2) + (-1 \cdot 0) & (0 \cdot 1) + (3 \cdot 2) + (-1 \cdot 3) \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ -6 & 3 \end{pmatrix}$$

Facendo altri calcoli si può verificare che il prodotto tra matrici non è commutativo (spesso neanche è possibile fare $B \cdot A$)

Nell'ipotesi in cui il prodotto sia eseguibile, valgono la

proprietà associativa $A(BC) = (AB)C$ e la

prop. distributiva del prod. rispetto alla somma $A(B+C) = AB+AC$

La matrice identità Id_m è l'elemento neutro nel caso di moltiplicazione di matrici quadrate

Non vale la legge di annullamento del prodotto: $AB = 0$ ma $A \neq 0$ e $B \neq 0$

(es)

$$A = \begin{pmatrix} 3 & 6 \\ 2 & 2 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} \quad AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Una matrice qualsiasi può essere trasformata in una matrice a scala tramite 3 operazioni elementari:

- Moltiplicare una riga per uno scalare $\lambda \neq 0$
- Scambiare due righe
- Sommare ad una riga il multiplo di un'altra

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 2 & 1 & 5 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 2 & 1 & 5 \end{pmatrix} \xrightarrow{R_3 \rightarrow R_3 - R_2} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} \xrightarrow{R_3 \rightarrow R_3 - R_2} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \checkmark$$

Il metodo di eliminazione di Gauss è un algoritmo ricorsivo che sfrutta le tre operazioni appena viste:

consideriamo la prima colonna A_1 della matrice A.

Su A_2 è nulla, consideriamo la matrice B ottenuta togliendo ad A la riga A_1 . Se invece A_2 è non nulla, possiamo fare in modo che il primo elemento di A_2 sia diverso da zero e tutti gli altri siano 0. Fatto ciò, consideriamo la matrice C ottenuta togliendo ad A sia la prima riga che la prima colonna.

N.B.: l'algoritmo prevede risultati diversi in base alle scelte effettuate

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \\ 3 & 0 & 1 \end{pmatrix} \Rightarrow \text{La } 1^{\text{a}} \text{ colonna } c_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \text{ dunque vanno annullati } 2 \text{ e } 3$$

$$\lambda R_1 + R_2 = 0 \Rightarrow \lambda = -2 \quad \text{e} \quad \lambda R_1 + R_3 = 0 \Rightarrow \lambda = -3$$

$$\xrightarrow{\begin{array}{l} R_2 \rightarrow R_2 - 2R_1 \\ R_3 \rightarrow R_3 - 3R_1 \end{array}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & -3 & 1 \end{pmatrix} \quad \text{Trascuriamo } 1^{\text{a}} \text{ riga e prima colonna}$$

$$B_1 = \begin{pmatrix} -1 \\ -3 \end{pmatrix} \Rightarrow \lambda R_1 + R_2 = 0 \Rightarrow \lambda = -3$$

$$\xrightarrow{R_3 \rightarrow R_3 - 3R_2} \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -2 \end{pmatrix} \checkmark$$

Data una matrice M a scala, questa si dice a scala ridotta se tutti i pivot sono uguali ad 1 e la parte di colonna ad essi sovrastante è posta a 0. Questa matrice è univocamente determinata, cioè è unica data la matrice di partenza A : A è equivalente a $T = A \sim T$

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix} \xrightarrow{\begin{array}{l} R_2 \leftarrow -1 \cdot R_2 \\ R_3 \leftarrow -\frac{1}{2}R_3 \end{array}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{R_2 \leftarrow R_2 + R_3} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{R_1 \leftarrow R_1 - R_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \checkmark$$

La Id_m e la mat. nulla sono entrambe a scala ridotta

Pomo associare ad un sistema d. eq. lineari una matrice in cui il m. d. eq. = m. righe e m. inc. + 1 (termini noti) = n col.

Con il método di Gauss-Jordan è possibile ricavare le soluzioni di un sistema mettendo a scala ridotta la mat. associata al sistema

$$\begin{cases} x - 2y + z = 1 \\ 3x - 2y + z = 0 \\ 2x + 3y - 4z = 2 \end{cases} \quad A = \begin{pmatrix} 1 & -2 & 1 & 1 \\ 3 & -2 & 1 & 0 \\ 2 & 3 & -4 & 2 \end{pmatrix}$$

$$R_2 \rightarrow R_2 + 2R_1 \Rightarrow 3 + 2 \cdot 1 = 0 \Rightarrow 2 = -3$$

$$R_3 \rightarrow R_3 + 2R_1 \Rightarrow 2 + 2 \cdot 1 = 0 \Rightarrow 2 = -2$$

$$A = \begin{pmatrix} 1 & -2 & 1 & 1 \\ 0 & 4 & -2 & -3 \\ 0 & 7 & -6 & 0 \end{pmatrix} \quad 7 + 2 \cdot 4 = 0 \Rightarrow 2 = -7/4$$

$$A = \begin{pmatrix} 1 & -2 & 1 & 1 \\ 0 & 4 & -2 & -3 \\ 0 & 0 & -\frac{5}{2} & \frac{23}{4} \end{pmatrix} \xrightarrow{\begin{array}{l} R_2 \leftarrow \frac{1}{4}R_2 \\ R_3 \leftarrow -\frac{1}{2}R_3 \end{array}} \begin{pmatrix} 1 & -2 & 1 & 1 \\ 0 & 1 & -\frac{1}{2} & -\frac{3}{4} \\ 0 & 0 & 1 & -\frac{23}{10} \end{pmatrix} \xrightarrow{R_1 \rightarrow R_1 + 2R_2} \begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & -\frac{1}{2} & -\frac{3}{4} \\ 0 & 0 & 1 & -\frac{23}{10} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & -\frac{1}{2} & -\frac{3}{4} \\ 0 & 0 & 1 & -\frac{23}{10} \end{pmatrix} \xrightarrow{R_2 \rightarrow R_2 + \frac{1}{2}R_3} \begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & -\frac{9}{5} \\ 0 & 0 & 1 & -\frac{23}{10} \end{pmatrix}$$

Dunque la soluzione del sistema è:

$$\begin{cases} 1x + 0y + 0z = -1/2 \\ 0x + 2y + 0z = -2/5 \\ 0x + 0y + 1z = -21/20 \end{cases} \rightarrow \begin{cases} x = -1/2 \\ y = -1/5 \\ z = -21/20 \end{cases}$$

Il sistema ha una sola soluzione, dunque l'insieme S delle soluzioni è un singoletto.

→

$$\begin{cases} 2x - 3y + 5z = 3 \\ 6x - 2y + z = 2 \\ 2x + 4y - 9z = 2 \end{cases}$$

Dalla mat. completa si ottiene in pochi passaggi:

$$\left(\begin{array}{ccccc} 2 & -3 & 5 & 3 \\ 0 & 7 & -14 & -7 \\ 0 & 0 & 0 & 5 \end{array} \right) \xrightarrow{\begin{array}{l} \frac{1}{2}R_1 \\ 4R_2 \\ \frac{1}{5}R_3 \end{array}} \left(\begin{array}{ccccc} 1 & -3/2 & 5/2 & 3/2 \\ 0 & 1 & -2 & -1 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$0x + 0y + 0z = 1$ è impossibile

$S = \emptyset$, il sistema non è compatibile

→

$$\begin{cases} x + y - z + t = 1 \\ 2x - 4y + 3z + t = 4 \\ 3x - 3y + 2z + 2t = 5 \\ 4x - 2y + z + 3t = 6 \end{cases}$$

In breve si raggiunge una mat. con 2 righe nulle

$$\left(\begin{array}{ccccc} 1 & 1 & -1 & 1 & 1 \\ 0 & -6 & 5 & -1 & 2 \\ 0 & -6 & 5 & -1 & 2 \\ 0 & -6 & 5 & -1 & 2 \end{array} \right)$$

$$\left(\begin{array}{ccccc} 1 & 0 & -1/6 & 5/6 & 4/3 \\ 0 & 1 & -5/6 & 1/6 & -1/3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$\Leftrightarrow 0x - \frac{1}{6}z + \frac{5}{6}t = -\frac{1}{3}$

Avendo un numero di punti inferiore al numero di incognite, introduco il numero necessario di equazioni banali nel sistema in modo da risolvere per parametri.

$$\left\{ \begin{array}{l} x - \frac{1}{6}z + \frac{5}{6}\epsilon = \frac{4}{3} \\ y - \frac{5}{6}z + \frac{1}{6}\epsilon = -\frac{1}{3} \\ z = z \\ \epsilon = \epsilon \end{array} \right.$$

$$\begin{pmatrix} x \\ y \\ z \\ \epsilon \end{pmatrix} = \begin{pmatrix} 4/3 \\ -1/3 \\ 0 \\ 0 \end{pmatrix} + z \begin{pmatrix} 1/6 \\ 5/6 \\ 1 \\ 0 \end{pmatrix} + \epsilon \begin{pmatrix} -5/6 \\ -1/6 \\ 0 \\ 1 \end{pmatrix}$$

S è infinito e le soluzioni variano al variare di z e ϵ

Il **determinante** di una matrice è un numero associato a ciascuna matr. quadra, e ne esprime alcune proprietà:

2x2

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$$

3x3 Regola di Sarrus

$$\det \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} + \\ - (a_{13} \cdot a_{22} \cdot a_{31} + a_{11} \cdot a_{23} \cdot a_{32} + a_{12} \cdot a_{21} \cdot a_{33})$$

Per ricordarla, basta accostare alla matrice se stessa:

- calcolare la somma dei prodotti delle prime 3 diag complete,
- calcolare $= = = = =$ 3 diag antidiag,
- calcolare la differenza tra le 2.

[ES.]

$$A = \begin{pmatrix} 2 & -1 & 4 \\ 1 & 2 & 0 \\ 3 & 5 & 1 \end{pmatrix}$$

$$\begin{aligned} \det(A) &= (2 \cdot 2 \cdot 1) + (-1) \cdot 0 \cdot 3 + (4 \cdot 1 \cdot 5) - ((4 \cdot 2 \cdot 3) + (-1) \cdot 1 \cdot 1 + (2 \cdot 0 \cdot 5)) = \\ &= 4 + 20 - 24 + 1 = 1 \end{aligned}$$

Teorema di Laplace

Valido per mat. ch. qualsiasi ordine, usa formule ricorsive
(sviluppi d. Laplace) ~~appena~~ applicabile sia per righe che per
colonne. Data la mat. A , denotiamo con A_{ij} la mat.
ottenuta eliminando la riga i e la colonna j da A .

Fissato un qualunque $a_{ij} \in A$, chiamiamo **complemento
algebrico (cofattore)** di a_{ij} il numero: $(-1)^{i+j} \cdot \det(A_{ij})$

Sviluppo

$$\det(A) = \sum_{j=1}^m [a_{1j} \cdot (-1)^{1+j} \cdot \det(A_{1j})]$$

\Rightarrow muovendosi lungo la i -esima riga opp.
 $i=1 \quad \Rightarrow$ la j -esima colonna

[ES.]

$$A = \begin{pmatrix} 1 & 0 & 5 \\ 2 & -1 & 0 \\ 7 & -2 & 0 \end{pmatrix}$$

Per svolgere il minor numero possibile di calcoli applichiamo
Laplace alla 3^a colonna.

$$\begin{aligned} \det(A) &= a_{23} \cdot (-1)^{2+3} \cdot \det \begin{pmatrix} 2 & -1 \\ 7 & -2 \end{pmatrix} = \\ &= 5 \cdot 2 \cdot [(2 \cdot (-2)) - ((-1) \cdot 7)] = \cancel{\cancel{\cancel{\det(A)}}} 5 \cdot 3 = 15 \end{aligned}$$

Riassunto

- Determinante nullo se una riga / col. (o più) è nulla, se
due righe / col. sono proporzionali o se
una // i comunitaz. lineare di altre
- Nelle mat. triangolari è il prod. della dg. principale
- Teorema d. Binet: $\det(A \cdot B) = \det(A) \cdot \det(B)$
- $\det(A^T) = \det(A)$
- $\det(\lambda A) = \lambda^n \cdot \det(A)$

È possibile calcolare il determinante anche con il metodo d'eliminazione di Gauss*, ma con alcune precisazioni:

- scambiare due righe cambia segno al det.
- moltiplicare per $\lambda \neq 0$ una riga ha l'effetto di moltiplicare anche il det. per quello stesso λ
- sommare ad una riga il multiplo di un'altra non ha effetto (Stiamo infatti ottenendo una mat. tr. syn.)

[E.S.]

$$A = \begin{pmatrix} 0 & 7 & 3 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 1 & 0 & 4 \\ 0 & 7 & 3 \\ 0 & 1 & 2 \end{pmatrix} \quad R_3 \Rightarrow R_2 + (-7)R_3 = \begin{pmatrix} 0 & 0 & -11 \end{pmatrix}$$

$$A' = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 7 & 3 \\ 0 & 0 & -11 \end{pmatrix} \quad \det(A) = -77 \quad \det(A) = \frac{-\det(A')}{-7} = -11$$

Il rango di una matrice (quad o rett.) è un intero non negativo associato alla matrice dalle molteplici definizioni:

- massimo numero di righe / colonne linearmente indipendenti
- ordine massimo dei minori non nulli estratti da A
- dimensione del sottospazio vettoriale generato dalle righe / col.
- numero di pivot di della mat. a scala ridotta

Tramite elim. gaussiana possiamo trovare il range d'una matrice data l'ultima definizione.

Data una matrice qualsiasi A, si dicono sottomatrici di A tutte quelle matrici estratte da A eliminando da A un numero arbitrario di righe e/o colonne. Si definisce minore della matrice A il determinante di una sottomat. quad. di A; l'ordine della sottomat. è detto ordine del minore.

Teorema di Rouché-Capelli

$m = \text{num. linc.}$

Studia la compatibilità di un sistema lineare (se è risolvibile) tramite l'analisi del rango della matrice completa e incompleta.

- $\text{rk}(\text{inc. comp.}) < \text{rk}(\text{comp.}) \Rightarrow$ sistema impossibile
- $\text{rk}(\text{inc.}) = \text{rk}(\text{comp.}) = m \Rightarrow$ una e una sola soluzione
- $\text{rk}(\text{inc.}) = \text{rk}(\text{comp.}) < m \Rightarrow$ infinite soluzioni
che dipendono da $m - \text{rk}()$ param.

OSS.

In ogni campo finito, il numero di soluzioni di un sistema è pari a m^{R-n} dove $m = \text{num. elem. del campo}$, $n = m^{\circ}$ incognite e $R = \text{rango della matrice associata}$

ES.

$$\begin{cases} x + y + 2z = 5 \\ 3x - 2y + z = 0 \\ 7x - 3y + 4z = 6 \end{cases}$$

Det. della mat. incompleta con la regola di Sarrus:

$$\det(A) = \det \begin{pmatrix} 1 & 1 & 2 \\ 3 & -2 & 1 \\ 7 & -3 & 4 \end{pmatrix} = (-8 + 7 - 18) - (-28 + 12 - 3) = -29 + 29 = 0$$

dunque il rango di A è minore di 3; la matrice

$$\begin{pmatrix} 1 & 1 & 2 \\ 3 & -2 & 1 \\ 7 & -3 & 4 \end{pmatrix} \text{ ha } \det = -2 - 3 = -5, \text{ dunque } \text{rk}(A) = 2$$

$$\begin{pmatrix} 1 & 1 & 2 & 5 \\ 3 & -2 & 1 & 0 \\ 7 & -3 & 4 & 6 \end{pmatrix} \xrightarrow{\begin{array}{l} R_2 \rightarrow R_2 - 3R_1 \\ R_3 \rightarrow R_3 - 7R_1 \end{array}} \begin{pmatrix} 1 & 1 & 2 & 5 \\ 0 & -5 & -5 & -15 \\ 0 & 10 & 10 & 21 \end{pmatrix} \xrightarrow{R_3 \rightarrow R_3 - 2R_2} \begin{pmatrix} 1 & 1 & 2 & 5 \\ 0 & -5 & -5 & -15 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{R_2 \Rightarrow R_2 + \frac{1}{5}R_3} \begin{pmatrix} 1 & 1 & 2 & 5 \\ 0 & 1 & 1 & 15 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{\begin{array}{l} R_2 \rightarrow R_2 - 15R_3 \\ R_1 \rightarrow R_1 - 5R_3 \end{array}} \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{R_1 \rightarrow R_1 - R_2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ che è a scala ridotta e d. rango 3}$$

Poiché il rango dell'incompleta è minore di quello della comp.
il sistema non ammette soluzioni

(E.S.)

$$\begin{cases} 3x + 2ky + z = l \\ kx + y + 2z = 0 \quad \text{con } k \in \mathbb{R} \\ -x + y + 2z = 2 \end{cases}$$

$$\det(A) = \det \begin{pmatrix} 3 & 2k & 1 \\ k & 1 & 2 \\ -1 & 1 & 2 \end{pmatrix} = (6 - 4k + k) - (-1 + 4k^2 + 6) = -4k^2 - 3k + 1$$

Se $\det(A) \neq 0$ allora $\text{rk}(A) = 3 = \text{rk}(B)$ = num. inc.

e quindi il sistema ha una e una sola soluz.

$$-4k^2 - 3k + 1 = 0 \Rightarrow \begin{cases} k = -1 \\ k = \frac{1}{4} \end{cases} \quad \text{vediamo cosa succede al sistema con questi valori di } k$$

$$\begin{cases} 3x - 2y + z = l \\ -x + y + 2z = 0 \\ -x + y + 2z = 2 \end{cases}$$

La mat. A ha sicuramente $\det. = 0$ per quanto detto \rightarrow

$$\Rightarrow \det \begin{pmatrix} 3 & -2 \\ -1 & 0 \end{pmatrix} = 3 + 2 = 5 \quad \text{dunque } \text{rk}(A) = 2$$

Eliminando la prima col. dalla mat. completa, calcoliamo il ~~det.~~ della mat. quad. di ordine 3 ottenuta con Sarrus:

$$\det * \begin{pmatrix} -2 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 2 & 2 \end{pmatrix} = (-8 + 0 + 2) - (2 + 2 + 0) = -6 - 4 = -10 \Rightarrow \text{rk} = 3$$

Da ciò ricaviamo che per $k = -1$ il sistema è impossibile; tramite altri calcoli si può dire lo stesso per $k = \frac{1}{4}$

In conclusione

per $k \in \mathbb{R} - \{-1, \frac{1}{4}\}$ il sistema ammette un'unica soluzione;

mentre per $k = -1$ e $k = \frac{1}{4}$ il sistema è impossibile

SPAZI VETTORIALI

Uno spazio vettoriale è una struttura algebrica definita a partire da un insieme di vettori, un campo di scalari e due operazioni binarie.

Un generico campo K , che in genere coincide con \mathbb{C} o \mathbb{R} , è detto **Campo di scalari**.

La prima operazione è interna ed è la somma di vettori:

$$+ : V \times V \rightarrow V$$

$$(v, w) \mapsto v + w$$

La seconda è esterna ed è il prodotto di un vettore per uno ^{scalar} scalare

$$\circ : K \times V \rightarrow V$$

$$(\lambda, v) \mapsto \lambda \cdot v$$

$(V, +, \circ)$ è spazio vettoriale su K se sono valide le seguenti proprietà:

$$\forall u, v, w \in V \quad \forall \lambda, \beta \in K$$

• $(V, +)$ è un gruppo abeliano

• $+$ è associativa $(u + v) + w = u + (v + w)$

• \exists el. neutro rispetto a $+$ $v + 0_v = v = 0_v + v$

• $\forall v \in V \exists w \in V : v + w = 0_v = w + v$ ogni elem. ha inverso rispetto a $+$

• $+$ è commutativo $v + w = w + v$

• • è pseudo-associativa $\lambda \cdot (\beta \cdot v) = (\lambda \beta) \cdot v$

• \exists neutro rispetto a \circ . $1 \cdot v = v$

• distributivo rispetto a ~~somma~~ somma d' vett. $\lambda \cdot (v + w) = \lambda v + \lambda w$

• distrib. rispetto a somma tra scalari $(\lambda + \beta) v = \lambda v + \beta v$

E.S.

$$\mathbb{R}^m := \{(x_1, x_2, \dots, x_m) : x_i \in \mathbb{R} \quad \forall i \in \{1, 2, \dots, m\}\}$$

gli elem. sono le m -uple ordinate di numeri reali

$$+ : \mathbb{R}^m \times \mathbb{R}^m \rightarrow \mathbb{R}^m$$

$$x = (x_1, x_2, \dots, x_m) \quad x + y = (x_1 + y_1, x_2 + y_2, \dots, x_m + y_m)$$

$$\circ : \mathbb{R} \times \mathbb{R}^m \rightarrow \mathbb{R}^m$$

$$\lambda \in \mathbb{R} \quad \lambda \cdot x = (\lambda x_1, \lambda x_2, \dots, \lambda x_m)$$

$$\lambda \cdot x = (\lambda x_1, \lambda x_2, \dots, \lambda x_m)$$

E.S.

Spazio vettoriale dei polinomi di grado al più n a coeff reale

$$\mathbb{R}_n[x] := \{a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + a_n x^n \mid a_i \in \mathbb{R} \quad \forall i \in \{0, 1, \dots, n\}\}$$

diverenti spazio vett. se definiamo

$$\text{la somma } p(x) + q(x) =$$

$$= (a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + a_n x^n) + (b_0 + b_1 x + \dots + b_{n-1} x^{n-1} + b_n x^n) =$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_{n-1} + b_{n-1})x^{n-1} + (a_n + b_n)x^n$$

$$\text{e il prodotto } \lambda \cdot p(x) =$$

$$= \lambda a_0 + \lambda a_1 x + \dots + \lambda a_{n-1} x^{n-1} + \lambda a_n x^n$$

Un sottospazio vettoriale S è un sottoinsieme di uno spazio vettoriale V tale da essere a sua volta uno spazio vettoriale rispetto alle operazioni definite in V .

Preso quindi un $S \subseteq V$ con $S \neq \emptyset$, bisogna dimostrare che valgono tutte le proprietà descritte.

(S è parte stabile rispetto a somma e prodotto)

Teorema di caratterizzazione: si tratta di dimostrare tutte le proprietà e ci limita a verificare chi:

$$\forall s_1, s_2 \in S \Rightarrow s_1 + s_2 \in S$$

$$\forall s \in S \quad \forall \lambda \in K \Rightarrow \lambda s \in S$$

E5/

Sia W l'insieme delle matrici 2×2 sul campo razionale aventi traccia (somma degli elem. della diag. princ.) nulla

Dim. che W è sottosp. vett. dello spazio delle mat. 2×2 su \mathbb{Q}

So che $W \neq \emptyset$ perché posso sicuramente costruire una matrice, la cui forma generica è $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} + \begin{pmatrix} d & e \\ f & -d \end{pmatrix} = \begin{pmatrix} a+d & b+e \\ c+f & -a-d \end{pmatrix} = \begin{pmatrix} a+d & b+e \\ c+f & -(a+d) \end{pmatrix}$$

e ancora una volta si ha traccia nulla \Rightarrow

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \cdot \lambda \in K = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & -\lambda a \end{pmatrix} \in W \quad \Leftrightarrow$$

OSS.

L'elemento neutro di V rispetto alla somma deve appartenere ad S e tale condizione è necessaria per la verifica: Ora $\in S$ consente di procedere, mentre se $0 \notin S$ si può immediatamente concludere

Una combinazione lineare è un'espressione in cui compaiono somme di vettori e moltiplicazioni di vettori per scalari

(vett. = elem. di un qualsiasi spazio vett., ~~per~~ dunque anche polinomio mat.)

Sia V spazio vett. su K e prendiamo m vettori v_1, \dots, v_m :

definiamo comb. lineare di questi vettori: qualsiasi espressione nella forma $a_1 v_1 + a_2 v_2 + \dots + a_m v_m$ dove a_1, a_2, \dots, a_m sono m scalari qualsiasi appartenenti a K . È scritta anche come

$$\sum_{i=1}^m a_i v_i$$

Prende tale nome perché definita solamente da operazioni lineari

Indipendentemente dal num. di vett. e dagli scalari, il risultato $\in V$

CS.

$$v_1(1,0), v_2(18,-5) \text{ in } \mathbb{R}^2 \quad a_1 = 4, a_2 = -7$$

$$a_1 v_1 + a_2 v_2 =$$

$$= 4(1,0) + (-7)(18,-5) =$$

$$= (4,0) + (-126, 35) = (-122, 35) \in \mathbb{R}^2$$

$$p_1(x) = 2+3x^2 \quad p_2(x) = -3-x \text{ in } \mathbb{R}_2[x] \quad a_1 = 1, a_2 = -1$$

$$a_1 p_1(x) + a_2 p_2(x) =$$

$$= 2(2+3x^2) + (-1)(-3-x) =$$

$$= 2+3x^2+3+x = 5+x+3x^2 \in \mathbb{R}_2[x]$$

Un insieme di vettori di uno sp. vett. è formato da vettori linearmente indipendenti se nessuno di essi può essere espresso come combinazione lineare degli altri vettori.

Consideriamo $v_1, v_2, \dots, v_m \in V$ spazio vett. su K : Gli n vettori sono indip. se $a_1 v_1 + a_2 v_2 + \dots + a_m v_m = 0$ risulta evidentemente se e solo se $a_1 = a_2 = \dots = a_m = 0$ cioè se è solo se l'unica m -upla che annulla la combinazione lineare è la m -upla di coeff. nulli.

Se esiste almeno un'altra m -upla in grado di annullarla allora i vettori sono linearmente dipendenti.

CS.

$$v_1(1,0), v_2(0,1) \in \mathbb{R}^2 \quad a, b \in \mathbb{R}$$

$$a v_1 + b v_2 \Rightarrow a(1,0) + b(0,1)$$

$$(a,0) + (0,b) = (0,0)$$

$$(a,b) = (0,0)$$

Vera se e solo se $a=b=0 \Rightarrow$ v. lin. indip.

$$v_1(1,1,0), v_2(0,0,2), v_3(0,0,-3) \in \mathbb{R} \quad a, b, c \in \mathbb{R}$$

$$av_1 + bv_2 + cv_3 = 0$$

$$(a, a, 0) + (0, 0, 2b) + (0, 0, -3c) = (0, 0, 0)$$

$$(a, a, 2b - 3c) = (0, 0, 0)$$

Soddisfatta per $a = b = c = 0$ ma anche $a = 0, 2b = 3c$

dunque v_1, v_2 e v_3 sono lin. dipendenti

OSS.

- Se tra i vettori v_1, v_2, \dots, v_m di uno sp. vett. V c'è il vettore nullo, allora gli m vettori sono lin. dipendenti

- Se tra i vettori v_1, v_2, \dots, v_m di uno sp. vett. V ci sono $K < m$ vett. lin. dipendenti, allora sono tutti lin. dip.

Un sistema o insieme di generatori di uno spazio o sottospazio vettoriale è un insieme di vettori con cui è possibile ricostruire, tramite comb. lin., tutti i vett. dello spazio $\{v_1, v_2, \dots, v_m\} \subseteq V$ è sistema di gen. se e solo se $\forall w \in V$

\exists scalari $a_1, a_2, \dots, a_m \in K$ t.c.:

$$a_1 v_1 + a_2 v_2 + \dots + a_m v_m = \sum_{i=1}^m a_i v_i = w$$

(ES.)

$$M_{2 \times 2}(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ con } a, b, c, d \in \mathbb{R} \right\}$$

l'insieme $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ è insieme di gen.

OSS. Per ogni sp. vett. $V \neq \{0\}$ esistono infiniti sist. di gen.

Per stabilire se un insieme di vett. è generatore basta

svolgere i calcoli dell'eq. $a_1 v_1 + \dots + a_m v_m = w$ in

modo da avere un'ugaglianza tra vettori. A quel punto

ci associamo un sistema lineare e ne verifichiamo la

compatibilità con R.C.

[ES]

$$\{(1,0,1), (0,0,3), (1,2,1), (1, -1, 0)\} \text{ per } \mathbb{R}^3$$

Possi $a, b, c, d \in \mathbb{R}$, deve valere:

$$a(1,0,1) + b(0,0,3) + c(1,2,1) + d(1,-1,0) = w$$

$$(a,0,a) + (0,0,3b) + (c,2c,c) + (d,-d,0) = (w_1, w_2, w_3)$$

$$\begin{cases} a+0+c+d = w_1 \\ 0+0+2c-d = w_2 \\ a+3b+c+0 = w_3 \end{cases}$$

Applichiamo l'eliminazione gaussiana alla mat. completa A:

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & w_1 \\ 0 & 0 & 2 & -1 & w_2 \\ 1 & 3 & 1 & 0 & w_3 \end{array} \right) \xrightarrow{\downarrow} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & w_1 \\ 0 & 0 & 2 & -1 & w_2 \\ 0 & 3 & 0 & -1 & w_3 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & w_1 \\ 0 & 0 & 2 & -1 & w_2 \\ 0 & 0 & 2 & -1 & w_3 \end{array} \right)$$

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & w_1 \\ 0 & 0 & 2 & -1 & w_2 \\ 0 & 0 & 0 & -1 & w_3 - w_1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & w_1 \\ 0 & 0 & 3 & 0 & w_2 - w_1 \\ 0 & 0 & 2 & -1 & w_3 \end{array} \right) \quad \text{a mat. ridotta}$$

i cui pivot sono 1, 3 e 2 e di rango 3 come la
(perché non ci sono pivot nella colonna dei term. not.)

dunque i valori assegnati costituiscono un sistema di generatori
di \mathbb{R}^3

Si dice base di uno spazio vettoriale un insieme di vettori
grazie ai quali possiamo ricostruire in modo unico tutti i vettori
dello spazio mediante comb. lineare.

Dato uno spazio vettoriale V su un campo K , diciamo che
un insieme di vettori $\{v_1, v_2, \dots, v_n\} \subseteq V$ è una base di V se:

a) $\{v_1, v_2, \dots, v_n\}$ è un sistema di generatori di V

b) v_1, v_2, \dots, v_n sono vettori lin. indip.

Permutando l'ordine dei vettori si ottengono nuove basi diverse
tra loro, dunque ogni base va vista come insieme ordinato

[CS.1] 8 pt

Sia $5\mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$ la relazione definita da $a 5\mathbb{Z} b \Leftrightarrow 5 \mid (a-b)$

Dim. che $5\mathbb{Z}$ è rel. eq. ; descrivere la classe d. eq. d. 0 e l'insieme quoziente $\mathbb{Z}/5\mathbb{Z}$

$a 5\mathbb{Z} b \Leftrightarrow 5 \mid (a-b) \Leftrightarrow \exists k \in \mathbb{Z} : a-b = 5k$

(i) $\forall a \in \mathbb{Z}, 5 \mid (a-a) ?$

$$5 \mid 0 \text{ è vero } \Rightarrow 0 = 5 \cdot 0$$

(ii) $\forall a, b \in \mathbb{Z} : 5 \mid (a-b) \Rightarrow 5 \mid (b-a)$

$$\text{per ip. } 5 \mid (a-b) \Rightarrow \exists k \text{ t.c. } a-b = 5k \Rightarrow$$

$$\Rightarrow \exists k : -(a-b) = -5k \Rightarrow \exists k : b-a = 5(-k)$$

(iii) $\forall a, b, c \in \mathbb{Z} : 5 \mid (a-b) \& 5 \mid (b-c) \Rightarrow 5 \mid (a-c)$

$$\text{per ip. } \exists k : (a-b) = 5k, \exists h : (b-c) = 5h$$

$$a-c = (a-b)+(b-c) = 5k+5h = 5(k+h) \Rightarrow 5 \mid (a-c)$$

$$[0]_5 = \{x \in \mathbb{Z} \mid x \in 5\mathbb{Z}\} = \{x \in \mathbb{Z} \mid 5 \mid x\} = \{x \in \mathbb{Z} \mid 5 \mid x\}$$

$$\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

[CS.2] 7 pt

$$\begin{cases} x \equiv 6 \pmod{9} \\ x \equiv 2 \pmod{11} \end{cases} \quad \text{mcd}(9, 11) = 1 \rightarrow \text{esiste unica soluzione}$$

$$x = 6 + 9k, \quad k \in \mathbb{Z}$$

$$6 + 9k \equiv 2 \pmod{11} \Rightarrow 9k \equiv -4 \pmod{11} \quad (\text{non serve rendere mai})$$

$$\text{mcd}(9, 11) = 1$$

$$11 = 9 \cdot 1 + 2 \quad 1 = 9 + (-4) \cdot 2 = 9 + (-4)(11 - 9) =$$

$$9 = 2 \cdot 4 + 1 \quad = 9 + (-4) \cdot 11 + 4 \cdot 9 = (-4)11 + 5 \cdot 9$$

$$2 = 1 \cdot 2 + 0$$

$$\text{dove } k = -4 \cdot 5 = -20 \Rightarrow k \equiv -20 \pmod{11} \Rightarrow k \equiv 2 \pmod{11}$$

$$x = 6 + 2 \cdot 9 = 24$$

$$S = [24]_{9, 11} = [24]_9,$$

ES 3 7pt

Dim. che $M_2(\mathbb{R})$ è un insieme delle mat. quad. 2×2 su \mathbb{R} , un gruppo abeliano rispetto alla somma tra matrici.

La somma tra matrici è così definita:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \quad A + B = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

- Trovando nei \mathbb{R} , definire le proprietà commutativa e associativa è banale
- L'elem. neutro è la mat. nulla $N = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, la quale appartiene all'insieme
- $\forall C \in M_2(\mathbb{R})$, $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, la mat. $-C = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ è il suo simmetrica

ES. 4 8pt

$$\begin{cases} x - 3y + z = 0 \\ x + 2y = -1 \\ x - 3z = 2 \end{cases}$$

$$\begin{pmatrix} 1 & -3 & 1 & 0 \\ 1 & 2 & 0 & -1 \\ 1 & 0 & -3 & 2 \end{pmatrix} \xrightarrow{\text{R1} \rightarrow R1 - R2} \begin{pmatrix} 1 & -3 & 1 & 0 \\ 0 & 5 & -1 & -1 \\ 1 & 0 & -3 & 2 \end{pmatrix} \xrightarrow{\text{R2} \rightarrow R2 - \frac{1}{5}R2} \begin{pmatrix} 1 & -3 & 1 & 0 \\ 0 & 5 & -1 & -1 \\ 0 & 0 & -\frac{2}{5} & \frac{7}{5} \end{pmatrix} \xrightarrow{\text{R3} \rightarrow R3 - \frac{1}{5}R2} \begin{pmatrix} 1 & -3 & 1 & 0 \\ 0 & 5 & -1 & -1 \\ 0 & 0 & 0 & \frac{1}{5} \end{pmatrix}$$

$$\begin{pmatrix} 1 & -3 & 1 & 0 \\ 0 & 1 & -\frac{1}{5} & \frac{1}{5} \\ 0 & 0 & 1 & -\frac{7}{25} \end{pmatrix} \xrightarrow{\text{R1} \rightarrow R1 - R2} \begin{pmatrix} 1 & 0 & \frac{2}{5} & \frac{3}{5} \\ 0 & 1 & -\frac{1}{5} & \frac{1}{5} \\ 0 & 0 & 1 & -\frac{7}{25} \end{pmatrix} \xrightarrow{\text{R1} \rightarrow R1 - \frac{2}{5}R3} \begin{pmatrix} 1 & 0 & 0 & -\frac{11}{25} \\ 0 & 1 & 0 & -\frac{6}{25} \\ 0 & 0 & 1 & -\frac{7}{25} \end{pmatrix}$$

$$\xrightarrow{\text{R1} \rightarrow R1 - \frac{2}{3}R2} \begin{pmatrix} 1 & -3 & 1 & 0 \\ 0 & 5 & -1 & -1 \\ 0 & 0 & -\frac{17}{5} & \frac{13}{5} \end{pmatrix} \xrightarrow{\text{R1} \rightarrow R1 - R3} \begin{pmatrix} 1 & -3 & 1 & 0 \\ 0 & 1 & -\frac{1}{5} & -\frac{1}{5} \\ 0 & 0 & 1 & -\frac{13}{25} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 215 & -3/5 \\ 0 & 1 & -1/5 & -2/5 \\ 0 & 0 & 1 & -13/17 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & -5/17 \\ 0 & 1 & 0 & -6/17 \\ 0 & 0 & 1 & -13/17 \end{pmatrix}$$

Dunque le soluzioni sono

$$\begin{cases} x = -5/17 \\ y = -6/17 \\ z = -13/17 \end{cases}$$

ESAME 30/06/22 → appello estivo

ES. 1 8 pt

Dati $A, B \subseteq X$ con $X \neq \emptyset$, dim. che

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$$

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

$$\Leftrightarrow x \in (X \setminus A) \text{ e } x \in (X \setminus B) \Leftrightarrow x \in (X \setminus A) \cap (X \setminus B) \quad \diamond$$

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$$

$$x \in X \setminus (A \cap B) \Leftrightarrow x \in X \text{ e } x \notin (A \cap B) \Leftrightarrow x \in X \text{ e } (x \notin A \text{ o } x \notin B)$$

$$\Leftrightarrow x \in (X \setminus A) \text{ o } x \in (X \setminus B) \Leftrightarrow x \in (X \setminus A) \cup (X \setminus B)$$

ES. 2 7 pt

$\text{rest}(a, 19) = 16$ e $\text{rest}(a, 20) = 17$, dese. gli interi a

e determina quello compreso tra 1000 e 1500

$$\begin{cases} a \equiv 16 \pmod{19} \\ \text{mcd}(19, 20) = 1 \end{cases}$$

$$\begin{cases} a \equiv 17 \pmod{20} \end{cases}$$

$$a = 16 + 19k \rightarrow 16 + 19k \equiv 17 \pmod{20} \rightarrow 19k \equiv 1 \pmod{20}$$

$$\text{mcd}(19, 20) = 1$$

$$20 = 19 \cdot 1 + 1 \rightarrow 1 = 20 - 19 \cdot 1$$

$$k = -1 \rightarrow a = 16 - 19 = -3$$

$$S = [E3]_{19 \cdot 20} = [377]_{380}$$

la cercata è 1737

ES. 3 7 pt

$$N = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 3 \right\}, \text{ dim. che } N \text{ non è sottogruppo di}$$

$(GL_2(\mathbb{R}), \cdot)$, gruppo moltiplicativo delle mat. invertibili

Ricordiamo che una mat. è invertibile quando il suo determinante è diverso da zero.

Possiamo dimostrarlo in più modi:

- el. neutro di $GL_2(\mathbb{R})$ è $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ il cui det è 1,

dunque non appartiene ad N .

- Proviamo ad usare il teorema di Binet:

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

$$\text{Se } A, B \in N, \det(A \cdot B) = 3 \cdot 3 = 9 \Rightarrow A \cdot B \notin N$$

- Possiamo scegliere due mat. qualsiasi e vedere come il loro prodotto non appartenga ad N :

$$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix} \quad \det \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix} = 9$$

ES. 4 8 pt

Dim. che il prod di due mat. $m \times n$ tr. sup i tr. sup.

$$A \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & & & \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} \quad B \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ 0 & b_{22} & \dots & b_{2m} \\ \vdots & & & \\ 0 & \dots & 0 & b_{nn} \end{pmatrix}$$

a_{ik}

b_{kj}

$$c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \dots + a_{im} b_{mj}$$

Sia $j > i$ allora analizzando le due mat. e l'espressione:
(def. di mat. tr. sup. and.)

\exists $j \geq i$, si ha $a_{ij} \neq 0$

$j < i$, si ha $a_{ij} = 0$

dunque $a_{i1}, a_{i2}, \dots, a_{i,i-1} = 0$

e $b_{j+1,j}, b_{j+2,j}, \dots, b_{m,j} = 0$

In conclusione, gli elementi che componevano i prodotti $a_{ik} \cdot b_{kj}$ sono tutti nulli quando $i > j$, quindi

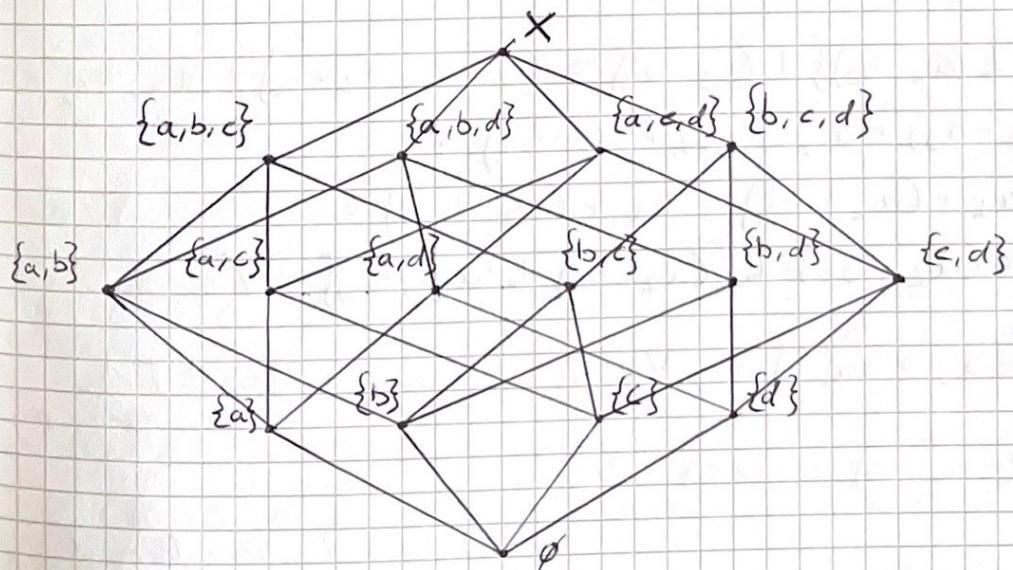
$c_{ij} = 0$ e la matrice C è triangolare superiore

ESAME 22-07-2022 II appello estivo

[ES.1] 7 pt

$X = \{a, b, c, d\}$; dato $P(X)$ insieme delle parti di X , disegnare il diagramma di Hasse di $(P(X), \subseteq)$

$$P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, X\}$$



ES. 2 8 nt

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 3 \pmod{7} \\ x \equiv 2 \pmod{3} \end{cases} \quad \text{mcd}(2, 7, 3) = 1$$

$$x = 2k + l \rightarrow 2k + 1 \equiv 3 \pmod{7} \rightarrow k \equiv 1 \pmod{3}$$

$$x = 2k + 1 = 3 \rightarrow S_2 = [3]_{14} = 3 + 14t$$

$$14t + 3 \equiv 2 \pmod{3} \rightarrow 14t \equiv -1 \pmod{3} \rightarrow t \equiv 1 \pmod{3}$$

$$S = [3 + 14 \cdot 1]_{14 \cdot 3} = [17]_{42}$$

ES. 3 7 nt

$(\mathbb{Z}, +, 0)$ gruppo degli interi. Sotiamo il prod. cartesiano $\mathbb{Z} \times \mathbb{Z}$ della seguente op., $\forall (a_1, b_1), (a_2, b_2) \in \mathbb{Z} \times \mathbb{Z}$

$$(a_1, b_1) \perp (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

Dim. che $\mathbb{Z} \times \mathbb{Z}$ è un gruppo abeliano

Serve dim. che \perp sia comm. chi ass. e che c'è uno neutro ed è

$$\begin{aligned} (a_1, b_1) \perp (a_2, b_2) &= (a_1 + a_2, b_1 + b_2) = (a_2 + a_1, b_2 + b_1) = \\ &= (a_2, b_2) \perp (a_1, b_1) \quad \checkmark \end{aligned}$$

$$\begin{aligned} [(a_1, b_1) \perp (a_2, b_2)] \perp (a_3, b_3) &= (a_1 + a_2, b_1 + b_2) \perp (a_3, b_3) = \\ &= ((a_1 + a_2) + a_3, (b_1 + b_2) + b_3) = \\ &= (a_1 + (a_2 + a_3), b_1 + (b_2 + b_3)) = \\ &= (a_1, b_1) \perp [(a_2, b_2) \perp (a_3, b_3)] \quad \checkmark \end{aligned}$$

$$(a, b) \perp (0, 0) = (a, b), \quad \forall (a, b) \quad \text{dunque } (0, 0) \text{ è l'elemento neutro} \quad \checkmark$$

$$(a, b) \perp (-a, -b) = (0, 0), \quad \forall a, b \quad \text{dunque}$$

$(-a, -b)$ è il simmetrico di (a, b)

ES4 8 pt

$$M = \begin{pmatrix} [0] & [-2] & [1] & [0] \\ [0] & [1] & [4] & [1] \\ [1] & [0] & [2] & [3] \\ [0] & [1] & [-1] & [0] \end{pmatrix}$$

stabilisce se è invertibile in \mathbb{Z}_5 e determina il rango.

Calcoliamo il det. osservando la prima colonna

$$\det(M) = (-1)^{2+3} \cdot [1] \cdot \det \begin{pmatrix} 2 & 1 & 3 \\ 1 & 4 & 2 \\ 1 & 1 & 0 \end{pmatrix} =$$

poiché
ha un
solo
val $\neq 0$

$$\begin{aligned} &= [-2] \cdot (([0] + [-2] + [3]) - ([-2] + [0] + [2])) = \\ &= [-2] \cdot ([4] - [2]) = [-10] = [0] \text{ dunque} \end{aligned}$$

M non è invertibile

Prendiamo una sottomat. e calcoliamo il det:

$$\det(N) = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 4 \\ 1 & 0 & 2 \end{pmatrix} = -[0] + [8] + [0] - [-2] - [0] - [0] = [7] = [2]$$

poiché il rango di N è $\neq 0$, il rango di M è 3

ES4 22-02-2022 II appello

ES1 9 pt

Dato \mathbb{Z} insieme dei numeri interi, $\forall c \in \mathbb{Z}$ sia $f_c : \mathbb{Z} \rightarrow \mathbb{Z}$

l'applicazione definita da $f_c(x) := x - cx + c$, $\forall x \in \mathbb{Z}$

Determ. per qual val di c f_c è iniett., suratt. e/o biett.

- Per $c=0$ si ha $f_c(x) = x$ che è la funzione identità e dunque f_c è biettiva
- Per $c=1$ si ha $f_c(x) = 1$ e la funzione è costante (dunque né iniettiva né suriettiva)

• Nel caso di $c \neq 1$

$$f_c(x_1) = f_c(x_2) \Leftrightarrow x_1 - cx_1 + c = x_2 - cx_2 + c \Leftrightarrow \\ \Leftrightarrow x_1(1-c) = x_2(1-c) \Leftrightarrow x_1 = x_2$$

dunque f_c è iniettiva per ogni $c \neq 1$

• f_c è suriettiva se $\forall z \in \mathbb{Z} \exists x \in \mathbb{Z} : z = x - cx + c$

$$\text{da cui si ricava } x = \frac{z-c}{1-c}; \text{ ad ogni val. di } z$$

dovrà dunque corrispondere un valore intero

• nel caso di $c=2$ si ha $1-2 = -1$ e questo è sempre vero

• nel caso di $c \neq 2$ a affergiamo subito che $z=0$ non app. all'immagine di f_c , in quanto si avrebbe per assurdo $\frac{-c}{1-c} = \frac{c}{c-1} \in \mathbb{Z}$

[ES. 2] 8 pt

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 3 \pmod{7} \\ x \equiv 6 \pmod{11} \end{cases} \quad \text{mcd}(2, 7, 11) = 1$$

$$x = 2k \rightarrow 2k \equiv 3 \pmod{7}$$

$$\text{mcd}(2, 7) = 1$$

$$7 = 2 \cdot 3 + 1 \rightarrow 1 = 1 \cdot 7 + (-3) \cdot 2$$

$$K = -3 \cdot 3 = -9 \rightarrow K \equiv -9 \pmod{7} \rightarrow k \equiv 5 \pmod{7}$$

$$x = 2 \cdot 5 + 10 \rightarrow S_1 = [10]_{11} \rightarrow x = 10 + 1 \cdot 5$$

$$10 + 1 \cdot 5 \equiv 6 \pmod{11} \Rightarrow 1 \cdot 5 \equiv -4 \pmod{11} \Rightarrow 3 \cdot 5 \equiv 7 \pmod{11}$$

$$\text{mcd}(3, 11) = 1$$

$$11 = 3 \cdot 3 + 2$$

$$1 = 3 + (-1) \cdot 2 = 3 + (-1)(11 + (-3) \cdot 3) =$$

$$3 = 2 \cdot 1 + 1$$

$$= \cancel{(-1)} \cdot \cancel{(11)} + (-1) \cdot 3 + (-1) \cdot 11$$

$$J = 7 \cdot 4 = 28 \rightarrow S = [10 + 1 \cdot 28]_{11 \cdot 11} = [402]_{121} = [24]_{121}$$

[ES.3] 8 pt

Dim che $M = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}$ è sottogr. abeliano del gruppo moltiplicativo $(GL_2(\mathbb{R}), \cdot)$ delle mat. invert. 2×2 a coeff. reali

Notiamo subito che il det. di una matrice qualunque $\in M$ vale $1 \cdot 1 = 1 \neq 0$, dunque ogni mat. di M è invertibile e

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$$

Dette le mat. A e B :

$$A = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \quad \text{si ha } AB = \begin{pmatrix} 1 & 0 \\ a+b & 1 \end{pmatrix} \in M$$

dunque M è chiuso per prodotto

[ES.4] 5 pt

Calcolare il rango di $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 4 & 6 & 8 \end{pmatrix}$

$$\det(A) = 32 + 40 + 54 - 48 - 48 - 30 = 0$$

$$\det \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 4 - 6 = -2 \neq 0 \quad \text{dunque il rango è 2}$$

~~Calcolo dei minori~~

[ES.1] 9 pt

~~Dim che $\forall m \geq 8 \exists a, b \in \mathbb{N}_0 : m = 5a + 3b$~~

~~Sugg. $8 \leq m \leq 15$ si può verificare caso per caso, mentre per $m \geq 16$ si usa l'ipotesi di induzione~~

ESAME 21-03-22

Appello straordinario

Q3.1 (8 pt)

$X = \{1, 2, 3, \dots, 7, 8\}$ e $Y = \{a, b, c\}$; sia $f: X \rightarrow Y$ definita da

$$f(1) = a, f(2) = a, f(3) = c, f(4) = b, f(5) = a$$

$$f(6) = b, f(7) = c, f(8) = a$$

1) Scrivere $f^{-1}(\{a\})$, $f^{-1}(\{b\})$, $f^{-1}(\{c\})$

$$f^{-1}(\{a\}) = \{1, 2, 5, 8\}$$

$$f^{-1}(\{b\}) = \{4, 6\}$$

$$f^{-1}(\{c\}) = \{3, 7\}$$

Formare una partizione di X ?

$A \cap B = A \cap C = B \cap C = \emptyset$ e $A \cup B \cup C = X$, quindi si

2) Sia $\sim \subseteq X \times X$ la relazione

$$x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$$

dim. che è di equivalenza

$$x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2) \text{ sempre vero}$$

$$x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2) \Leftrightarrow f(x_2) = f(x_1) \Leftrightarrow x_2 \sim x_1$$

$$x_1 \sim x_2 \wedge x_2 \sim x_3, \text{ allora } f(x_1) = f(x_2) \wedge f(x_2) = f(x_3)$$

$$\text{da cui } f(x_1) = f(x_3) \text{ e quindi } x_1 \sim x_3$$

3) Scrivere le classi di eq. di X e l'insieme quan. X/\sim

$$[1]_\sim = [2]_\sim = [5]_\sim = [8]_\sim$$

$$[4]_\sim = [6]_\sim$$

$$[3]_\sim = [7]_\sim$$

$$X/\sim = \{[1]_\sim, [4]_\sim, [3]_\sim\}$$

ES. 2 (7 pt)

Estraendo da un cesto le palline a 2a2, questo rimane vuoto,
a 5a5 ne restano 4 e a 3a3 ne restano 2. Numero min d.
palline?

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{3} \end{cases} \quad \text{mcd}(2, 5, 3) = 1$$

$$x = 2k \rightarrow 2k \equiv 4 \pmod{5} \Rightarrow k \equiv 2 \pmod{5}$$

$$S_1 = [2 \cdot 2]_{2 \cdot 5} = [k]_{20} \Rightarrow t = 4 + 10j$$

$$4 + 10j \equiv 2 \pmod{3} \Rightarrow 10j \equiv -2 \pmod{3} \Rightarrow 10j \equiv 1 \pmod{3}$$

Qui è semplice
verificare d'
"forma bruta"
che la sol. è
 \downarrow
 $j = 2$

Num. pari che
chitano 5 da
resto 4

$$S = [k+10j]_{10 \cdot 3} = [k+2]_{30} \text{ dunque il numero minimo di palline è } 2k$$

ES. 3 (8 pt)

Stabilire se le seguenti applicazioni sono omomorfismi:

- 1) $f: (\mathbb{R}, +) \rightarrow (\mathbb{Z}, +)$, $f(x)$ è il più grande intero minore di x
(detto parte intera di x)

$$\forall a, b \in \mathbb{R}, \quad f(a+b) = f(a) + f(b)$$

$$f\left(\frac{1}{2}\right) + f\left(\frac{1}{2}\right) = 0 + 0 = 0 \quad \text{ma} \quad f\left(\frac{1}{2} + \frac{1}{2}\right) = f(1) = 1$$

quindi non è omomorf.

- 2) $f: (\mathbb{Z}_2, +) \rightarrow (\mathbb{Z}_2, +)$, $f(x) = \text{rest}(x, 2)$

$$f([a]_2 + [b]_2) = f([a+b]_2) = \cancel{[a+b]_2} = [a]_2 + [b]_2 = \cancel{[a]_2} + \cancel{[b]_2} \quad \checkmark$$

$$= f([a]_2) + f([b]_2)$$

- 3) $f: (\mathbb{R}, +) \rightarrow (\mathbb{R} \setminus \{0\}, \cdot)$, $f(x) = 2^x$

$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y) \quad \checkmark$$

[ES. 4] (7 pt)

State le mat. A e B sullo stesso campo e sapendo che A è sottomat. di B, dim. che il rango di A è \leq rango di B

Se $n = rk(A)$ allora ha sicuramente una sottomat. $C_{n \times n}$ di A il cui det è diverso da 0. Questa C però è anche sottomat. di B, dunque il rango di B è almeno n, di conseguenza $rk(A) \leq rk(B)$

ESAME 21-01-22 Pro - appello

[ES. 1] (8 pt)

$A = N \times N$ e $R \subseteq A \times A$ data da

$$(a, b) R (c, d) \Leftrightarrow a+d = b+c$$

1) Dim che i rel. di eq. su A

Riflessività e simmetria sono banali

$(a, b) R (c, d) \wedge (c, d) R (e, f)$ implicano

$$a+d = b+c \wedge c+f = d+e \quad \text{da cui, per sost.,}$$

$$a+d = b+d+e-f \Rightarrow a+f = b+e \Rightarrow (a, b) R (e, f)$$

2) Desc. le classi $(1,1), (2,1) \wedge (1,2)$, più in generale

(a, b) distingue tra $a < b$ e $a > b$

$$[(1,1)]_R = \{(a, a) \mid a \in N\}$$

$$a > b \quad [(a, b)]_R = \{(\cancel{a}, \cancel{b}) (m+k, m) \mid k = a-b, m \in N\}$$

$$a < b \quad [(a, b)]_R = \{(m, m+k) \mid k = b-a, m \in N\}$$

[ES. 2] (7 pt)

$$\begin{cases} x \equiv 5 \pmod{9} \\ x \equiv 3 \pmod{7} \end{cases}$$

$$x = 5 + 9k \Rightarrow 5 + 9k \equiv 3 \pmod{7} \Rightarrow 9k \equiv -2 \pmod{7}$$

$$\text{mcd}(9, 7) = 1 \Rightarrow 1 = (-3) \cdot 9 + (8) \cdot 7$$

$$k \equiv -2 \cdot 4 \pmod{7} \Rightarrow k \equiv 6 \pmod{7}$$

$$S = [5 + 9 \cdot 6]_{9,7} = [59]_{63}$$

ES.3 (7 pt)

Sia $G = \{e, a, b, c\}$ con

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Se ne fa la tavola di mult. d. $(G, *)$ con * prodotto usuale tra mat. e si stabilisce se è un gruppo abeliano

	e	a	b	c
e	e	a	b	c
a	a	\bar{x}	c	b
b	b	c	a	e
c	c	b	e	a

Dalla tavola osserviamo per che l'operazione è associativa, l'elemento appart. a G , $*$ è anche commutativa in G e infine gli inversi appartengono ancora a G

$$a^{-1} = a \quad \text{e} \quad b^{-1} = c$$

$(G, *)$ è un gruppo abeliano

ES.4 (8 pt.)

Sia A una mat. $m \times m$ su K . Dim. che le mat. X $m \times n$ su K t.c. $AX = XA$ formano uno spazio vett. su K

Sia $S = \{X \in M_{n \times m}(K) \mid AX = XA\}$. Sappiamo che M_n è già uno sp. vett., dunque basta ver. che S sia chiuso per

somma tra mat. e prodotto per uno scalare.

$$\begin{aligned} - \forall X, Y \in S, A(X+Y) &= AX+AY = AX+XA = A(X+Y) \\ &= XA+YA = (X+Y)A \Rightarrow (X+Y) \in S \end{aligned}$$

$$- \forall \lambda \in K \text{ e } X \in S, A(\lambda X) = \lambda(AX) = \lambda(XA) = (\lambda X)A$$

da cui $\lambda X \in S$

5

ESAME 04.02.2022 I appello

[ES 1] 9 pt

Dim. che $\forall m \geq 8 \exists a, b \in \mathbb{N}_0 : m = 3a + 5b$

Hmit: $8 \leq m \leq 15$ caso per caso ; $m \geq 16$ ipotesi di induzione

Per $m=8$ si ha banalmente $a=b=1$

Supponiamo l'assunto vero per ogni $8 \leq t < m$ e dim. per m .

$$m=9 \Rightarrow a=3, b=0$$

$$m=10 \Rightarrow a=0, b=2$$

$$m=11 \Rightarrow a=2, b=1$$

$$m=12 \Rightarrow a=4, b=0$$

$$m=13 \Rightarrow a=1, b=2$$

$$m=14 \Rightarrow a=3, b=1$$

$$m=15 \Rightarrow a=0, b=3$$

Se $m \geq 16$, sarà $m = t_1 + t_2$ con $8 \leq t_1, t_2 < m$

Per ipotesi di induzione si ha

$$t_1 = 3a_1 + 5b_1 \quad e \quad t_2 = 3a_2 + 5b_2$$

$$m = 3a_1 + 5b_1 + 3a_2 + 5b_2 = 3(a_1 + a_2) + 5(b_1 + b_2)$$

[ES 2] 6 pt.

Risolvere $13x + 19y = 1$ con l'algoritmo di divisione euclidea

$$19 = 13 \cdot 1 + 6$$

$$13 = 6 \cdot 2 + 1$$

$$1 = 6 \cdot 2 + 0$$

$$\text{da cui } 1 = 13 + (-2) \cdot 6 =$$

$$= 13 + (-2)(19 + (-1) \cdot 13) =$$

$$= 13 - 13 + (-2) \cdot 19$$

$$\text{quindi } x=3 \quad e \quad y=-2$$

es 3 8 pt

Det. gli elem. invertibili e i divisori dello zero nell'anello $(\mathbb{Z}_{20}, +, \cdot)$.

Determ. anche l'inverso degli elem. trovati.

$[a]_{20} \in \mathbb{Z}_{20}$ è invertibile se e solo se $\text{MCD}(a, 20) = 1$.

Gli elem. inv. sono: $[2]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20},$

$[17]_{20}, [1]_{20}$

I divisori dello zero sono gli elem. non invert. divisori da 20.

Basta $[a]_{20}$, l'inverso $[b]_{20}$ è la classe tale che $ab \equiv 1 \pmod{20}$

$$[2]_{20}^{-1} = [1]_{20}$$

$$[3]_{20}^{-1} = [7]_{20} \Rightarrow [7]_{20}^{-1} = [3]_{20}$$

$$[5]_{20}^{-1} = [9]_{20}$$

$$[11]_{20}^{-1} = [11]_{20}$$

$$[13]_{20}^{-1} = [17]_{20} \Rightarrow [17]_{20}^{-1} = [13]_{20}$$

$$[17]_{20}^{-1} = [1]_{20}$$

es 4 7 pt.

Dim. che il sottospazio del piano cartesiano \mathbb{R}^2 di eq. $x^2 - y^2 = 0$

non è un sottosp. vett. di \mathbb{R}^2 .

$$S = \{(x, y) \in \mathbb{R}^2 \mid x^2 - y^2 = 0\}$$

Basta trovare due copie appartenenti ad S la cui somma
non fa parte di S

$$(1, -1) \in S \text{ e } (1, 1) \in S \text{ ma}$$

$$(1, -1) + (1, 1) = (2, 0) \notin S$$

[ES. 4] Fpt

$$M = \begin{pmatrix} [0] & [2] & [1] \\ [0] & [2] & [4] \\ [1] & [0] & [2] \end{pmatrix}$$

è invertibile in \mathbb{Z}_6 ? stabilire anche il range

$$\det(M) = [0] + [8] - [0] - [2] - [0] - [0] = [0] = [0]$$

dunque M non è invertibile

$$\det \begin{pmatrix} [2] & [4] \\ [0] & [2] \end{pmatrix} = [2][2] - ([2][0]) = [4] \neq [0]$$

quindi $\text{rk}(M) = 2$

[ES. 2] Fpt

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{2} \end{cases}$$

$$\text{med}(5, 3, 2) = 1$$

$$x = 2 + 5k \rightarrow 2 + 5k \equiv 1 \pmod{3} \rightarrow 5k \equiv 5 \pmod{3}$$

\downarrow

$$k \equiv 1 \pmod{3}$$

$$x = 7 \rightarrow S_2 = [7]_{25} = 7 + 15j$$

$$7 + 15j \equiv 1 \pmod{2} \rightarrow 15j \equiv -6 \pmod{2} \rightarrow 15j \equiv 0 \pmod{2}$$

$$15 \cdot j \equiv 0 \pmod{2}$$

$$S = [7 + 15 \cdot 0]_{30} = [7]_{30}$$

$$\Delta_1 = 67 - 1 \quad \Delta_2 = 97$$

[ES. 3] 8pt

$$*: \mathbb{N}_0 \rightarrow \mathbb{N}_0 : a * b = |a - b|$$

val ass della dfl.

$$1) a * b = |a - b| = |b - a| = b + a \quad \text{comm.} \quad \checkmark$$

$$3) a * e = a \quad \text{con } e \text{ elem. neutro}$$

$$a * e = |a - e| = a \rightarrow e = 0 \in \mathbb{N}_0$$

4) Simmetria ris. abili: $a * a^{-1} = e$

$$a * a^{-1} = |a - a^{-1}| = e \Rightarrow a^{-1} = a \in N_0$$

dunque ogni $a \in N_0$ è simmet.

2) basta un contro esempio per l'associatività

$$(2 * 3) * 5 = 1 * 5 = 4 \text{ ma}$$

$$2 * (3 * 5) = 2 * 2 = 0$$

ES 1 8 pt

Dati A insieme con n elementi ed il suo insieme delle parti $P(A)$

1) Poiché $|A| = n$ e $|P(A)| = 2^n > n$ esiste sempre una f. iniettiva

$$\text{es. } f: A \rightarrow P(A) : f(a) = \{a\}$$

2) Per lo stesso motivo non esiste una f. suriettiva: dato avan assegnato ad ogni $a_i \in A$ un'immagine $f(a_i) \in P(A)$, restano $2^n - n$ elem. senza corrispondente immagine

3) $R_1 = \{(a, X) \in A \times P(A) \mid a \in X\}$ non è una funzione:

se $A = \{a, b, c\}$ si ha che $(a, A) \in (c, \{a, b\})$ sono entrambi $\in R_1$, dunque ci sono due coppie con la stessa 1^a comp.

4) $R_2 = \{(a, \{a\}) \in A \times P(A)\}$ è una funzione in quanto

$\forall a \in A$, $\{a\}$ è univocam. det.; inoltre è iniettiva in quanto $a \neq b$ implica $\{a\} \neq \{b\}$