

Algebra

Teoria degli insiemi

24/09

Un insieme è una "collezione" di elementi (definizione non rigorosa)

es

$$\{0, 1\} \quad \{\text{rosso, nero}\} \quad \{0, 1, 2, \dots\} = \mathbb{N}$$

\emptyset = insieme vuoto

↪ privo di elementi e contenuto in tutti gli insiemi

Quando un insieme non può essere descritto con una lista viene preso un insieme un insieme "universo" U . I sottoinsiemi di U si caratterizzano con delle proprietà

es $U = \mathbb{N}$

$$I = \{x \in \mathbb{N} : x \text{ è pari}\} \text{ oppure } \{x \in \mathbb{N} : 2 \mid x\}$$

↓ è divisibile per 2

Inoltre gli insiemi hanno delle relazioni tra di essi

es I, J sottoinsiemi di U

$$I \subseteq J \leftrightarrow \forall x \in I, x \in J$$

$$I \not\subseteq J \leftrightarrow \exists x \in I, x \notin J$$

$$x \in I \leftrightarrow \{x\} \subset I$$

↳ singleton x

equivalentemente si può scrivere

$$\{(I, J) \text{ con } I \subseteq U, J \subseteq U : J \subsetneq I \wedge I \not\subseteq J\} \neq \emptyset$$

$$\exists I, J | I \not\subseteq J \wedge J \not\subseteq I$$

DEF COMPARABILITÀ

dati: $I, J \subseteq U$

$I \in J$ sono comparabili se $I \subseteq J \vee J \subseteq I$

DEF UGUAGLIANZA

dati: $I, J \subseteq U$

$I \in J$ sono uguali se $I \subseteq J \wedge J \subseteq I \leftrightarrow I = J$

Esempi di basi

$$V = \mathbb{C}, K = \mathbb{R}$$

Ogni singleton con elemento non nullo è una base. Per esempio $B = \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$ è una base

$$V = \mathbb{C}, K = \mathbb{R}$$

Sappiamo che ogni numero complesso $z \in \mathbb{C}$ si scrive in modo unico nella forma $z = x \cdot 1 + y \cdot i$ con $x, y \in \mathbb{R}$ dunque z risulta essere una combinazione lineare di i e 1 .

Questo vuol dire che $B = \{1, i\}$ è una base

$$\dim_{\mathbb{R}}(\mathbb{C}) = 1 \text{ e } \dim_{\mathbb{R}}(\mathbb{C}) = 2$$

Inoltre anche $\{1+i, 1-i\}$ è una base di $V = \mathbb{C}, K = \mathbb{R}$

infatti $\{1+i, 1-i\}$ è libero

$$x(1+i) + y(1-i) = 0 \Rightarrow x+i+x+y-y(-i)=0 \Rightarrow (x+y)+i(x-y)=0 \quad x, y \in \mathbb{R}$$

$$\text{dunque deve essere verificato} \quad \begin{cases} x+y=0 \\ x-y=0 \end{cases} \Rightarrow \begin{cases} y+y=0 \\ x+x=0 \end{cases} \Rightarrow \begin{cases} y=0 \\ x=0 \end{cases}$$

parte reale di z
parte immaginaria di z

Esercizio

Dimostrare che

$$\dim_{\mathbb{R}}(M_2(\mathbb{C})) = 4$$

base $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

$$\dim_{\mathbb{R}}(M_2(\mathbb{C})) = 8$$

base $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix} \right\}$

operazioni tra insiemi ($I, J \subset U$)

$$I \cap J := \{x \in U : x \in I \wedge x \in J\}$$

$$I \cup J := \{x \in U : x \in I \vee x \in J\}$$

(es)

$$I = \{1, 2, 3\}, J = \{3, 4, 5\}$$

$$I \cap J = \{3\} \quad I \cup J = \{1, 2, 3, 4, 5\}$$

$$\mathbb{N} \supset I = \{x \in \mathbb{N} : x \text{ pari}\} \quad \mathbb{N} \supset J = \{x \in \mathbb{N} : x \text{ dispari}\}$$

$$I \cap J = \emptyset \quad I \cup J = \mathbb{N}$$

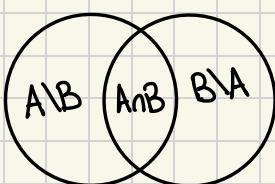
↪ supponiamo per assurdo $\exists x \in I \cap J$, il che vuol dire che

$x = 2q = 2q' + 1 \rightarrow 2(q - q') = 1$ che è impossibile dato che 1 non
è divisibile per 2

algoritmo della divisione euclidea per 2

$$x \in \mathbb{N} \quad \exists !(q, r) \in \mathbb{Z} \times \mathbb{N} \text{ t.c. } x = 2q + r \text{ con } 0 \leq r \leq 1$$

Diagramma di Venn (e la sua fallacia)

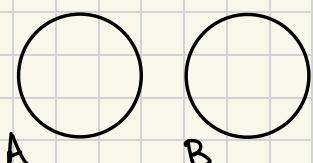


$$A \setminus B = \{x \in A : x \notin B\}$$

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

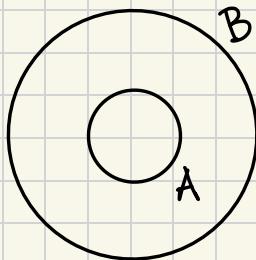
→ unione disgiunta
 $A \cup B = A \cup B$ nel caso in cui
A e B sono disgiunti

$$A \cap B = \emptyset$$

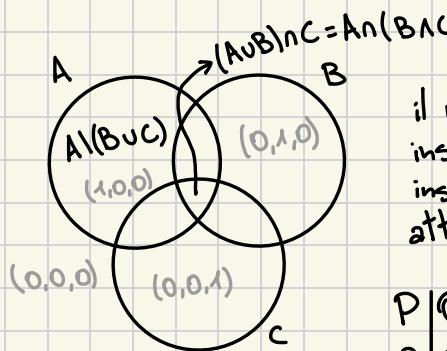


$$A \setminus B = A$$

$$B \setminus A = B$$



$$\begin{aligned} & A \subset B \\ & A \setminus B = \emptyset \\ & A \cap B = A \end{aligned}$$

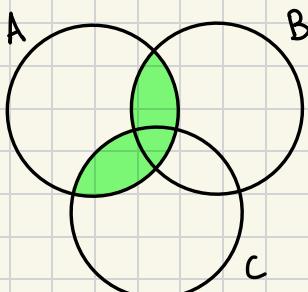


il numero massimo di sezioni date dall'unione di più insiemi è dato da 2^n (dove n è il numero di insiemi, in questo caso $2^3=8$). Questo è verificabile attraverso una tavola di verità:

P	Q	R
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Questa verità però crolla quando si provano a rappresentare tutte le sezioni date dall'unione di 4 insiemi dato che in 2 dimensioni posso rappresentare solo 14 sezioni, e non 16

Esercizio



$$A := \{x \in U : P(x) \text{ vera}\}$$

$$B := \{x \in U : Q(x) \text{ vera}\}$$

$$C := \{x \in U : R(x) \text{ vera}\}$$

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

Prodotto cartesiano

dati: X, Y due insiemi non vuoti

si definisce $X \times Y = \{(x, y) : x \in X, y \in Y\}$

$$\begin{aligned} \mathbb{R}^n &:= \mathbb{R} \times \mathbb{R}^{n-1} \\ \mathbb{R}^1 &:= \mathbb{R} \end{aligned}$$

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\} \quad X = Y = \mathbb{R}$$

es

$$(x, y, z) = (x(y, z)) = (x, \{y, \{z\}\}) = \{x, \{x, \{y, \{z\}\}\}\}$$

Corrispondenza

DEF CORRISPONDENZA

una corrispondenza su X e Y è il dato (X, Y, Γ) questo è detto grafo

dominio codominio gamma, sottoinsieme non vuoto di $X \times Y$

Relazione

DEF RELAZIONE

una relazione è un tipo particolare di corrispondenza in cui il codominio è uguale al dominio

$(X, X, \Gamma) \rightarrow$ generalmente si scrive (X, Γ)

$$x R y \leftrightarrow (x, y) \in \Gamma$$

$\hookrightarrow x$ e y si dice che sono in relazione

proprietà

riflessiva

R è riflessiva se $\forall x \in X \quad x R x \quad (\leftrightarrow \forall x \in X, (x, x) \in \Gamma)$

simmetrica

R è simmetrica se $\forall x, y \in X$ se $x R y$ allora $y R x$

transitiva

R è transitiva se presi $x, y, z \in X$, ($x R y$ e $y R z \rightarrow x R z$)

una relazione che contemporaneamente soddisfa le 3 proprietà è detta **relazione di equivalenza**

es relazione di uguaglianza

si prende $R = (\mathbb{R}, \Delta)$ dove $\Delta = \{(x, x) : x \in \mathbb{R}\}$

$$x R y \leftrightarrow x = y$$

= è riflessiva $\forall x \in \mathbb{R} x = x$

= è simmetrica $\forall x, y \in \mathbb{R} x = y \rightarrow y = x$

= è transitiva $\forall x, y, z \in \mathbb{R}, x = y \wedge y = z \rightarrow x = z$

es $X = \{\text{rette di } \mathbb{R}^2\}$

→ rette di \mathbb{R}^2

$r, r' \in X$

$r \parallel r' \leftrightarrow r e r'$ sono parallele

il parallelismo è una relazione di equivalenza

Il è riflessiva: ogni retta è parallela a sé stessa

Il è simmetrica: se $r \parallel r'$ allora $r' \parallel r$

Il è transitiva: se $r \parallel r' \wedge r' \parallel r'' \rightarrow r \parallel r''$

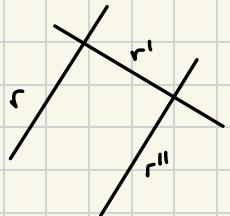
es $X = \{\text{rette di } \mathbb{R}^2\}$

$r, r' \in X r \perp r' \leftrightarrow r e r'$ sono ortogonali

\perp è simmetrica \rightarrow se $r \perp r' \rightarrow r' \perp r$

\perp non è riflessiva $\rightarrow r \not\perp r$

\perp non è transitiva \rightarrow se $r \perp r', r' \perp r'' \rightarrow r \not\perp r''$



es $X = \mathbb{R}$ $x \leq y$

riflessiva $\forall x, x \leq x$

transitiva $\forall x, y, z \quad x \leq y \wedge y \leq z \rightarrow x \leq z$

non è simmetrica $2 \leq 3$ ma $3 \not\leq 2$

è una relazione antisimmetrica

$\hookrightarrow \forall x, y \in X, x \leq y \wedge y \leq x \rightarrow x = y$

oss notare che c relazione su $\{Y : Y \subset X\}$ è, come \leq , riflessiva antisimmetrica e transitiva

è una relazione totale $\Rightarrow \forall x, y \in \mathbb{R}, x R y \vee y R x$ (non è esclusivo)

Studio delle relazioni di equivalenza

sia $R = (X, \Gamma)$ relazione di equivalenza

$x \in X$, poniamo $C(x) = \{y \in X \mid x R y\} \subset X$

\hookrightarrow insieme con tutti gli elementi in relazione tra loro

$C(x)$ è la classe di equivalenza di x e x è un rappresentante di tale classe $C(x) = C(x')$

con $x \neq x'$

oss notare che $C(x) \neq \emptyset$, infatti $x \in C(x)$ dato che R è riflessiva

proposizione 1 $R = (X, \Gamma)$ d'equivalenza

1) $x, y \in X$, allora $C(x) = C(y) \leftrightarrow x R y$

2) $\forall x, y \in X$ allora $\begin{cases} \circ C(x) = C(y) \\ \circ C(x) \cap C(y) = \emptyset \end{cases} \rightarrow$ disgiunti

in particolare, date una classe di equivalenza C , allora $\forall x \in C \quad C = Cl(x)$
(ogni elemento è rappresentante)

dim 1

supponiamo $Cl(x) = Cl(y) \rightarrow y \in Cl(x) \rightarrow x R y$

supponiamo $x R y$ allora $y \in Cl(x)$

sia $z \in Cl(y)$ si ha che $y R z$, si ha quindi che $x R y \wedge y R z \rightarrow x R z \rightarrow z \in Cl(x)$

Quindi $Cl(y) \subset Cl(x)$. Ma posso scambiare i ruoli di x e y e mostrare
nello stesso modo che $Cl(x) \subset Cl(y) \rightarrow Cl(x) = Cl(y)$

dim 2

siano $x, y \in X$.

se $Cl(x) \cap Cl(y) = \emptyset$ non c'è nulla da dimostrare

supponiamo che $Cl(x) \cap Cl(y) \neq \emptyset$

sia $z \in Cl(x) \cap Cl(y)$ allora si ha $x R z$ e $z R y$ per transitività
 $x R y$ inoltre per ① si ha $Cl(x) = Cl(y)$

DEF INSIEME DELLE PARTI

dato X insieme non vuoto

consideriamo \mathcal{P} : cui elementi sono sottoinsiemi di X ($P \in \mathcal{P} \rightarrow P \subseteq X$)

$\mathcal{P} := \{P : P \subseteq X\}$ è detto **insieme delle parti di X**

es) $X = \{1, 2, 3\}$

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

DEF PARTIZIONE

sia $\mathcal{P} \subset \mathcal{P}(X)$ non vuoto

si dice che \mathcal{P} è una **partizione di X** se:

1) $\forall P \in \mathcal{P} \quad P \neq \emptyset$

2) $\forall P, Q \in \mathcal{P}, P \neq Q \rightarrow P \cap Q = \emptyset$

3) $\forall x \in X \quad \exists P \in \mathcal{P} \mid x \in P$

es $X = \{1, 2, 3\}$

$$\mathcal{P} = \{\{1\}, \{2\}, \{3\}\} \quad \mathcal{Q} = \{\{1, 3\}, \{2\}\} \quad \mathcal{R} = \{\{1, 2\}, \{3\}\}$$

proposizione 2 $\mathcal{R} = (X, \Gamma)$ relazione di equivalenza

$\mathcal{P} = \{Cl(x) : x \in X\}$ è una partizione di X

dim
se $P \in \mathcal{P}$, allora $P = Cl(x) \exists x \in X$
 $\textcircled{1} \quad \mathcal{R}$ riflessiva $\rightarrow x \in P \rightarrow P \neq \emptyset$

$\textcircled{2}$ se $Cl(x) \neq Cl(y) \rightarrow Cl(x) \cap Cl(y) = \emptyset$ (dimostrato prima)

$\textcircled{3}$ sia $x \in X$ allora $x \in Cl(x)$ (\mathcal{R} riflessiva)

DEF QUOTIENTE DI X PER \mathcal{R}

X/\mathcal{R} (\circ $\frac{X}{\mathcal{R}}$) è l'insieme delle classi di equivalenza di X per \mathcal{R}

$$X/\mathcal{R} = \{Cl(x) : x \in X\}$$

Sistema completo di rappresentanti $\mathcal{R}(X, \Gamma)$

26/09

Un sistema completo di rappresentanti di \mathcal{R} (o SCR) è un sottoinsieme $X' \subset X$ t.c.

1) $\forall x'_1, x'_2 \in X', x'_1 \neq x'_2 \rightarrow C(x'_1) \cap C(x'_2) = \emptyset$

un insieme che ha
un elemento per
classe d'equivalenza

2) $\forall x \in X \exists! x' \in X' \text{ t.c. } x \in C(x')$

es) $X = \{r \text{ retta di } \mathbb{R}^2\}$

$\mathcal{R} = \parallel \text{parallelismo} \rightarrow \mathcal{R}$ è una relazione di equivalenza

$X' = \{\text{rette per l'origine}\}$ è un sistema completo di rappresentanti per \mathcal{R}
 $X' \subset X$

① è verificata in quanto due rette per l'origine distinte non sono parallele

② $r \in X$ esiste un'unica retta $r' \in X'$ con $r' \parallel r$

oss) in generale non c'è unicità per un SCR ad esempio possiamo scegliere $P \in \mathbb{R}$ e il fascio di rette per $P: X_P$ è un SCR
non c'è in generale canonicità nella scelta di un SCR

es)

$X \neq \emptyset \quad x, x' \in X \quad x \mathcal{R} x' \Leftrightarrow x = x'$ (relazione d'equivalenza)

\mathcal{R} è l'uguaglianza $\frac{X}{\mathcal{R}} = X \rightarrow X$ è l'unico SCR

ogni classe di equivalenza è un singleton

es)

$x, x' \in X$ allora $x \mathcal{R} x'$ sempre \Rightarrow es. $\frac{X}{\mathcal{R}} = X$

c'è una sola classe di equivalenza $\frac{X}{\mathcal{R}} = \{x\}$

in questo caso ogni SCR è un singleton della forma $\{x\}$ con $x \in X$

Esercizi

Esercizio 1. Determinare il grafico della corrispondenza tra $X := \{1, 2, 3, 4\}$ ed $Y := \{1, 3, 5\}$ definita nella seguente maniera:

x "è minore o uguale a" y .

sto considerando una corrispondenza $C = (X, Y, \Gamma)$

$$\begin{aligned}\Gamma \subset X \times Y &= \{(x, y) : x \in X, y \in Y, x \leq y\} = \\ &= \{(1, 1)(1, 3)(1, 5)(2, 3)(2, 5)(3, 3)(3, 5)(4, 5)\}\end{aligned}$$

$$X = \mathbb{N}^* := \mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}$$

introduciamo la relazione di divisibilità
se $x, y \in \mathbb{N}^*$, $x | y$ se y è un multiplo di x per un fattore intero
 \hookrightarrow "divide"

ovvero:

$$x | y \Leftrightarrow \exists k \in \mathbb{N}^* \text{ t.c. } y = kx$$

$$1) \text{ riflessiva} \rightarrow \forall x \in \mathbb{N}^* \quad x | x \quad x = x \cdot 1$$

$$2) \text{ transitiva} \rightarrow x, y, z \in \mathbb{N}^* \text{ con } x | y \wedge y | z \text{ si ha } y = kx, z = k'y$$
$$z = k'(kx) = (k'k)x \Rightarrow x | z$$

$$3) \text{ antisimmetrica} \rightarrow x, y \in \mathbb{N}^* \text{ con } x | y \text{ e } y | x \Leftrightarrow y = kx \text{ e } x = k'y$$

quindi $y = k(k'y)$ ma $y \neq 0 \Rightarrow 1 = k \cdot k'$
ma in \mathbb{N}^* , $kk' = 1 \Rightarrow k = k' = 1$ se ne deduce $y = 1 \cdot x = x \Rightarrow y = x$

Esercizio

Esercizio 7. Dire quali delle seguenti relazioni è antisimmetrica: (a) x è minore o uguale a y (b) x è minore di y (c) $x + 2y = 10$ (d) x divide y .

Ⓐ

$$x = \mathbb{R} \quad x R y \Leftrightarrow x + 2y = 10$$

$$x R y \Leftrightarrow x + 2y = 10$$

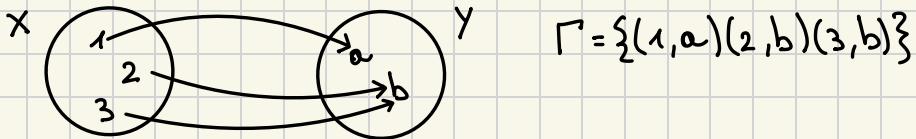
$$y R x \Leftrightarrow y + 2x = 10$$

supponiamo quindi $x R y, y R x$

$$\begin{cases} x + 2y = 10 \\ y + 2x = 10 \end{cases} \quad \begin{cases} x = 10 - 2y \\ y + 20 - 4y = 10 \end{cases} \quad \begin{cases} x = 10 - 2 \cdot \frac{10}{3} \\ y = \frac{10}{3} \end{cases} \quad \begin{cases} x = \frac{10}{3} \\ y = \frac{10}{3} \end{cases}$$

Applicazioni (funzioni)

Una funzione è una corrispondenza $f = (X, Y, \Gamma)$ con le proprietà che $\forall x \in X \exists! y \in Y$ con $(x, y) \in \Gamma$
 si scrive $y = f(x)$ o anche $X \xrightarrow{f} Y$

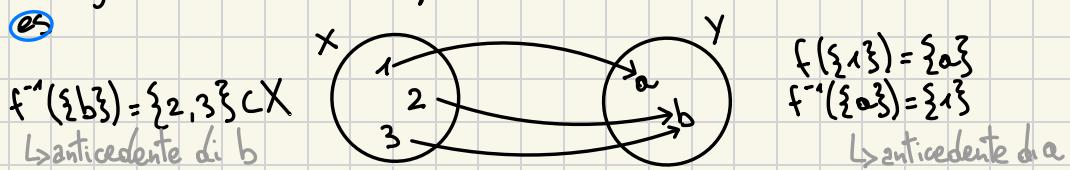


Il **codominio** si dice insieme immagine. Sia $f: X \rightarrow Y$ funzione $X' \subset X$
 $f(X') = \{y \in Y : \exists x \in X' \text{ con } f(x) = y\}$

↳ tutti gli elementi raggiunti
dal primo insieme

immagine di X' per f $f(X') \subset Y$
 $Y' \subset Y$ $f^{-1}(Y') = \{x \in X : f(x) \in Y'\}$ corrispondente
 immagine inversa di Y' ($f^{-1}(Y')$ sottoinsieme di X)

es



particolari tipi di funzioni

funzioni iniettive $X \xrightarrow{f} Y$

una funzione è detta iniettiva se $x, x' \in X$ $f(x) = f(x')$ allora $x = x'$
 alternativamente

$$\forall y \in Y \quad f^{-1}(\{y\}) = \begin{cases} \emptyset \\ \text{singleton} \end{cases}$$

es

$$f: \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0} \quad f(x) := \frac{1}{x} \quad f(x) = f(x') \Rightarrow x = x' \Rightarrow$$

$$x \mapsto \frac{1}{x} \qquad \qquad \qquad \Rightarrow \frac{1}{x} = \frac{1}{x'} \Rightarrow x \cdot \frac{1}{x} = x' \cdot \frac{1}{x'} \Rightarrow x = x'$$

funzione suriettiva $f: X \rightarrow Y$

si dice che f è suriettiva se $f(X) = Y$
 alternativamente $\forall y \in Y, \exists x \in X$ $f(x) = y$

o anche $\forall y \in Y, f^{-1}(\{y\}) \neq \emptyset$

(es) $f: \mathbb{R} \rightarrow \mathbb{R}$

sia $y \in \mathbb{R}_{\geq 0}$ allora esiste una radice x dell'equazione polinomiale $x^2 - y = 0$ $f(x) = y$

dim $\forall y \in \mathbb{R}_{\geq 0}, \exists x \in X$ t.c. $f(x) = x^2 = y$ posso porre $x = \sqrt{y}$ l'unico reale positivo tale che $x^2 = y$

funzione biettive

una funzione $f: X \rightarrow Y$ è biettiva se è al tempo stesso suriettiva e iniettiva
 f iniettiva $\Leftrightarrow \forall y \in Y, f^{-1}(\{y\}) = \emptyset$

oppure è un singleton

f suriettiva $\Leftrightarrow \forall y \in Y, f^{-1}(\{y\}) \neq \emptyset$

dunque f è biettiva $\Leftrightarrow \forall y \in Y, f^{-1}(\{y\})$ è un singleton
ogni elemento del codominio ha un unico antecedente

(es)

X insieme $\neq \emptyset$ $Id_X := (X, X, \Delta_X)$

$\Delta_X = \{(x, x) : x \in X\} \quad \forall x \quad Id_X(x) = x$

\hookrightarrow sottoinsieme diagonale ($X \times X$)

$Id_X^{-1}(\{x\}) = \{x\}$



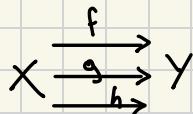
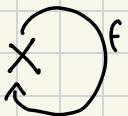
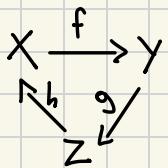
DEF DIAGRAMMA

un diagramma è una collezione di insiemi non vuoti collegati da applicazioni

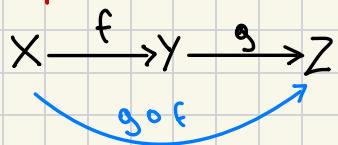
(es)

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \downarrow & \\ & Z & \end{array}$$

è un diagramma



Operazioni sulle funzioni



in questo caso si ha una funzione f che unisce X e Y e una funzione g che unisce Y e Z , dunque la funzione che collega X e Z è detta g composto f

Si definisce la funzione composta come funzione definita da $(g \circ f)(x) = g(f(x))$

$$X \xrightarrow{g \circ f} Z$$

(es)

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$$

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

DEF FUNZIONE INVERSA

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ f \text{ biettiva} & \leftrightarrow & \exists g: Y & \longrightarrow & X \text{ t.c. } f \circ g = \text{id}_Y \quad g \circ f = \text{id}_X \end{array}$$

\hookrightarrow parte Y poi applica g e arriva in X poi applica f per tornare in Y
 $y \in Y, g(y) \in X, f(g(y)) \in Y$

g è chiamata la funzione inversa (se esiste è unica)

dim

$$f \text{ biettiva} \rightarrow \forall y \in Y \ \exists ! x \in X \mid f(x) = y$$

poniamo $g(y) = x$ ben definita

Osserviamo $g \circ f$ se $x \in X$ $g(f(x)) = g(y)$ e x è l'unico elemento t.c. $f(x) = y$ quindi $g(y) = x \rightarrow g \circ f = id_X$
omettiamo di verificare che $f \circ g = id_Y$

Mostriamo che g è suriettiva

Sia $x \in X$ e poniamo $y = f(x)$

$g(y) = g(f(x)) = (g \circ f)(x) = x$, in quanto $f \circ g = id_Y \rightarrow g^{-1}(\{x\}) \neq \emptyset$
quindi f è suriettiva

Mostriamo che g è iniettiva

Siano $y, y' \in Y$ | $g(y) = g(y') = x$

Allora applicando f a sinistra ottengo $f(g(y)) = f(g(y')) = f(x)$

$$y = (f \circ g)(y) = (f \circ g)(y') = y$$

Teorema di struttura per le applicazioni [link](#)

$X \xrightarrow{f} Y$ obiettivo costruire una relazione d'equivalenza \sim su X

Si pone $x, x' \in X$, $x \sim x' \Leftrightarrow f(x) = f(x')$

\sim è una relazione d'equivalenza

$$x \sim x \rightarrow f(x) = f(x)$$

riflessiva

$$x \sim x' \Leftrightarrow f(x) = f(x') \Leftrightarrow x' \sim x$$

simmetrica

$$x \sim x', x' \sim x'' \Leftrightarrow f(x) = f(x'), f(x') = f(x'') \rightarrow f(x) = f(x'') \rightarrow x \sim x''$$

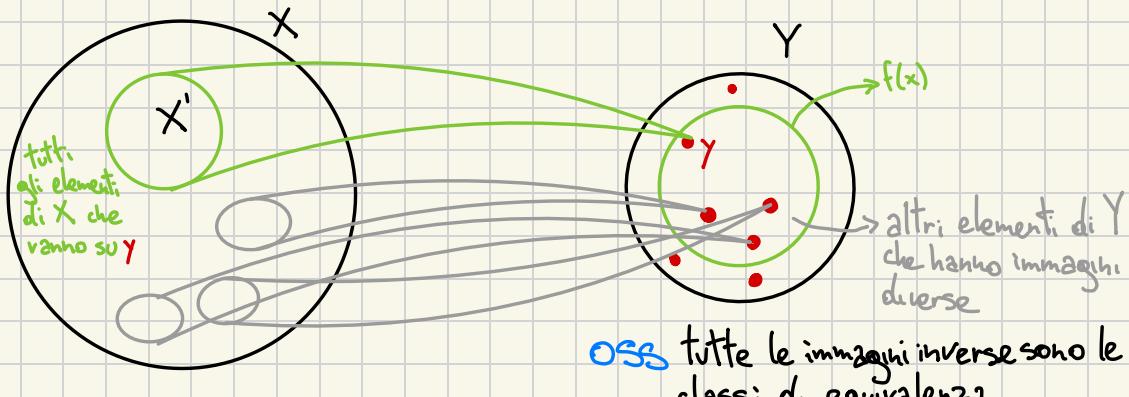
transitiva

consideriamo l'insieme quoziente X/\sim

Allora $x' \in X/\sim \Leftrightarrow x' \in X$ e $\exists y \in Y, x' = f^{-1}(\{y\})$

L se sono nella stessa classe di equivalenza hanno la stessa immagine

$$x, x' \in X, x \sim x' \Leftrightarrow f(x) = f(x')$$



OSS tutte le immagini inverse sono le classi di equivalenza $X' \subset X$ e

1) $\forall x \in X, \exists x' \in X' \text{ t.c. } x \in X' \rightarrow$ ogni elemento ha la propria classe di equivalenza

2) $X'_1, X'_2 \in X'$ e $X'_1 \neq X'_2 \rightarrow X'_1 \cap X'_2 = \emptyset \rightarrow$ due cl. eq. distinte non hanno elementi in comune

3) se $X' \in X'$ allora $f|_{X'}$ è costante, ovvero la sua immagine è un singleton
 (restringimento del dominio della funzione su X')

si costruisca a partire da $X \xrightarrow{f} Y$ una funzione $\phi: X' \rightarrow f(X) \subset Y$

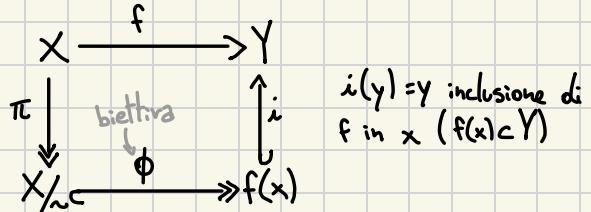
si $X' \in X'$, allora $X' = [x] \exists x \in X$

si pone $y = f(x) \in Y$, allora definiamo $\phi(X') = y$

L'applicazione ϕ è ben definita (l'immagine di una classe non dipende dalla scelta di un rappresentante se $c = [x] = [x'] \Rightarrow f(x) = f(x')$), è biettiva, e permette di calcolare f fattorizzandola come diagramma seguente

$$f = i \circ \phi \circ \pi$$

fattorizzazione di f



Per vedere che ϕ è biettiva, basta porre per $y \in f(x)$, $\psi(y) = \{x \in X : f(x) = y\}$
Quindi l'insieme $\psi(y)$ è $\neq \emptyset$
 f è suriettiva su Y (la sua immagine) dunque
 $\psi(y) = [x]$ con $f(x) = y$ in modo che $\psi = \phi^{-1}$

↳ funzione inversa
 $f(x) \xrightarrow{\psi} Y$

Esercizi

02/10

Esercizio 20. Definizione costruttiva di \mathbb{Q} a partire da \mathbb{Z}
Definiamo in $\mathbb{Z} \times \mathbb{N}^*$ (dove $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$) la relazione

$$(m, n) \sim (m', n') \Leftrightarrow mn' = nm'.$$

(a) Verificare che \sim è una relazione d'equivalenza.

poniamo $X = \mathbb{Z} \times \mathbb{N}^* = \{(n, d) : \frac{n}{d} \in \mathbb{Z}\}$

\sim è definita come $(n, d) \sim (n', d') \Leftrightarrow nd' = n'd$

riflessiva $\rightarrow (n, d) \sim (n, d)$ infatti $nd = nd$

simmetrica $\rightarrow (n, d) \sim (n', d') \Leftrightarrow (n', d') \sim (n, d)$ infatti $nd' = n'd \Leftrightarrow n'd = nd'$

In questo modo ovvio, questa relazione è riflessiva e simmetrica

transitività $(n, d) \sim (n', d') \Leftrightarrow nd' = n'd$

$$(n', d') \sim (n'', d'') \Leftrightarrow \overset{x}{n'd''} = \overset{x}{n''d'}$$

possiamo supporre $n \neq 0$ ($\Leftrightarrow n, n'' \neq 0$)

moltiplicando termine a termine le due uguaglianze troviamo

$$nd' \cdot n''d'' = n'd \cdot n''d' \Rightarrow nd'' = nd'' \Leftrightarrow (n, d) \sim (n'', d'')$$

notazione poniamo $\frac{n}{d}$ la classe di equivalenza della coppia (n, d)

$$\frac{n}{d} := [(n, d)]$$

la classe $r = \frac{x}{y}$ (rappresentante di (x, y)) è $\{(x', y') \in \mathbb{Z} \times \mathbb{N}^* : xy' = x'y\}$

tal insieme è il grafo di \sim

poniamo $\mathbb{Q} = \frac{\mathbb{Z} \times \mathbb{N}^*}{\sim}$ l'insieme dei numeri razionali

È conseguenza del teorema fondamentale dell'aritmetica ovvero, che ogni intero positivo si scrive in modo unico come prodotto di minimi termini

Il fatto che ogni classe contenga un unico elemento della forma (x, y) con x e y primi tra loro

OSS $\frac{10}{5} = \frac{2 \cdot 5}{5} = \frac{2}{1} = 2$ abbiamo più scritture della stessa frazione in quanto quelli che leggiamo sono solo dei rappresentanti della classe di equivalenza

L'insieme $\left\{ \frac{n}{d} \in \mathbb{Q} : n, d \text{ primi tra loro} \right\}$ è un SCR per \mathbb{Q}

mostriamo che esiste un'operazione di addizione + su \mathbb{Q}

consideriamo $r = \frac{n}{d}, r' = \frac{n'}{d'} \in \mathbb{Q}$

poniamo $r + r' := \frac{nd' + n'd}{dd'} \in \mathbb{Q}$

ma mi chiedo, è ben definita? non deve dipendere dalla scelta dei rappresentanti.

Mostriamo che l'addizione di $\mathbb{Q} = \frac{\mathbb{Z} \times \mathbb{N}^*}{\sim}$ è ben definita

Se $r = \frac{x}{y}$ allora $r = [(x, y)]$

Allora

$$r = [(x, y)] = [(z, t)] \xleftrightarrow{\text{1}} xt = yz$$

$$r' = [(x', y')] = [(z', t')] \xleftrightarrow{\text{2}} x't' = y'z'$$

$$\Rightarrow \frac{x}{y} + \frac{x'}{y'} = \frac{xy' + x'y}{yy'} \text{ sotto forma di } []$$

$$r + r' = [(x, y)] + [(x', y')] := \underset{\sim}{[(xy' + x'y, yy')]} := \underset{\sim}{[(x, y) + (x', y')]} := \underset{\sim}{[(x + x', y + y')]} := \underset{\sim}{[(x + x', y + y', 1)]}$$

$$r + r' = [(z, t)] + [(z', t')] := \underset{\sim}{[(zt' + z't, tt')]} := \underset{\sim}{[(z, t) + (z', t')]} := \underset{\sim}{[(z + z', t + t', 1)]}$$

per mostrare che le due operazioni sono uguali le devo mettere in relazione

utilizzo la definizione di \sim

si ha che $[(x'y' + x'y, yy')] = [(zt' + z't, tt')] \leftrightarrow (xy' + x'y)tt' = (zt' + z't)yy'$

calcoliamo

\hookrightarrow se sono uguali (stanno nella stessa classe d'equivalenza) vuol dire che sono in relazione

$$(xy' + x'y)tt' \stackrel{?}{=} (zt' + z't)yy'$$

$$xy' \underset{||}{tt'} + x'y \underset{||}{tt'} = zt' \underset{||}{yy'} + z't \underset{||}{yy'}$$

$$xt' \underset{||}{y't'} + xt' \underset{||}{yt} = zt' \underset{||}{yy'} + z't \underset{||}{yy'}$$

$$\text{|| } \textcircled{1} \quad \text{|| } \textcircled{2}$$

$$yzyt' + y'zyt = zt'yy' + z'tyy'$$

$$yzyt' + y'z't = yzyt' + y'z't \quad \text{VERO}$$

quindi $[(xy' + x'y, yy')] = [(zt' + z't, tt')]$

Se $r = \frac{n}{d}$ e $r' = \frac{n'}{d'} \in \mathbb{Q}$

$r \cdot r' := \frac{nn'}{dd'}$ è ben definito?

$$r = [(x, y)] = [(z, t)] \stackrel{\textcircled{1}}{\leftrightarrow} xt = yz$$

$$r' = [(x', y')] = [(z', t')] \stackrel{\textcircled{2}}{\leftrightarrow} x't' = z't$$

$$r \cdot r' = [(x, y)] \cdot [(x', y')] := [(\underset{||}{xx'}, \underset{||}{yy'})]$$

$$r \cdot r' = [(z, t)] \cdot [(z', t')] := [(\underset{||}{zz'}, \underset{||}{tt'})]$$

applico quindi la definizione di \sim

$$[(xx', yy')] = [(zz', tt')] \leftrightarrow xx'tt' = yy'zz'$$

$$x \cdot x' + t' = yy'zz'$$

||

$$\boxed{x} \cdot \boxed{x'} + t'$$

① ②

$$yz \cdot y'z'$$

||

$$yy'zz' = yy'zz' \text{ VERO}$$

Tornando indietro

es

$$X = \mathbb{Z}, b \in \mathbb{N}^* \quad Y = \{0, \dots, b-1\}$$

algoritmo della divisione euclidea per b

$$\forall x \in \mathbb{Z} \quad \exists! (q, r) \in \underbrace{\mathbb{Z}}_x \times \underbrace{\{0, \dots, b-1\}}_{Y=r} \text{ tale che}$$

$$x = qb + r$$

↳ resto
↳ quoziente

oss $y \in \mathbb{Z}$ e che $f|_Y = id_Y$

definiamo $f: X \longrightarrow Y$ ponendo $f(x) := r$

questa funzione è chiamata **riduzione di modulo b** (funzione che mi restituisce il resto di una divisione tra numeri interi) ed è un'applicazione suriettiva $f(x) = Y$

↳ qualsiasi divisione del tipo $\frac{x}{b}$ ha un resto $0 \leq r \leq b-1$

Allora la relazione d'equivalenza associata, notiamola \equiv , si chiama **congruenza modulo b**

↳ due numeri sono in relazione se, quando divisi per b hanno lo stesso resto

se due interi x, x' sono in relazione si scrive $x \equiv x' \pmod{b}$ e si legge "x congruenza x' modulo b"

$$X' \in \frac{X}{\equiv} \leftrightarrow \exists r \in Y, \forall x \in X', x = qb + r$$

L'insieme $Y \subset \mathbb{Z}$ è in questo caso un SCR infatti:

① f è suriettiva e quindi $\forall r \in Y \ \exists x \in X$ t.c. $x \equiv r \pmod{b}$ ②

$$\hookrightarrow X = \mathbb{Z} \quad b = 5 \quad Y = \{0, 1, 2, 3, 4\}$$

$$0 \equiv 0 \rightarrow 0 = 5 \cdot 0 + 0$$

$$2 \equiv 2 \rightarrow 2 = 5 \cdot 0 + 2$$

$$4 \equiv 4 \rightarrow 4 = 5 \cdot 0 + 4$$

$$1 \equiv 1 \rightarrow 1 = 5 \cdot 0 + 1$$

$$3 \equiv 3 \rightarrow 3 = 5 \cdot 0 + 3$$

$$9 \equiv 4 \rightarrow 9 = 5 \cdot 1 + 4$$

② $r \neq r'$ con $r, r' \in Y$, $r \not\equiv r' \pmod{b}$. Infatti, supponiamo per assurdo che $r \equiv r' \pmod{b}$,

$$\begin{cases} r = qb + \tilde{r} \\ r' = q'b + \tilde{r}' \end{cases} \text{ quindi } r - r' = (q - q')b \Rightarrow r - r' = bK \quad (K \in \mathbb{Z} - \{0\})$$

con $K > 0$ $r = r' + bK \geq r' + b$ ma $r \geq r' + b \geq b$ contraddizione r deve essere strettamente $<$ di b

ϕ è la biezione tra $\frac{X}{\equiv}$ e Y che manda ogni classe X' nell'unico $r \in Y$ t.c. $\forall x \in X', f(x) = r$ ①

In pratica, r è il resto della divisione euclidea di x per b , e non cambia al variare di x in X'

$\forall X' \in \frac{X}{\equiv}$ si scrive $X' = [x] = [x'] = [r] \quad (\forall x, x' \in X')$
 e se $\phi(X') = r \in Y = f(X) (= f(Y))$

Esercizio

Esercizio 14. Data la funzione $f : \mathbb{N} \rightarrow \mathbb{Z}$ definita da:

$$f(n) = \begin{cases} 3n & \text{se } n \text{ è pari} \\ n - 1 & \text{se } n \text{ è dispari} \end{cases}$$

determinare $f^{-1}(0)$, $f^{-1}(1)$ e $f(\mathbb{N})$.

$$f^{-1}(0) = f^{-1}(\{0\}) = \{n \in \mathbb{N} \text{ t.c. } f(n) = 0\}$$

Si ha 0 pari e $3 \cdot 0 = 0$ quindi $f(0) = 0$ e $0 \in f^{-1}(\{0\})$

Inoltre 1 è dispari e $f(1) = n - 1 = 0$
quindi $\{0, 1\} \subset f^{-1}(\{0\})$ \hookrightarrow con $n=1$

controllo quindi se ci sono altri elementi

sia adesso $n \in f^{-1}(\{0\})$, quindi $f(n) = 0$

1) se n è pari, $f(n) = 3n = 0 \Rightarrow n = 0$

2) se n è dispari, $f(n) = n - 1 = 0 \Rightarrow n = 1$

ne deduciamo $f^{-1}(\{0\}) = \{0, 1\}$

sia $n \in f^{-1}(1)$

1) se n è dispari $f(n) = n - 1 = 1 \Rightarrow n = 2 \rightarrow$ impossibile (è pari)

2) se n è pari $f(n) = 3n = 1 \Rightarrow$ impossibile (definito su \mathbb{N})

quindi $f^{-1}(1) = \emptyset$

$f(\mathbb{N}) = \{y \in \mathbb{Z} \text{ t.c. } \exists x \in \mathbb{N} \text{ con } f(x) = y\}$

$f(\mathbb{N}) = f(\underbrace{\{ \text{numeri pari} \}}_{2\mathbb{N}}) \cup f(\underbrace{\{ \text{numeri dispari} \}}_{2\mathbb{N}+1}) =$

$$= 3(2\mathbb{N}) \cup (2\mathbb{N}+1) - 1 = 6\mathbb{N} \cup 2\mathbb{N}$$

ma $6\mathbb{N} \subset 2\mathbb{N}$ quindi $f(\mathbb{N}) = 2\mathbb{N}$

variante funzione di Lothar Collatz

definiamo $f: \mathbb{N}^* \rightarrow \mathbb{N}^*$ $f(n) = \begin{cases} 3n+1 & \text{se } n \text{ è dispari} \\ \frac{n}{2} & \text{se } n \text{ è pari} \end{cases}$

calcolare $f^{-1}(1), f^{-1}(2), f^{-1}(4)$

$f(n) = 1$ se n dispari $f(n) = 3n+1 > 1$ quindi n non può essere dispari
 se n pari $f(n) = \frac{n}{2} = 1 \Leftrightarrow n = 2$
 quindi $f^{-1}(1) = \{2\}$

$f(n) = 2$ se n dispari $f(n) = 3n+1 > 2$ quindi n non può essere dispari
 se n pari $f(n) = \frac{n}{2} = 2 \Leftrightarrow n = 4$
 quindi $f^{-1}(2) = \{4\}$

$f(n) = 4$ se n dispari $f(n) = 3n+1 = 4 \Leftrightarrow n = 1$
 se n pari $f(n) = \frac{n}{2} = 4 \Leftrightarrow n = 8$
 quindi $f^{-1}(4) = \{1, 8\}$

Calcoliamo $f^{-1}(\{1, 8\}) = f^{-1}(1) \cup f^{-1}(8) = \{2\} \cup f^{-1}(8)$

n dispari $f(n) = 3n+1 = 8 \rightarrow 3n = 7$ impossibile

n pari $f(n) = \frac{n}{2} = 8 \rightarrow n = 16$

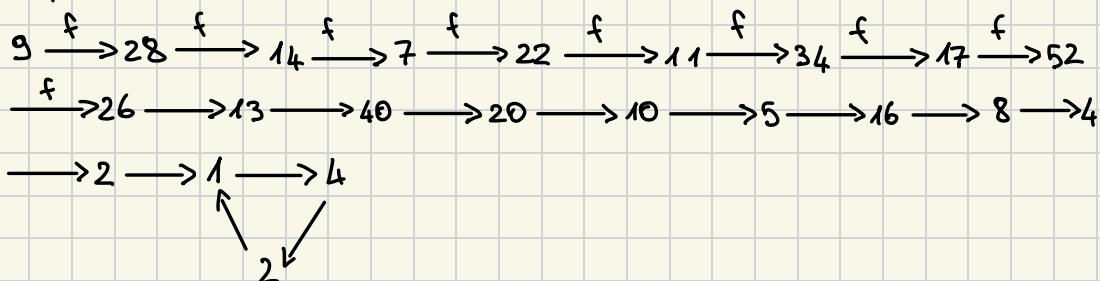
quindi $f^{-1}(\{1, 8\}) = \{2, 16\}$ continuiamo

$f^{-1}(\{2, 16\}) = \{4\} \cup f^{-1}(16) = \{4, 5, 22\}$

$f^{-1}(\{4, 5, 22\}) = \{1, 8, 10, 64\}$

congettura (Collatz) $\forall n \in \mathbb{N}^*$ esiste m t.c. $n \in \underbrace{f^{-1}(f^{-1}(\dots f^{-1}(1) \dots))}_{m \text{ volte}}$

essendo una congettura non è stata ancora riuscita a dimostrarne, ad ora è la congettura della dinamica (cose iterabili) più complessa



questo vuol dire che $9 \in \underbrace{f^{-1}(\dots f^{-1}(1) \dots)}_{19 \text{ volte}}$

Esercizio

03/10

- Esercizio 3. Studiare l'applicazione $f : \mathbb{Z} \rightarrow \mathbb{Z}$ che ad $x \in \mathbb{Z}$ associa $f(x) = ax + 1$, al variare del parametro $a \in \mathbb{Z}$. Dire quando essa è suriettiva, iniettiva.

Se $a=0$ $\forall x \in \mathbb{Z}, f(x)=1 \rightarrow$ non è né iniettiva né suriettiva

Se $a=1$ $f(x)=x+1$ quindi f ha inversa $g(y)=y-1$ ed è quindi biiettiva
infatti: $(f \circ g)(y) = f(y-1) = (y-1)+1 = y \Rightarrow f \circ g = \text{Id}_{\mathbb{Z}}$

$(g \circ f)(x) = (x+1)-1 = x \Rightarrow x=x \Rightarrow g \circ f = \text{Id}_{\mathbb{Z}} \Rightarrow f$ biiettiva

Lo stesso si può dire per $a=-1$ (con lo stesso metodo f è biiettiva)

Se $a \neq 0$ allora f è iniettiva:

$$\begin{aligned} f(n_1) = f(n_2) &\Leftrightarrow an_1 + 1 = an_2 + 1 \Leftrightarrow an_1 - an_2 = 0 \Leftrightarrow a(n_1 - n_2) = 0 \\ &\Leftrightarrow n_1 - n_2 = 0 \Leftrightarrow n_1 = n_2 \end{aligned}$$

Quindi se $a \neq 0$ si ha che f è iniettiva

Se $a \notin \{1, 0, -1\}$ f non è suriettiva

Infatti: $f^{-1}(\{a\}) = \emptyset$. Se f fosse suriettiva avremmo $\exists x \in \mathbb{Z}$ t.c. $f(x) = a$
ma allora

$$f(x) = ax + 1 = a \rightarrow a(x-1) = -1 \rightarrow a(1-x) = 1$$

ma in \mathbb{Z}^2 ci sono soltanto due coppie di interi (x, y) con $xy = 1$: $(1, 1)$ e $(-1, -1)$

Oss si riformula scrivendo " $\mathbb{Z}^X = \{1, -1\}$ "

In particolare questo implica $a \in \{1, -1\}$, ipotesi che abbiano escluso

preparazione all'esercizio 21



sia $\mathcal{P} = \{X_1, X_2\}$ una partizione di $X (\neq \emptyset)$

sia $\mathcal{Q} = \{Y_1, Y_2, Y_3\}$ una partizione di Y ($\neq \emptyset$)

quindi X ha almeno 2 elementi e Y ha almeno 3 elementi.

Mostrare che $\mathcal{R} = \{X_i \times Y_j : i=1,2, j=1,2,3\}$ è una partizione di $X \times Y$

partizione di X insieme di sottoinsiemi $\neq \emptyset$

$$\{X_i : i \in I\} \subset \mathcal{P} \text{ t.c. } ① X = \bigcup_{i \in I} X_i$$

insieme degli indici, nel nostro caso $I = \{1, 2\}$

$$② \forall i \neq j \quad X_i \cap X_j = \emptyset$$

rappresentazione grafica di \mathcal{R}

\hookrightarrow ① e ② si sintetizzano

$$\text{con } X = \bigcup_{i \in I} X_i$$

nel nostro caso

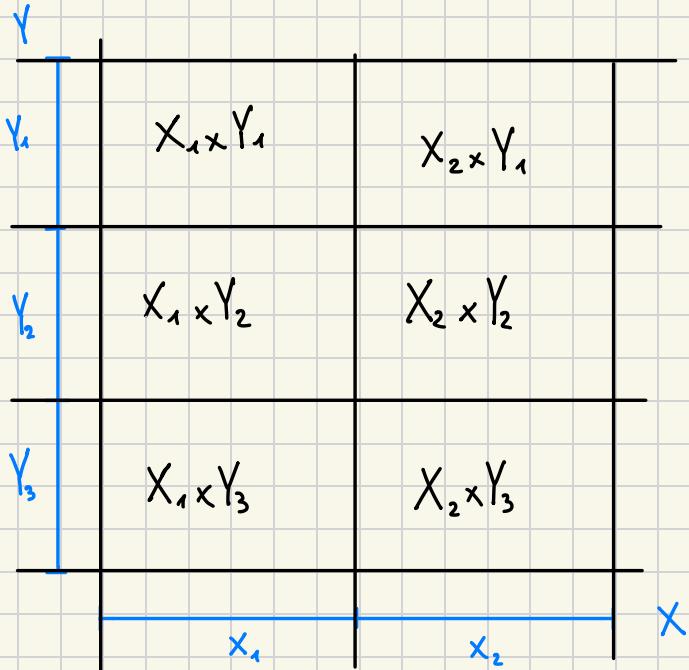
$$X = \bigcup_{i \in \{1, 2\}} X_i$$

$$Y = \bigcup_{i \in \{1, 2, 3\}} Y_i$$

$$\text{con } \{X_1, X_2, Y_1, Y_2, Y_3\} \cap \emptyset = \emptyset$$

$$\text{poniamo } I = \{1, 2\}$$

$$J = \{1, 2, 3\}$$



Allora $\mathcal{R}' = \{X' \times Y' : X' \in \mathcal{R}, Y' \in \mathcal{Q}\} =$

$$= \{X_1 \times Y_1, X_2 \times Y_1, X_1 \times Y_2, X_2 \times Y_2, X_1 \times Y_3, X_2 \times Y_3\}$$

Dimostra che \mathcal{Q} è una partizione di $X \times Y$

① $\forall (i, j) \in I \times J \quad X_i \times Y_j \neq \emptyset$

② $\forall (x, y) \in X \times Y \quad \exists (i, j) \text{ t.c. } (x, y) \in X_i \times Y_j$

③ se $(i, j) \neq (i', j')$ allora $X_i \times Y_j \cap X_{i'} \times Y_{j'} = \emptyset$

① siccome $X_i \neq \emptyset$ (\mathcal{Q} è una partizione) $\exists x \in X_i$
in modo analogo $Y_j \neq \emptyset$ ed $\exists y \in Y_j$

Quindi $(x, y) \in X_i \times Y_j \Rightarrow X_i \times Y_j \neq \emptyset$

② dati $(x, y) \in X \times Y$, \mathcal{Q} partizione $\Rightarrow \exists i \in I$ t.c. $x \in X_i$
 \mathcal{Q} partizione $\Rightarrow \exists j \in J$ t.c. $y \in Y_j$

$(x, y) \in X_i \times Y_j$

③ ma $(i, j) \neq (i', j') \Leftrightarrow i \neq i' \vee j \neq j'$

se $i = i'$ allora $X_i \cap X_{i'} = \emptyset$ (\mathcal{Q} partizione)

calcoliamo allora $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'}) = \{(x, y) : \begin{array}{l} x \in X_i \cap X_{i'} \\ y \in Y_j \cap Y_{j'} \end{array}\} = \emptyset$

se invece si ha $j \neq j'$ allora $Y_j \cap Y_{j'} = \emptyset$ questo implica, per lo stesso ragionamento $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'}) = \emptyset$

Esercizio 21. Mostrare che se $\{X_i : i \in I\}$ è una partizione di un insieme X e $\{Y_j : j \in J\}$ è una partizione di un insieme Y , allora $\{X_i \times Y_j : (i, j) \in I \times J\}$ è una partizione di $X \times Y$.

Siano date due partizioni $\{X_i : i \in I\}$ e $\{Y_j : j \in J\}$

oss l'insieme quoziente di una relazione d'equivalenza su un insieme è una partizione

$\forall (i,j) \in I \times J$ si ha $X_i \times Y_j \in X \times Y$ e chiaramente $X_i \times Y_j \neq \emptyset$ dato che $X_i \neq \emptyset$ e $Y_j \neq \emptyset$

Inoltre sia $m = (x, y) \in X \times Y$

$\exists i \in I$ t.c. $x \in X_i$ ($\{X_i : i \in I\}$ è una partizione).

In modo simile, $\exists j \in J$ t.c. $y \in Y_j$

Quindi $(x, y) \in X_i \times Y_j$

Da qui ne segue che $X \times Y \subset \bigcup_{(i,j) \in I \times J} X_i \times Y_j$

siccome $\forall (i,j)$ $X_i \times Y_j \subset X \times Y$, si ottiene $X \times Y = \bigcup_{(i,j)} X_i \times Y_j$

Inoltre siano $(i,j), (i',j') \in I \times J$ distinti

Allora si ha $i \neq i'$ oppure $j \neq j'$.

Calcoliamo $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'})$ nel caso $i \neq i'$

$(X_i \times Y_j) \cap (X_{i'}, Y_{j'}) = \{(x, y) \in X \times Y \text{ t.c. } x \in X_i \cap X_{i'} \text{ e } y \in Y_j \cap Y_{j'}\}$
ma $i \neq i' \rightarrow X_i \cap X_{i'} = \emptyset$

Da cui $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'}) = \emptyset$

si tratta il caso $j \neq j'$ in modo analogo

Esercizio (pigeon hole principle)

Esercizio 12. Sia $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ un'applicazione. Si provi che se $n > m$ allora f non è iniettiva, se $n < m$ allora f non è suriettiva.

① mostriamo che se $n > m \geq 1$ allora $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ non è iniettiva
 $\forall f$ applicazione

Per semplificare scriviamo $E_n := \{1, \dots, n\}$

Arremo bisogno delle seguenti proprietà

1) $E_n = E_{n-1} \sqcup \{n\}$

2) $\forall m_0 \in E_{m_0}, \exists E_m \setminus \{m_0\} \xrightarrow[\cong]{f} E_{m-1}$

3) Sia $X \xrightarrow{h} Y$ iniettiva. Allora il grafo Γ di h ha la proprietà che
 $\forall y \in Y, \text{ se } \exists x \in X \text{ con } (x, y) \in \Gamma, \text{ allora } x \text{ è unico}$

1) chiaro

2) l'applicazione $E_{m_0} \setminus \{m_0\} \xrightarrow{f} E_{m-1} \rightarrow \{1, 2, 4, 5\} \rightarrow \{1, 2, 3, 4\}$

$$\text{definita da } f(x) = \begin{cases} x & \text{se } x < m_0 \\ x-1 & \text{se } x \geq m_0 \end{cases}$$

$$f(1) = 1 \quad f(2) = 2$$

$$f(4) = 3 \quad f(5) = 4$$

è invertibile di inversa

$$f^{-1}(x) = \begin{cases} y & \text{se } y < m_0 \\ y+1 & \text{se } y \geq m_0 \end{cases}$$

$$\begin{aligned} f \circ f^{-1}(y) &= \begin{cases} y & \text{se } y < m_0 \\ y+1 & \text{se } y \geq m_0 \end{cases} \\ &= y \end{aligned}$$

$$\begin{aligned} f^{-1} \circ f(x) &= \begin{cases} x & \text{se } x < m_0 \\ x-1 & \text{se } x \geq m_0 \end{cases} \\ &= x \end{aligned}$$

3) chiaro: h iniettiva $\Leftrightarrow \forall y \in Y \ h^{-1}(y) = \emptyset$ oppure singleton

Si ha $\exists x \in X$ t.c. $h(x) = y \Leftrightarrow h^{-1}(y) \neq \emptyset$

$$\text{In tal caso } (x, y) \in \Gamma \Leftrightarrow f(x) = y \Leftrightarrow \{x\} = f^{-1}(y)$$

Se $m=1$ non c'è nulla da dimostrare

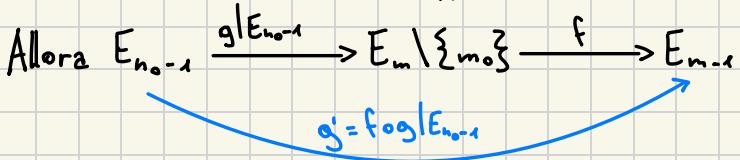
Supponiamo per assurdo che l'affermazione sia falsa

Allora $\exists n_0, m$ con $n_0 > m > 1$ e $g: E_{n_0} \rightarrow E_m$ iniettiva

Poniamo $m_0 := g(n_0)$

2) $\Rightarrow \exists E_m \setminus \{m_0\} \xrightarrow[\cong]{f} E_{m-1}$

ma $n_0 - 1 > m - 1$ possiamo supporre $m - 1 \geq 1$



g' non è iniettiva (per minimalità di n_0)

↳ se non è valido per il valore minimo di n_0 , ovvero $n_0 = m + 1$ allora non è più valido quindi sostituendo si ha $g': m \rightarrow m - 1$

3) \Rightarrow sia Γ' : il grafo di g'

$$\exists y \in Y = E_{m - 1} \text{ e } x_1, x_2 \in X = E_{n_0 - 1} \quad x_1 \neq x_2 \quad \text{t.c. } (x_1, y), (x_2, y) \in \Gamma'$$

questo implica che $g|_{E_{n_0 - 1}}$ non è iniettiva (f è necessariamente biettiva come dimostrato)

Infatti $(x_1, f^{-1}(y)), (x_2, f^{-1}(y))$ appartengono al suo grafo $\tilde{\Gamma}$

Ma il grafo Γ di g è dato da $\tilde{\Gamma} \sqcup \{(n_0, m_0)\}$ che contiene sempre i due elementi per cui g non è iniettiva. Contraddizione

2) si può procedere in modo analogo. Altrimenti, si può fare un'induzione su n (equivolentemente)

$$f: \{1, \dots, n\} \longrightarrow \{1, \dots, m\} \text{ con } m_0 = f(n) \text{ si ha}$$

$$\{1, \dots, n-1\} \xrightarrow{f|_{\{1, \dots, n-1\}}} \{1, \dots, m\} \setminus \{m_0\} \xrightarrow{g} \{1, \dots, m-1\}$$

per ipotesi induttiva $g \circ f|_{\{1, \dots, n-1\}}$ non è suriettiva

Quindi $f|_{\{1, \dots, n\}}$ non è suriettiva, e quindi neanche f lo è

L'insieme \mathbb{Z} è munito di operazione "opposto"

08/10

opposto

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ a & \longmapsto & -a \end{array}$$

e di due operazioni binarie

somma

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\ (a,b) & \longmapsto & a+b \end{array}$$

prodotto

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\cdot} & \mathbb{Z} \\ (a,b) & \longmapsto & a \cdot b = \begin{cases} \text{se } b=0 \Rightarrow 0 \text{ } b \text{ volte} \\ \text{se } b>0 \Rightarrow \underbrace{a+a+\dots+a}_{b \text{ volte}} \\ \text{se } b<0 \Rightarrow (-a)+(-a)\dots+(-a) \end{cases} \end{array}$$

L'operazione di "opposto" associa ad ogni $a \in \mathbb{Z}$ l'unico elemento
e.t.c. $a + (-a) = 0$

Ci sono diverse condizioni di compatibilità, tra queste:

$$a(b+c) = ab + ac$$

$$a+b = b+a$$

$$a+(b+c) = (a+b)+c$$

$$(ab)c = a(bc)$$

formalizziamo

DEF ANELLO (commutativo unitario)

Un anello è il dato di una sestupla $(A, +, -, \cdot, 0_A, 1_A)$

dove

$$A = \text{insieme} \neq \emptyset$$

↑. Il tutto forma A

$+: A \times A \longrightarrow A$ (addizione, mult. plazione)

$-: A \longrightarrow A$ (oppuesto)

0_A elemento neutro per addizione $0_A \in A$

1_A elemento neutro per moltiplicazione $1_A \in A$

Questi dati devono soddisfare le condizioni seguenti.

- ① $\forall a, b \in A, a+b = b+a$ + è commutativa
- ② $\forall a, b, c \in A (a+b)+c = a+(b+c)$ + è associativa
- ③ $\forall a \in A a+0_A = 0_A + a = a$
- ④ $\forall a \in A a+(-a) = 0_A$

queste proprietà stanno ad indicare che $(A, +, -, 0_A)$ è un gruppo abeliano in notazione additiva (sarà descritto ulteriormente)

- ⑤ $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ • è associativa
- ⑥ $a \cdot (b+c) = a \cdot b + a \cdot c$ • è distributiva
- ⑦ $a \cdot 1_A = 1_A \cdot a = a$
↳ l'elemento neutro per la moltiplicazione
rende l'anello "unitario"
- ⑧ $a \cdot b = b \cdot a$ • è commutativa

es)

$\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ è un anello commutativo unitario

\mathbb{N} non è un anello dato che non c'è l'oppuesto

L'anello $A = \mathbb{Z}$ ha proprietà più specifiche: buon ordinamento e ordine totale

esiste un sottoinsieme $\mathbb{N}^* \subset \mathbb{Z}$ che permette di definire una relazione su \mathbb{Z}

si scrive $a > b \iff a - b \in \mathbb{N}^*$

↳ relazione ordine totale?

proprietà di tricotomia ordine totale?

$\forall a \in \mathbb{Z}$ si ha che:
o $a = 0$
o $-a \in \mathbb{N}^*$ $\rightarrow a$ è positivo, $a > 0$

o $-a \notin \mathbb{N}^*$ $\rightarrow a$ è negativo, $a < 0$

Ogni sottoinsieme $E \subset \mathbb{N}^*$ non vuoto possiede un più piccolo elemento per $\exists c \in E$ t.c. $\forall e \in E \setminus \{c\}$ si ha che $e > c$ buon ordinamento

Un anello commutativo e unitario che soddisfa le proprietà di tricotomia e la proprietà del buon ordinamento è "essenzialmente" \mathbb{Z}

Se $a < b$ $c < d$ allora $a+c < b+d$ e $-a > -b$

\hookrightarrow l'operazione + e < sono compatibili

In modo simile $ac < bd$

\hookrightarrow l'operazione · e < sono compatibili

Legge di cancellazione in \mathbb{Z}

hp $ab = ac$ con $a \neq 0$

th $b = c$

dim

si può supporne $a > 0$. Induzione su $a \geq 1$

$a=1$ chiaro

$(a-1)b = (a-1)c$ supponiamo che $b \neq c$ $b > c \Rightarrow (a-1)b + b > (a-1)c + c \Rightarrow$
 $\Rightarrow b(a-1+1) > c(a-1+1) \Rightarrow$
 $\Rightarrow ab > ac$
contraddizione

Elementi invertibili A anello $1_A \neq 0_A$ DEF

$a \in A$ t.c. $\exists b \in A$ $ab = ba = 1_A$ è detto elemento invertibile
(si dice che b è inverso di a e si scrive $b = a^{-1}$)

es

1_A è invertibile d. inverso $1_A^{-1} = 1_A$

Si pone $A^{\times} = \{a \in A \text{ t.c. } a \text{ è invertibile}\}$

Teorema

Se $a \in A$ è invertibile a^{-1} è unicamente determinato

dim

$$a \cdot b = a \cdot b' = 1 \text{ con } b, b' \in A \quad (a \cdot b)b' = a \cdot (b \cdot b') = a(b' \cdot b) = (ab')b$$

$$\text{allora } (ab)b' = 1_A b' = b'$$

$$(ab')b = 1_A b = b$$

quindi $b = b'$ è l'inverso a^{-1} di a è ben definito

Teorema

① A^{\times} è non vuoto

② se $a \in A^{\times}$ allora $a^{-1} \in A^{\times}$ inverso chiuso per il prodotto

③ se $a, b \in A^{\times}$ allora $ab \in A^{\times} \Rightarrow (ab)^{-1} = a^{-1} \cdot b^{-1}$

④ $\mathbb{Z}^{\times} = \{1, -1\}$

dim

① $1_A \in A \quad 1_A \cdot 1_A = 1_A \Rightarrow 1_A \in A^{\times}$

② $a^{-1} \cdot b = b \cdot a^{-1} = 1_A$

possiamo vedere che b è proprio a infatti: $a^{-1} \cdot a = a \cdot a^{-1} = 1_A$

③ $a \cdot a^{-1} = a^{-1} \cdot a = 1_A \quad bb^{-1} = b^{-1}b = 1_A$

$$ab \cdot (a^{-1} \cdot b^{-1}) = aa^{-1} \cdot bb^{-1} = a \cdot 1_A = 1_A \cdot 1_A = 1_A$$

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

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

④ sia $a \in \mathbb{Z}^{\times}$ mostriamo che $a \in \{-1, 1\}$

sia quindi $a \in \mathbb{Z}^{\times}$ con $a > 0$

$\exists b \in \mathbb{Z}$ t.c. $ab = 1$. Ne deduciamo che $b > 0$ (altrimenti $b \leq 0$)

$$\text{ma } ab = \underbrace{b + \dots + b}_{a \text{ volte}} = 1$$

siccome b è positivo $a \geq b > 0 \Rightarrow b = 1$

quindi $a = a \cdot 1 = 1$

Esercizio

$(\mathbb{Q}, +, -, \cdot, 0, 1)$ è un anello calcolare \mathbb{Q}^x

dati: $q, r \in \mathbb{Q}$ $q \neq r$ per essere invertibili $qr=1$

$$q = \frac{a}{b} \text{ e } r = \frac{c}{d} \quad a, c \in \mathbb{Z} \quad b, d \in \mathbb{Z} \setminus \{0\}$$

$$\frac{a}{b} \cdot \frac{c}{d} = 1 \Rightarrow \text{ma poiché } qr=1 \text{ allora } a, c \neq 0$$

$$\text{dunque } q = \frac{a}{b} \text{ e } q^{-1} = \frac{b}{a} \quad q q^{-1} = \frac{a}{b} \cdot \frac{b}{a} = 1 \text{ per cancellazione di } \mathbb{Z}$$

$$\mathbb{Q}^x = \{r \in \mathbb{Q}, r \neq 0\}$$

"piccoli esempi"

$$\textcircled{1} \forall a \in A, a \cdot 0_A = 0_A$$

$$a \cdot 0_A = a(0_A + (-0_A)) = a0_A + a(-0_A) = a0_A + (-a) \cdot 0_A = a0_A + (-a0_A) = a0_A - (a0_A) = 0_A$$

$$\textcircled{2} \text{ supponiamo } 0_A = 1_A \text{ mostriamo che } \forall a \in A \text{ si ha } a = 0_A \quad (A = \{0_A\})$$

$$a \in A : 1_A = 0_A \Rightarrow \underbrace{a \cdot 1_A}_{=a} = a \cdot 0_A = 0_A$$

$$\textcircled{3} \text{ se } 1_A \neq 0_A \text{ allora } 0_A \notin A^x$$

$$\text{supponiamo per assurdo che } \exists x \in A^x \text{ t.c. } 1_A = x \cdot 0_A \stackrel{?}{=} 0_A$$

contraddizione
 $1_A \neq 0_A$

Esercizio

C'è un unico elemento neutro (in ogni anello)

Siano v, v' due elementi neutri

$$\forall \alpha \in A \quad \alpha v = v \alpha = \alpha$$

$$\alpha v' = v' \alpha = \alpha$$

↓

$$\alpha = v \quad vv' = v'v = v$$

$$\alpha = v' \quad v'v = vv' = v'$$

$$\left. \begin{array}{l} \alpha = v \\ \alpha = v' \end{array} \right] \longrightarrow v'v = v = v'v = v' \Rightarrow v = v'$$

Esercizio

Dedurre che anche l'elemento neutro dell'addizione è unicamente determinato

Siano v, v' due elementi neutri

$$\forall \alpha \in A \quad v + \alpha = \alpha + v = \alpha$$

$$v' + \alpha = \alpha + v' = \alpha$$

↓

$$\alpha = v \quad v' + v = v + v' = v$$

$$\alpha = v' \quad v + v' = v' + v = v'$$

$$\left. \begin{array}{l} \alpha = v \\ \alpha = v' \end{array} \right] \longrightarrow v' + v = v = v' + v = v' \Rightarrow v = v'$$

Relazione di divisibilità DEF

sia A un anello e introduciamo la relazione $a, b \in A$

$$a|b \iff \exists c \in A \text{ t.c. } b = ac$$

es

$$2|6 \rightarrow 6 = 2 \cdot 3$$

è una relazione riflessiva $\forall a \in A, a = a \cdot 1_A$ e transitiva $a, b, c \in A$

supponiamo che

$$a|b \iff b = aa' \quad \exists a' \in A$$

$$b|c \iff c = bb' \quad \exists b' \in A$$

$$\Rightarrow c = bb' = (aa')b' = a(ab') = aa'' \iff a|c$$

ma non è una relazione né simmetrica né antisimmetrica su \mathbb{Z}
 supponiamo per assurdo $a|b$ e $b|a$ con $a \neq b$ (SIMMETRIA)
 vuol dire che

$$\begin{aligned} b &= ac \quad c \in A \quad \Rightarrow a = bc' \rightarrow a = acc' \rightarrow a = ac'' \stackrel{c''=1}{\rightarrow} c'' = 1 \quad \text{prendendo} \\ a &= bc' \quad c' \in A \quad \stackrel{c=c'=1}{\text{si ha contraddizione}} \end{aligned}$$

non è antisimmetrica infatti

$$a, b \in \mathbb{Z} \quad a|b \text{ e } b|a \Rightarrow \exists c \in \mathbb{Z}^{\times} \text{ t.c. } a = bc \text{ ovvero } a \in \{b, -b\}$$

o anche $\{a, -a\} = \{b, -b\}$

possiamo supporre che $a, b \neq 0$

$$a|b \text{ e } b|a \Rightarrow b = aa', a = bb' \quad \exists a', b' \in \mathbb{Z}$$

$$b = bb'a' \rightarrow 1 = a'b' \rightarrow a', b' \in \{1, -1\} \Rightarrow \{a, -a\} = \{b, -b\}$$

altre proprietà

se $a|b$ e $a|c$ allora $a|b+c$ (compatibilità)

$$\begin{aligned} a|b &\Leftrightarrow \exists a' \in A \text{ t.c. } b = aa' \quad \Rightarrow b + c = aa' + ac'' = a(a' + a'') \Leftrightarrow a|b+c \\ a|c &\Leftrightarrow \exists a'' \in A \text{ t.c. } c = aa'' \end{aligned}$$

più generalmente se $\alpha, \beta \in A$, $a|b$, $a|c$ $\rightarrow a|ab + \beta c$

Elementi irriducibili e primi

DEF

$a \in A \setminus A^{\times}$ $a \neq 0$ è detto **irriducibile** se $\forall b, c \in A$, $a = bc$ allora $0 < b \in A^{\times}$ o $c \in A^{\times}$

es $A = \mathbb{Z}$

$12 = 4 \cdot 3$ ma $4, 3 \notin \mathbb{Z}^{\times} \Rightarrow 12$ non è irriducibile

$7 = 1 \cdot 7 = 7 \cdot 1 \quad 1 \in \mathbb{Z}^{\times} \Rightarrow 7$ è irriducibile

$9 = 3 \cdot 3 \Rightarrow$ non è irriducibile

$1 \in \mathbb{Z} \Rightarrow$ non è irriducibile per ipotesi

DEF

$a \in A \setminus A^{\times}$ $a \neq 0$ è **primo** se $\forall b, c \in A$, se $a \mid bc$ allora $a \mid b$ oppure $a \mid c$

LEMMA $p \in \mathbb{Z}$ primo $\Leftrightarrow p$ è irriducibile

dim

p primo, siano $a, b \in \mathbb{Z}$ t.c. $p \mid ab \Rightarrow p \mid ab \Rightarrow p \mid a$ o $p \mid b$

Supponiamo che $p \mid a \Rightarrow a = pa'$ $\exists a' \in \mathbb{Z} \Rightarrow p = p(a'b) \Rightarrow 1 = a'b \Rightarrow a, b \in \{-1, 1\}$

se $a = 1$ allora $a = p \Rightarrow p = pb \Rightarrow b = 1$

se $b = 1$ allora $a = -p \Rightarrow p(-b) \Rightarrow -b = 1 \Rightarrow b = 1 \quad \boxed{\Rightarrow p \text{ è irriducibile}}$

Valore assoluto $\mathbb{Z} \xrightarrow{| \cdot |} \mathbb{Z}$

$a \in \mathbb{Z}$ se $a = 0$ $|a| = 0$

se $a \neq 0$ allora $|a|$ è l'unico elemento di \mathbb{N} contenuto nell'insieme da due elementi $\{a, -a\}$

Algoritmo della divisione euclidea DEF

hp $a, n \in \mathbb{Z}$ $n \neq 0$

th esistono unicamente determinati, $q \in \mathbb{Z}$ $r \in \{0, \dots, n-1\}$ t.c. $a = nq + r$

↑ quoziente
↑ resto

legame con la congruenza

$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b \Leftrightarrow \exists q \in \mathbb{Z}$ t.c. $a - b = qn$

ovvero, il resto della divisione di $a - b$ per n è zero

link

La congruenza modulo n è una relazione di equivalenza

ricordiammo perché è transitiva $a \equiv b \pmod{n}$ $b \equiv c \pmod{n} \Leftrightarrow n \mid b - a$ e $n \mid c - b$
 $\Rightarrow n \mid c - b - a \Rightarrow n \mid c - a \Leftrightarrow c \equiv a \pmod{n}$

es

congruenza modulo 2

$$\mathbb{Z} = \underbrace{\mathbb{Z}}_{\substack{\bar{0} \\ \text{classe di } 0}} \sqcup \underbrace{\mathbb{Z}}_{\substack{\bar{1} \\ \text{classe di } 1}} + \mathbb{Z}$$

$$\mathbb{Z}/\equiv_{\text{mod}_2} = \{2\mathbb{Z}, 2\mathbb{Z}+1\} = \{\bar{0}, \bar{1}\}$$

congruenza modulo 3

$$\mathbb{Z}/\equiv_{\text{mod}_3} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\} = \{\bar{0}, \bar{1}, \bar{2}\}$$

$\bar{0}$	$\bar{1}$	$\bar{2}$
$\frac{0}{3}$	$\frac{1}{3}$	$\frac{2}{3}$
$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$
$\frac{6}{9}$	$\frac{7}{9}$	$\frac{8}{9}$

$$\mathbb{Z}/\equiv_{\text{mod}_n} = \mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+(n-1)\}$$

$$\mathbb{Z}_3 = \{m \in \mathbb{Z} : m \equiv 2 \pmod{3}\} = \{m \in \mathbb{Z} \text{ t.c. } 3 \mid m-2\}$$

$$m=2 \quad m-2=0 \quad 3 \mid 0$$

$$m=5 \quad m-2=3 \quad 3 \mid 3$$

$$m=-1 \quad m-2=-3 \quad 3 \mid -3$$

Operazioni compatibili con la congruenza

10/10

① $\forall a, a' \in \mathbb{Z} \quad a \equiv a' \pmod{n} \Leftrightarrow -a \equiv -a' \pmod{n}$

dcm

$$a \equiv a' \Leftrightarrow n \mid a - a'$$

$$n \mid a - a' \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a' - a = nk \Rightarrow -a + a' = kn \Leftrightarrow -a \equiv_n a' \Leftrightarrow -a' \equiv_n -a$$



② $a, a', b, b' \in \mathbb{Z} \quad a \equiv_n a' \quad b \equiv_n b' \text{ allora } a+b \equiv_n a'+b'$

dcm

$$a \equiv a' \Leftrightarrow n \mid a - a' \quad b \equiv b' \Leftrightarrow n \mid b - b'$$

$$n \mid a - a' \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a' - a = nk$$

$$n \mid b - b' \Leftrightarrow \exists k' \in \mathbb{Z} \text{ t.c. } b' - b = nk'$$

addizione termine a termine

$$a' + b' - (a + b) = n(k + k') \Rightarrow n | (a' + b') - (a + b) \Leftrightarrow a' + b' \equiv_n a + b$$



③ $a, a', b, b' \in \mathbb{Z} \quad a \equiv_n a' \quad b \equiv_n b' \rightarrow ab \equiv_n a'b'$

dcm

$$a \equiv_n a' \Leftrightarrow n \mid a - a' \quad b \equiv_n b' \Leftrightarrow n \mid b - b'$$

$$n \mid a - a' \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a' - a = nk$$

$$n \mid b - b' \Leftrightarrow \exists k' \in \mathbb{Z} \text{ t.c. } b' - b = nk'$$

moltiplicazione delle equazioni

$$(a' - a)(b' - b) = nkk'$$

$$ab' - a'b - ab + ab = nkk' \Rightarrow a'b - ab = nkk' \Rightarrow n | a'b - ab \Leftrightarrow a'b \equiv_n ab$$

Operazioni su $\mathbb{Z}/n\mathbb{Z}$

Definiamo $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ricordando che $\bar{a} = a + n\mathbb{Z} \rightarrow \text{es. } \bar{1} = 1 + 2\mathbb{Z}$

$$-(\bar{a}) := (-\bar{a}) \text{ applicazione } \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

è l'operazione di **opposto** in $\mathbb{Z}/n\mathbb{Z}$

→ indipendente dalla scelta dei rappresentanti

Dette $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ definiamo $\bar{a} + \bar{b} = \bar{a+b}$ ben definito delle classi \bar{a} e \bar{b}

segniamo $a' \in \bar{a}$ ($\bar{a} \equiv a'$) e $b' \in \bar{b}$

$$\overline{a+b} = \{m : n|m-a-b\}^2 = \{m : n|m-a-b\} \leftrightarrow \overline{a+b} = \overline{a} + \overline{b}$$

l'operazione **addizione** appena introdotta su $\mathbb{Z}/n\mathbb{Z}$ è ben definita

Definiamo inoltre $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ $\bar{a} \cdot \bar{b} = \bar{ab}$ ben definita

es

$$\bar{x}, \bar{z} \in \mathbb{Z}/3\mathbb{Z} \quad \bar{x} + \bar{z} = \bar{3} = \bar{0}$$

$$\bar{x} = \bar{4} \quad 1-4=3 \quad 3|3$$

$$\bar{z} = -\bar{4} \quad 2-(-4)=6 \quad 6|3$$

$$\bar{4} + \bar{4} = \overline{4+4} = \bar{0}$$

Teorema

$(\mathbb{Z}/n\mathbb{Z}, +, -, \cdot, \bar{0}, \bar{1})$ è un anello

Alcuni sottoinsiemi di \mathbb{Z}

- $n\mathbb{Z} = \{m \in \mathbb{Z} \text{ t.c. } \exists k \in \mathbb{Z} \text{ con } m = kn\}$ = multipli di n
- $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

esercizi

$$a, b \in \mathbb{Z}^*, \quad ab \leftrightarrow b \mathbb{Z} \subset a\mathbb{Z}$$

link

supponiamo che $ab \leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } b = ka$

= l

sia $b' \in b\mathbb{Z}$ $\exists l \in \mathbb{Z} \text{ t.c. } b' = lb$ ma $b = ka \Rightarrow b' = (lk)a$

dunque $b' \in a\mathbb{Z}$

link

$b\mathbb{Z} \subset a\mathbb{Z}$ allora ab

supponiamo che $b\mathbb{Z} \subset a\mathbb{Z}$ vuol dire che $\forall b' \in b\mathbb{Z} \rightarrow b' \in a\mathbb{Z}$

se $b \in b\mathbb{Z} \exists k \in \mathbb{Z} \text{ t.c. } b = kb \quad K=1$

allora $b \in a\mathbb{Z} \exists l \in \mathbb{Z} \text{ t.c. } b = la \Rightarrow ab$

- $a\mathbb{Z} + b\mathbb{Z} := \{m \in \mathbb{Z} \text{ t.c. } \exists k, k' \in \mathbb{Z} \text{ con } m = ka + k'b\}$

es

$$2\mathbb{Z} + 3\mathbb{Z} = \left\{ \begin{array}{l} K \text{ varia, } K=0, -2, 0, 2, 4, 6, 8, \dots \\ K=0, K' \text{ varia } -3, 0, 3, 6, 9, \dots \\ K, K' \text{ variano } 5, 8, 13, 7, -1, 1, \dots \end{array} \right\} = \mathbb{Z}$$

$$\hookrightarrow 2 \cdot 2 + 3 \cdot 3 = 13$$

vedremo che
 $a\mathbb{Z} + b\mathbb{Z} = \text{MCD}(a, b)\mathbb{Z}$

es $\text{MCD}(2, 3) = 1$

$$2\mathbb{Z} + 3\mathbb{Z} = 1\mathbb{Z}$$

LEMMA sia $\mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$ $a, b \neq 0 \Rightarrow$ esiste $S \in \mathbb{N}^*$ unico t.c. $\mathcal{E} = S\mathbb{Z}$

dim

per il principio del minimo un sottoinsieme non vuoto di \mathbb{N}^* ammette un elemento minimo

poniamo $\mathcal{E}^* = \mathcal{E} \cap \mathbb{N}^* \subset \mathbb{N}^*$

osserviamo che \mathcal{E}^* non è vuoto $\mathcal{E}^* \neq \emptyset$ infatti se $a, b > 0$ esiste una coppia $(K, K') \in \mathbb{N}^2$ t.c. $Ka + K'b > 0$

$\in \mathcal{E}^*$

se invece $a > 0$ e $b < 0$ allora esiste $(K, K') \in \mathbb{N} \times \{-\mathbb{N}\}$ t.c. $Ka + K'b > 0$

ci sono ancora 2 casi ma è chiaro

OSS $\mathcal{E} = \mathcal{E}^* \cup \{0\} \cup (-\mathcal{E}^*)$
 $\forall x \in \mathcal{E} \quad -x \in \mathcal{E}$ se
 $x = Ka + K'b$
 $-x = -Ka + (-K)b$

se \mathcal{E}^* è vuoto vuol dire che $-\mathcal{E} = \emptyset$
il che vuol dire che $\mathcal{E} = \{0\}$ impossibile per ipotesi

poniamo $S = \min(\mathcal{E}^*)$ ben definito in \mathbb{N}^* (principio del minimo)

osserviamo che:

$S \leq |a|$ e $S \leq |b|$ infatti $|a|, |b| \in \mathcal{E}^*$

sia S/a per divisione euclidea si ha $a = qS + r$ $r \in \{0, \dots, S-1\}$

notiamo che $r = a - qS$, e dato che $S \in \mathcal{E}^* \subset \mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$

$S = qa + rb \quad q, r \in \mathbb{Z}$

dunque si ha

$$r = a - q(qa + rb) \rightarrow r = a(1-q) + b(-q) \Rightarrow r \in \mathcal{E}^* \Rightarrow r \geq S$$

quindi $r=0$ e S/a

per la stessa ragione S/b

CONTRADDIZIONE

se $r \neq 0$ allora $r \in \mathcal{E}^*$ e quindi deve essere $\geq S$ dato che S è il minimo ma è impossibile per la definizione di r

$\forall \alpha, \beta \in \mathbb{Z} \quad S | \alpha a + \beta b \Rightarrow \mathcal{E} \subset S\mathbb{Z}$ d'altronde $S \in \mathcal{E} \iff S = Ka + Kb$

$$\forall k \in \mathbb{Z} \quad lk = (lk)a + (lk')b \Rightarrow lS \subseteq E \Rightarrow S \subseteq E$$



Massimo comun divisore DEF

link

$(a, b) \in \mathbb{Z}^2$ con $(a, b) \neq (0, 0)$

$d \in \mathbb{N}^*$ è MCD di a e b se si scrive $d = \text{MCD}(a, b)$

① $d \mid a$ e $d \mid b$

② $d' \in \mathbb{N}^*$ t.c. $d' \mid a$ e $d' \mid b \Rightarrow d' \mid d$

LEMMA se d soddisfa ① e ② allora d è unicamente determinato

dim

supponiamo che d_1, d_2 soddisfino ① ②

mostriamo che $d_1 = d_2$

si ha $d_2 \mid d_1$ e $d_1 \mid d_2 \Rightarrow \{d_1, -d_1\} = \{d_2, -d_2\} \Rightarrow d_1 = d_2$ \rightarrow su \mathbb{N}^* la relazione di divisibilità è antisimmetrica quindi

$$alb, bla \Rightarrow a=b$$



Terminologia se $\text{MCD}(a, b) = 1$ si dice che a, b sono primi tra loro (coprimi)

link

LEMMA dato $a\mathbb{Z} + b\mathbb{Z} = S\mathbb{Z}$ con $a, b \neq 0$ allora $S = \text{MCD}(a, b)$

dim

$$S\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \supset a\mathbb{Z} \Rightarrow S \mid a$$

$$S\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \supset b\mathbb{Z} \Rightarrow S \mid b$$

condizione ① di MCD
verificata

sia $d' \in \mathbb{N}^*$ t.c. $d' \mid a, d' \mid b$

$$d' \mid a \Leftrightarrow a \in d'\mathbb{Z}$$

$$d' \mid b \Leftrightarrow b \in d'\mathbb{Z}$$

$$S\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset (d'\mathbb{Z} + d'\mathbb{Z}) \Rightarrow d' \mid S$$



Algoritmo di Euclide (MCD)

dati: $a, b > 0$ servirà a trovare $S = \text{MCD}(a, b)$

$$a = q_0 b + r_0 \quad 0 \leq r_0 < b$$

$$b = q_1 r_0 + r_1 \quad 0 \leq r_1 < r_0$$

$$r_0 = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

:

$$r_{n-2} = q_n r_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0 \quad \text{---}$$

es

$$a = 3522 \quad b = 321$$

$$3522 = 10 \cdot 321 + 312$$

$$321 = 1 \cdot 312 + 9$$

$$312 = 34 \cdot 9 + 6$$

$$\boxed{9 = 1 \cdot 6 + 3} \quad 3 = \text{MCD}(3522, 321)$$

$$6 = 2 \cdot 3 + 0$$

$$\text{inoltre } 6\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \Rightarrow \exists u, v \in \mathbb{Z} \quad 3 = 3522u + 321v$$

come calcolo u e v ?

Identità di Bezout link

dati $a, b \neq 0$ $\exists x, y: ax + by = \text{MCD}(a, b)$

coefficients di Bezout

es

saliamo nelle iterazioni dell'algoritmo di Euclide e prendiamo il resto

$$3 = 9 - 1 \cdot 6$$

$$6 = 312 - 34 \cdot 9$$

↓

$$3 = 9 - 1(312 - 34 \cdot 9) \Rightarrow 3 = 9 - 312 + (34 \cdot 9)$$

$$\Rightarrow 3 = 9 \cdot 35 - 312$$

$$9 = 321 - 312$$

↓

$$3 = (321 - 312) \cdot 35 - 312$$

$$3 = 321 \cdot 35 - 312 \cdot 36$$

$$312 = 3522 - 10 \cdot 321$$

↓

$$3 = 321 \cdot 35 - (3522 - 10 \cdot 321) \cdot 36 \Rightarrow 3 = 321 \cdot 35 - 3522 \cdot 36 + 36 \cdot 10 \cdot 321$$

↓

$$3 = 321(35 + 360) - 3522 \cdot 36$$

$$\text{dunque } 3 = (-36) \cdot 3522 + (395) \cdot 321$$

↓

↓

↓

↓

↓

LEMMA di Gauss se $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$ e se $\text{MCD}(a, b) = 1$
allora $a \mid bc \rightarrow a \mid c$

dim

$$\text{MCD}(a, b) = 1 \xrightarrow{\text{qui}} a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$$

questo vuol dire che $\exists u, v \in \mathbb{Z}$ t.c. $au + bv = 1$

moltiplico termine a termine per c

$$auc + bcv = c$$

\hookrightarrow per ipotesi è divisibile per a

$$a \mid bc \Leftrightarrow bc = ak$$

\Downarrow

$$auc + akv = c \Rightarrow a(uv + kv) = c \Rightarrow \exists l \text{ t.c. } al = c \Leftrightarrow a \mid c \quad \blacksquare$$

LEMMA $p \in \mathbb{N}$ $p > 1$. Allora p irriducibile $\Rightarrow p$ primo

dim

claim se p irriducibile e $p \nmid a$ allora $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$ ($\text{MCD}(a, p) = 1$)

infatti $\delta = 1$, altrimenti $\exists \delta > 1$ t.c. $\delta \mid a$ e $\delta \mid p$

visto che p è irriducibile $\delta = p \Rightarrow p \mid a$ CONTRADDIZIONE

suppongo $p \mid ab$ e che $p \nmid a$ (sto supponendo una parte delle ipotesi
dell'essere primi e verifico che $p \mid b$)

ma allora $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$, moltiplico tutto per b

$$\underbrace{ab\mathbb{Z} + pb\mathbb{Z}}_{p \mid ab} = b\mathbb{Z} \Rightarrow ab\mathbb{Z} + pb\mathbb{Z} = b\mathbb{Z} \subset p\mathbb{Z} \xrightarrow{\text{qui}} p \mid b$$

$p \mid ab$ $p \mid pb$

Esercizi

Esercizio 2. Dati i seguenti interi $a, b \in \mathbb{Z}$, calcolare il loro massimo comun
divisore d e trovare interi s, t tali che $as + bt = d$.

(Suggerimento: usare l'algoritmo di Euclide.)

- (i) $a = 168, b = 1911$
- (ii) $a = -143, b = 299$

$$a = 1911 \quad b = 168$$

$$1911 = 11 \cdot 168 + 63 \quad 21 = \text{MCD}(1911, 168)$$

$$168 = 2 \cdot 63 + 42$$

$$a = -143 \quad b = 299$$

$$-143 = -1 \cdot 299 + 156$$

$$299 = 1 \cdot 156 + 143$$

$$63 = 1 \cdot 42 + 21$$

$$42 = 2 \cdot 21 + 0$$

$$21 = u_a + v_b$$

$$u=3 \quad v=-34$$

$$21 = 63 - 42$$

$$21 = 63 - 168 + 2 \cdot 63$$

$$21 = 3(1911 - 11 \cdot 168) - 168$$

$$21 = 3 \cdot 1911 - 34 \cdot 168$$

$$156 = 1 \cdot 143 + 13$$

$$143 = 11 \cdot 13 + 0$$

$$13 = u_a + v_b$$

$$u=1 \quad v=2$$

$$13 = 156 - 143$$

$$13 = 156 - 299 + 156$$

$$13 = 2(299 - 143) - 299$$

$$13 = 1 \cdot 299 + 2(-143)$$

Esercizio 3. Dimostrare che, per ogni intero n , il numero $2n^{17} + 2n^{15} + 3n^3 + 3n$ è divisibile per 5.

la classe modulo 5 $\frac{\mathbb{Z}}{5\mathbb{Z}}$: $2n^{17} + 2n^{15} + 3n^3 + 3n = \bar{2} \cdot \bar{n}^{17} + \bar{2} \cdot \bar{n}^{15} + \bar{3} \cdot \bar{n}^3 + \bar{3} \cdot \bar{n} = \bar{0}$

se $n \equiv 0 \pmod{5} \Leftrightarrow \bar{n} = \bar{0}$ allora la proprietà richiesta è chiaramente verificata

\bar{n}	\bar{n}^3	\bar{n}^{15}	\bar{n}^{17}	$3\bar{n}$	$3\bar{n}^3$	$2\bar{n}^{15}$	$2\bar{n}^{17}$	$3\bar{n} + 3\bar{n}^3 + 3\bar{n}^{15} + 3\bar{n}^{17}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{2}$	$\bar{3} + \bar{3} + \bar{2} + \bar{2} = \bar{10} = \bar{0}$
$\bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{1}$	$\bar{4}$	$\bar{1} + \bar{4} + \bar{1} + \bar{4} = \bar{10} = \bar{0}$
$\bar{3}$	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{4}$	$\bar{1}$	$\bar{4} + \bar{1} + \bar{4} + \bar{1} = \bar{10} = \bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{2} + \bar{2} + \bar{3} + \bar{3} = \bar{10} = \bar{0}$

Studiamo le potenze di 2 modulo 5

$$\bar{2}^0 = \bar{1}$$

$m = 4q + r$ quindi per calcolare 2^m basta

$$\bar{2}^1 = \bar{2}$$

$\bar{2}^m = \bar{2}^4 \cdot \bar{2}^r$ calcolare 2^r dove r è il resto

$$\bar{2}^2 = \bar{4}$$

$\Rightarrow (\bar{2}^4)^q \bar{2}^r$ della divisione per 4

$$\bar{2}^3 = \bar{4} \cdot \bar{2} = \bar{8} = \bar{3}$$

$$\Rightarrow \bar{1} \cdot \bar{2}^r = \bar{2}^r$$

$$\bar{2}^4 = \bar{2} \cdot \bar{8} = \bar{2} \cdot \bar{3} = \bar{6} = \bar{1}$$

(es) $\bar{2}^{17} \Rightarrow 17 = 4 \cdot 4 + 1$

$$\bar{2}^{15} = \bar{2}^4 \cdot \bar{2}$$

$$\bar{2}^{15} = \bar{2}^4 = \bar{2}$$

$$\bar{3}^{15} \Rightarrow 15 = 3 \cdot 4 + 3$$

$$\bar{3}^{15} = \bar{3}^3 = \bar{2}$$

Esercizio 4. Calcolare $(\mathbb{Z}/N\mathbb{Z})^\times$ per N intero positivo. Cosa si osserva se N è un numero primo?

$$A = \frac{\mathbb{Z}}{N\mathbb{Z}} \quad \bar{a} + \bar{b} := \bar{a+b} \quad (\text{idem per la moltiplicazione})$$

con l'elemento $\bar{0}$ ($=N\mathbb{Z}$) per il neutro dell'addizione e con l'elemento $\bar{1}$ ($=N\mathbb{Z}+1$) il neutro della moltiplicazione, si ottiene che A è munito di struttura di un anello commutativo unitario.

$$\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^x = \left\{ \bar{a} \in \frac{\mathbb{Z}}{N\mathbb{Z}} \text{ t.c. } \exists \bar{b} \in \frac{\mathbb{Z}}{N\mathbb{Z}} \text{ con } \bar{a} \cdot \bar{b} = \bar{1} \right\}$$

$$\textcircled{1} \text{ Sia } \bar{a} \in \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^x : \exists \bar{b} \in \frac{\mathbb{Z}}{N\mathbb{Z}} \text{ t.c. } \bar{a} \cdot \bar{b} = \bar{1} \quad (\bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1})$$

$$\bar{a}\bar{b} = \bar{1} \iff N \mid ab - 1 \iff \exists K \in \mathbb{Z} \text{ t.c. } KN = ab - 1 \iff ab - KN = 1 \iff$$

è visto che sono due rappresentanti
della stessa classe sono congruenti
modulo N

$\iff a \in N$ sono primi tra loro

$$\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^x = \left\{ \bar{a} : a \in \mathbb{Z} \text{ e } \text{MCD}(a, N) = 1 \right\}$$

esiste quindi un'applicazione biettiva

$$\text{tra } \{r \in \{0, \dots, N-1\} \text{ t.c. } \text{MCD}(r, N) = 1\} \text{ e } \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^x$$

$$r \longrightarrow \bar{r}$$

es

$$N = 24 = 2^3 \cdot 3 \text{ verificare che } \left(\frac{\mathbb{Z}}{24\mathbb{Z}}\right)^x = \left\{ r : \frac{2^3 \mid r}{3 \nmid r} \right\}$$

$$\left(\frac{\mathbb{Z}}{24\mathbb{Z}}\right)^x = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{15}, \bar{16}, \bar{17}, \bar{18}, \bar{19}, \bar{20}, \bar{21}, \bar{22}, \bar{23} \}$$

$$\textcircled{2} N = p \text{ primo : sia } r \in \{1, \dots, p-1\}^{p-1 \text{ classi}}$$

$\text{MCD}(p, r) = 1$, altrimenti qualora si avesse $s = \text{MCD}(p, r) > 1$ avrei

$\text{S} \mid p, \text{S} \mid r \Rightarrow s \mid p$ quindi si avrebbe $p \mid r$ ma $r < p$ (è un resto) \rightarrow si avrebbe una CONTRADDIZIONE

qui

Si ottiene $(\mathbb{Z}/p\mathbb{Z})^* = \{\bar{r} : 1 \leq r \leq p-1\}$

$\forall r \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \Rightarrow r$ è invertibile

terminologia A anello commutativo unitario t.c. $\forall r \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ è invertibile si dice **campo**

Esercizio 5. Dimostrare il piccolo teorema di Fermat, che afferma che, dato un numero primo p e un intero n , $n^p \equiv n \pmod{p}$. Mostrare inoltre che se n e p sono primi fra loro, allora si ha $n^{p-1} \equiv 1 \pmod{p}$. ②

① proprietà in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ campo, ovvero l'insieme $\mathbb{F}_p^\times = \{\bar{1}, \bar{2}, \dots, \bar{p-1}\}$

$$(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p \text{ con } \bar{a}, \bar{b} \in \mathbb{F}_p$$

scegliamo $a, b \in \mathbb{Z}$ rappresentanti di \bar{a}, \bar{b}

$$(\bar{a} + \bar{b})^p = \bar{a}^p + \binom{p}{1} \bar{a}^{p-1} \bar{b} + \binom{p}{2} \bar{a}^{p-2} \bar{b}^2 + \dots + \binom{p}{p-2} \bar{a}^2 \bar{b}^{p-2} + \binom{p}{p-1} \bar{a} \bar{b}^{p-1} + \bar{b}^p$$

② $(a+b)^p = \bar{a}^p + 2ab + b^p = \binom{2}{0} \bar{a}^2 + \binom{2}{1} ab + \binom{2}{2} b^2$

ricordiamo alcune proprietà dei coefficienti binomiali:

$$0 \leq m \leq n \quad \binom{n}{m} = \frac{n!}{m!(n-m)!} = \text{card}(\{U \subset \{1, \dots, n\} \text{ t.c. } \text{card}(U) = m\})$$

$$\binom{n}{0} = \binom{n}{n} = 1 \quad \binom{n}{m} = \binom{n}{n-m}$$

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \quad \binom{p}{i} \in \mathbb{N} \text{ si ha che } i!(p-i)! \mid p!$$

supponiamo $1 \leq i \leq p-1$

$$\text{inoltre } i! = i(i-1)\dots 3 \cdot 2 \cdot 1$$

e siccome $p > i$, si ha che $p \nmid i!$ infatti $p > i, p > i-1, \dots$ ed essendo primo p non può essere il prodotto di alcuni di questi

$$\text{ho } p! = a \cdot i!(p-i)! \quad \exists a \in \mathbb{N}^*$$

$p \nmid b$ siccome p è primo ma $p \mid ab = p!$
per lemma di Gauss $\Rightarrow p \mid a = \binom{p}{i}$

dunque se $1 \leq i \leq p-1$ e p è primo si ha $\binom{p}{i} = \binom{p}{p-i} \equiv 0 \pmod{p}$
riducendo modulo p lo sviluppo del binomio di Newton ottengo

$$(\bar{a} + \bar{b})^p = \bar{a}^p + \binom{p}{1} \bar{a}^{p-1} \bar{b} + \dots + \bar{b}^p \equiv \bar{a}^p + \bar{b}^p \pmod{p}$$

e quindi ottengo $(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$ in \mathbb{F}_p

$$\bar{0}^p = \bar{0}$$

$$\bar{1}^p = \bar{1}$$

$$\bar{2}^p = (\bar{1} + \bar{1})^p = \bar{1}^p + \bar{1}^p = \bar{1} + \bar{1} = \bar{2}$$

⋮

$$\bar{n}^p = (\bar{n-1} + \bar{1})^p = \bar{n-1}^p + \bar{1}^p = \bar{n-1} + \bar{1} = \bar{n}$$

per ipotesi
induttiva

(2)

Precisazione $\bar{n} \neq \bar{0}$ in \mathbb{F}_p (ovvero se $\bar{n} \in \mathbb{F}_p^\times$) allora n è invertibile di inversa \bar{n}^{-1} per il PTF so già che $\bar{n}^p = \bar{n}$ (in \mathbb{F}_p)

moltiplichiamo per \bar{n}^{-1}

$$\text{ottengo } \bar{n}'\bar{n}^p = \bar{n}'\bar{n} = \bar{1}$$

$$\bar{n}'\bar{n}'\bar{n}^{p-1} \quad \begin{matrix} \uparrow \\ \bar{n}' \text{ è l'inversa di } \bar{n} \end{matrix}$$

$$\bar{n}^{p-1} \Rightarrow \text{se } \bar{n} \neq \bar{0} \\ \text{allora } \bar{n}^{p-1} = \bar{1}$$

problemi

se $a \in \mathbb{F}_p^\times$ calcolare \bar{a}^{-1} (inverso) in modo facile usando PTF sache $\bar{a}^{p-1} = \bar{1}$

Scrivendo $\bar{a}^{p-1} = \bar{a}^{p-2} \cdot a$ se ne deduce $\bar{a}^{-1} = \bar{a}^{p-2}$

$\frac{1}{\bar{a}}$

(es)

trovare il resto della divisione di 89741^{527} per 9

notare che $\bar{10} = \bar{1}$ ($10 \equiv 1 \pmod 9$). Allora visto che

$$89741 = 1 + 4 \cdot 10 + 7 \cdot 10^2 + 9 \cdot 10^3 + 8 \cdot 10^4 \text{ si trova}$$

$$\overline{89741} = \bar{1} + \bar{4} \cdot \bar{10} + \bar{7} \cdot \bar{10}^2 + \bar{9} \cdot \bar{10}^3 + \bar{8} \cdot \bar{10}^4 = \bar{1} + \bar{4} + \bar{7} + \bar{9} + \bar{8} = \bar{29} = \bar{2}$$

studiando $\bar{2}^k$, $k \in \mathbb{Z}$

$$(2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6) = (1, 2, 4, 8, 16, 32, 64) \equiv (1, 2, 4, 8, 7, 5, 1) \pmod 9$$

in particolare $\bar{2}^6 = \bar{1}$ quindi $2^k = 2^{9r+r} \equiv 2^r \pmod 9$ con $0 \leq r \leq 6$

$$k = 527 = 87 \cdot 9 + 5 \Rightarrow 89741^{527} \stackrel{?}{=} 2^5 \equiv 5 \pmod 9$$

(es)

Nessun intero in $4\mathbb{Z} + 3$ è la somma di due quadrati. Come provarlo?

Calcoliamo le classi resto modulo 4 dei quadrati.

\bar{n}	\bar{n}^2	la somma di due quadrati (mod 4)
$\bar{0}$	$\bar{0}$	può quindi essere soltanto
$\bar{1}$	$\bar{1}$	
$\bar{2}$	$\bar{0}$	
$\bar{3}$	$\bar{1}$	

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

in particolare non è mai $= \bar{3}$

Successione di Fibonacci

$(F_n)_{n \geq 0}$ definita induttivamente

$$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$$

proprietà

$$\text{MCD}(F_m, F_n) = F_{\text{MCD}(m, n)}$$

$$\text{in particolare } \text{MCD}(F_m, F_{m+1}) = F_1 = 1$$

Esercizio 9. Se F_n è l' n -esimo numero di Fibonacci, quanto vale il massimo comune divisore (F_n, F_{n+1}) ? Dimostrarlo per induzione, usando l'algoritmo euclideo.

$$F_0 = 0 \quad F_1 = 1 \quad F_{n+1} = F_n + F_{n-1}$$

$$\text{MCD}(F_n, F_{n+1}) = \delta_n$$

$$\mathbb{Z}F_n + \mathbb{Z}F_{n+1} = \mathbb{Z}\delta_n$$

"

claim

$$\{aF_n + bF_{n+1} \text{ t.c. } a, b \in \mathbb{Z}\} = \{aF_n + b(F_n + F_{n-1}), a, b \in \mathbb{Z}\} = \mathbb{Z}F_{n-1} + \mathbb{Z}F_n$$

$$aF_n + b(F_n + F_{n-1}) = (a+b)F_n + bF_{n-1}$$

$$\{(a+b, b), a, b \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$$

$$\text{definiamo } f: \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$

$$\text{con } f(a, b) = (a+b, b). \text{ Mostriamo che } f \text{ è biettiva}$$

$$f \text{ biettiva} \leftrightarrow \text{si ha: } \exists G: B \longrightarrow A \text{ t.c. } f \circ G: B \longrightarrow B = id_B \rightarrow \forall b \in B, f(G(b)) = b$$

$$\begin{array}{ccc} & f & \\ A & \xrightarrow{\hspace{2cm}} & B \\ & G & \end{array}$$

$\forall b \in B, f^{-1}(b)$ è singleton
quindi esiste una funzione inversa

$$G \circ f: A \longrightarrow A = id_A \rightarrow \forall a \in A, f(G(a)) = a$$

$$f: \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2 \quad f(a, b) = (a+b, b) \quad f(u, v) = (f(u, v)_1, f(u, v)_2)$$

sia $(u, v) \in \mathbb{Z}^2$. Per calcolare $f^{-1}(u, v)$ devo risolvere

$$\begin{cases} a+b=u \\ b=v \end{cases} \Rightarrow (a, b) = (u-v, v)$$

poniamo $g: \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2 \quad g(u, v) = (u-v, v)$

$$(f \circ g)(u, v) = f(g(u, v)) = f(\underbrace{u-v}_a, v) = (u-v+v, v) = (u, v)$$

$$(g \circ f)(a+b) = g(f(a+b)) = g(\underbrace{a+b}_u, \underbrace{b}_v) = (a+b-b, b) = (a, b)$$

si verifica che $f \circ g = \text{id}_{\mathbb{Z}^2} = g \circ f$

Ne deduciamo che

$$\{aF_n + b(F_{n+1} + F_{n-1}), a, b \in \mathbb{Z}\} = \{(a+b)F_n + bF_{n-1}, a, b \in \mathbb{Z}\} =$$

$$= \{\underbrace{f(a, b)}_v, \underbrace{F_n + f(a, b)}_v, F_{n-1}, a, b \in \mathbb{Z}\} =$$

$$= \{uF_n + vF_{n-1}, a, b \in \mathbb{Z}\} = \mathbb{Z}F_n + \mathbb{Z}F_{n-1}$$

conclusione

$$\mathbb{Z}F_{n+1} + \mathbb{Z}F_n = \mathbb{Z}F_n + \mathbb{Z}F_{n-1} = \dots \stackrel{\text{induzione}}{=} \mathbb{Z}F_1 + \mathbb{Z}F_0 = \mathbb{Z} \Rightarrow F_{n+1} \text{ e } F_n \text{ sono coprimi} \Leftrightarrow \text{qui} \quad \Leftrightarrow \text{MCD}(F_{n+1}, F_n) = 1 \quad \forall n \geq 0$$



Teorema fondamentale dell'aritmetica

$$\forall a \in \mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$$

② l'insieme $I_a = \{p \text{ primo: } p \mid a\}$ è finito

$$\text{b) inoltre } a = (\pm 1) \cdot \prod_p p^{v_p(a)}$$

dove $v_p(a) \in \mathbb{N}$ e sono unicamente determinati.

OSS si sa che $P = \{p \in \mathbb{N}, p \text{ primo}\}$ è infinito siccome per $\forall a \in \mathbb{Z}^*$ I_a è finito

$$a = \prod_p p^{v_p(a)} = \prod_{p \in I_a} p^{v_p(a)} \prod_{p \notin I_a} p^{v_p(a)}$$

dim

supponiamo $a > 0$

③ supponiamo per assurdo che I_a sia infinito \Rightarrow esiste una collezione infinita di primi p.t.c. $p \mid a \Rightarrow p \leq a$ CONTRADDIZIONE
 L'esisterebbero infiniti primi $\leq a$

b) procediamo per induzione

$$a=1 \quad v_p(1)=0 \quad \forall p$$

$$1 = \prod_p p^0 = 1 \cdot 1 \cdot \dots \cdot 1 \cdot \dots = 1$$

supponiamo adesso $a > 1$

1) se a è primo, diciamo $a = q$

allora $a = \prod_p p^{v_p(a)}$ dove $v_p(a) = 0$ se $p \neq q$

$v_p(a) = 1$ se $p = q$

④

$$a=3 \quad v_p(3)=0 \quad \forall p \neq 3$$

$$v_3(3)=1$$

2) se a non è primo allora non è irriducibile $\Rightarrow a = u \cdot v$ con 1LULa 1LVLa

per ipotesi induttiva visto che $u, v < a$

posso scrivere

$$u = \prod_p p^{v_p(u)} \quad \left[\begin{array}{l} \\ \end{array} \right] \rightarrow a = u \cdot v = \prod_p p^{v_p(u)} \cdot \prod_p p^{v_p(v)}$$

$$v = \prod_p p^{v_p(v)}$$

es

$$\alpha = 1 \Rightarrow 1 = 1 \cdot \prod_p p^{v_p(1)} \quad v_p(1) = 0 \quad \forall p$$

$I_\alpha = \emptyset$

$$\alpha = 2 \Rightarrow 2 = (+1) \prod_p p^{v_p(2)} = 2 \cdot \prod_{p \neq 2} p^0$$

$$v_p(2) = 0 \text{ se } p \neq 2$$

$$v_2(2) = 1$$

$$\alpha = -1 \Rightarrow -1 = (-1) \prod_p p^0 \quad v_p(-1) = 0 \quad \forall p$$

$$\alpha = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 7^1 \cdot 5^1 \cdot 3^2 \cdot 2^4$$

$$r_p(7!) = \begin{cases} 1 & p=7 \\ 1 & p=5 \\ 2 & p=3 \\ 4 & p=2 \\ 0 & p>7 \end{cases} \quad I_\alpha = \{2, 3, 5, 7\}$$

proprietà

$$\alpha = \prod_p p^{v_p(\alpha)} \quad b = \prod_p p^{v_p(b)}$$

$$\alpha \cdot b = \prod_p p^{v_p(\alpha)} \cdot \prod_p p^{v_p(b)} = \prod_p p^{v_p(\alpha) + v_p(b)}$$

$$v(\alpha \cdot b) = v_p(\alpha) + v_p(b)$$

es

$$\begin{aligned} \alpha = 12 &= 2^2 \cdot 3 & b = 15 &= 3 \cdot 5 & v_2(\alpha \cdot b) &= 2 \\ v_2(\alpha) &= 2 & v_2(b) &= 0 & v_3(\alpha \cdot b) &= 2 \\ v_3(\alpha) &= 1 & v_3(b) &= 1 & v_5(\alpha \cdot b) &= 1 \\ v_5(\alpha) &= 0 & v_5(b) &= 1 & v_{p>5}(\alpha \cdot b) &= 0 \end{aligned}$$

$\forall \alpha > 0 \quad \exists m$ numero finito di numeri primi distinti: p_1, \dots, p_r t.c. $\alpha = p_1^{e_1} \cdots p_r^{e_r}$ e questa fattorizzazione è unicamente determinata

prop

$$\text{dati } a, b \in \mathbb{N}^* \quad a = \prod_p p^{v_p(a)} \quad b = \prod_p p^{v_p(b)}$$

$$a | b \Leftrightarrow \forall p, v_p(a) \leq v_p(b)$$

dim

$$\text{supponiamo } v_p(a) \leq v_p(b) \Rightarrow v_p(b) - v_p(a) \geq 0$$

$$\text{poniamo } K = \prod_p p^{v_p(b) - v_p(a)}$$

OSS $v_p(a) - v_p(b) = 0$ $\forall p$ abbastanza grande

$$K \cdot a = \prod_p p^{v_p(b) - v_p(a)} \cdot \prod_p p^{v_p(a)} = \prod_p p^{v_p(b) - v_p(a) + v_p(a)} = \prod_p p^{v_p(b)} = b$$

quindi: $b = K a$ $\exists K \in \mathbb{N}^*$ e quindi albo

supponiamo che $a | b \Rightarrow b = K a$ $\exists K \in \mathbb{N}^*$

applichiamo TFA

$$\prod_p p^{v_p(b)} = \prod_p p^{v_p(K)} \cdot \prod_p p^{v_p(a)} = \prod_p p^{v_p(K) + v_p(a)}$$

per unicità della fattorizzazione

$$v_p(b) = v_p(K) - v_p(a) \Rightarrow v_p(b) \geq v_p(a)$$



prop

$$\text{dati } a, b \in \mathbb{N}^* \quad MCD(a, b) = \prod_p p^{\min(v_p(a), v_p(b))}$$

dim

$S = MCD(a, b)$ è l'unico intero di \mathbb{N}^* t.c.

① $S | a$ e $S | b$

② $\forall d' \in \mathbb{N}^*$ t.c. $d' | a$ e $d' | b$ allora $d' | S$

$$a | b \Leftrightarrow \forall p \quad v_p(a) \leq v_p(b)$$

$$\begin{aligned} ① &\Leftrightarrow \forall p \quad [v_p(S) \leq v_p(a)] \quad \boxed{v_p(S) \leq \min(v_p(a), v_p(b))} \\ &\quad [v_p(S) \leq v_p(b)] \end{aligned}$$

$$\begin{aligned} ② &\Leftrightarrow \text{se } d' \text{ è tale che } \forall p \quad [v_p(d') \leq v_p(a)] \quad \boxed{v_p(d') \leq \min(v_p(a), v_p(b))} \\ &\quad [v_p(d') \leq v_p(b)] \end{aligned}$$

$$\text{allora } \forall p \quad v_p(d') \leq v_p(S)$$

quindi: $\forall p, v_p(S)$ è il più grande degli interi n t.c. $n \leq \min(v_p(a), v_p(b)) \Rightarrow v_p(S) = \min(v_p(a), v_p(b))$

Esercizio

$$a, b, c \in \mathbb{N}^* \quad MCD(ab, c) \mid MCD(a, c) \cdot MCD(b, c)$$

$$MCD(ab, c) = \prod_p p^{\min(v_p(ab), v_p(c))} = \prod_p p^{\min(v_p(a) + v_p(b), v_p(c))} = j$$

$$MCD(a, c) \cdot MCD(b, c) = \prod_p p^{\min(v_p(a), v_p(c))} \cdot \prod_p p^{\min(v_p(b), v_p(c))} = \prod_p p^{\min(v_p(a), v_p(c)) + \min(v_p(b), v_p(c))} = k$$

siano $x, y, z \in \mathbb{N}^*$ allora dimostriamo che $\min(x+y, z) \leq \min(x, z) + \min(y, z)$
abbiamo quattro casi:

$$\textcircled{1} \quad z \leq x \wedge z \leq y \quad \text{quindi } z \leq x+y$$

$$z = \min(x+y, z) \leq 2z = \min(x, z) + \min(y, z)$$

$$\textcircled{2} \quad x \leq y \leq z \quad \min(x, z) = x \quad \min(y, z) = y$$

$$x+y \geq \min(x+y, z)$$

$$\textcircled{3} \quad x \leq z \leq y \quad \min(x, z) + \min(y, z) = x+z \quad \text{e} \quad \min(x+y, z) = z$$

$$x+z \geq z$$

$$\textcircled{4} \quad y \leq z \leq x \quad \min(x, z) + \min(y, z) = z+y \quad \text{e} \quad \min(x+y, z) = z$$

$$z+y \geq z$$

quindi abbiamo dimostrato che $\min(x+y, z) \leq \min(x, z) + \min(y, z)$

quindi $\min(v_p(a) + v_p(b), v_p(c)) \leq \min(v_p(a), v_p(c)) + \min(v_p(b), v_p(c))$

qui



Divisori di zero DEF

dato A anello, $a \in A$ è divisore di zero se $\exists b \in A \setminus \{0\}$ t.c. $ab = 0_A$

es

$$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} \quad \bar{2} \cdot \bar{3} = \bar{0} \quad \text{ma } \bar{2}, \bar{3} \neq \bar{0}$$

dunque $\bar{0}, \bar{2}, \bar{3}$ sono tutti divisori di zero

se $A = K$ campo (es. $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ primo)
cioè $\forall a \in K \setminus \{0\}$ a è invertibile, ovvero $K^\times = K \setminus \{0\} = K^*$

l'unico divisore di 0 in K campo è 0

0_K

"

Supponiamo a divisore di zero allora $\exists b \in K^*$ t.c. $ab=0$
 $b \neq 0 \Rightarrow b$ invertibile $\exists b^{-1} \in K^*$ t.c. $b \cdot b^{-1} = 1$
 $ab=0 \Rightarrow a = ab \cdot b^{-1} = 0 \cdot b^{-1} = 0 \Rightarrow a=0$

in \mathbb{Z} se a è divisore di zero allora $a=0$ (anche se \mathbb{Z} non è un campo)

sia a divisore di zero $\Leftrightarrow \exists b \in \mathbb{Z}^*$ t.c. $ab=0$

a divisore di zero $\Leftrightarrow -a$ è divisore di zero

$$(-a)(-b) = ab = 0$$

Supponiamo $a \geq 0 \Rightarrow \exists b$ t.c. $ab=0$

$\frac{1}{0}$

$$0 = ab = \underbrace{b + b + \dots + b}_{a \text{ volte}} \geq 0 \quad b > 0$$

se $a > 0$ non è possibile quindi $a=0$



Dominio DEF

dato A un anello, $A \neq \{0\}$ si dice che A è un dominio se l'unico divisore di zero in A è 0
in particolare ogni campo è un dominio

\mathbb{Z} è un dominio

$\mathbb{Z}/6\mathbb{Z}$ non è un dominio

prop $\mathbb{Z}/n\mathbb{Z}$ è un dominio $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ è un campo $\Leftrightarrow n$ primo

dim

$\mathbb{Z}/n\mathbb{Z}$ è un dominio $\Leftrightarrow n$ primo

① sapendo che $\mathbb{Z}/n\mathbb{Z}$ è un dominio

Supponiamo per assurdo che n non sia primo, allora $\exists a, b \in \mathbb{Z}$ t.c. $n = ab$ con $a, b \neq n$
quindi $\bar{a}\bar{b} = \bar{n} = \bar{0}$ dunque $\bar{a} \cdot \bar{b} = \bar{0}$ CONTRADDIZIONE $\rightarrow \mathbb{Z}/n\mathbb{Z}$ non è un dominio

② sapendo n è primo

Supponiamo $\mathbb{Z}/n\mathbb{Z}$

Allora $\forall a, b \in \mathbb{Z}$ t.c. $n \mid ab \Rightarrow \bar{a} \cdot \bar{b} = \bar{n} = \bar{0}$ allora $n \mid a$ oppure $n \mid b$

dunque $a \neq 0$ oppure $b = 0$

$\mathbb{Z}/n\mathbb{Z}$ è un campo $\Leftrightarrow n$ è primo

① sapendo che $\mathbb{Z}/n\mathbb{Z}$ è un campo

supponiamo per assurdo che n non è primo allora $\exists a, b \in \mathbb{Z} \text{ s.t. } ab = n \wedge a, b \neq n \wedge a, b > 1$

quindi $\exists k \in \mathbb{Z} \text{ s.t. } ab = kn = 0$ CONTRADDIZIONE \rightarrow l'unico divisore di zero per un campo è 0.

② sapendo che n è un numero primo

supponiamo $\bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \bar{a} \neq 0$ allora $\text{MCD}(a, n) = 1$

???

se $a \in A$ non è divisore di zero (a divisore di zero $\Leftrightarrow \exists b \in A \setminus \{0\}$ t.c. $ab=0$) 22/10
dunque $\forall b \in A \setminus \{0\}$ $ab \neq 0$

LEMMA (legge di cancellazione) $a \in A$ non divisore di zero, allora se $ab=ac \Rightarrow b=c$
dim poiché a non è divisore di zero $\Rightarrow a \neq 0$
 $ab=ac \Leftrightarrow a(b-c)=0 \Rightarrow b-c=0 \Rightarrow b=c$

OSS questo implica la legge di cancellazione $A = \mathbb{Z}$

Risoluzione di equazioni in A ($A = \mathbb{Z}$, $A = \mathbb{Z}_{n \in \mathbb{Z}}$)

ci interessiamo a $aX=b$ $a, b \in A$
↑ indeterminata

es

$A = \mathbb{Z}$: $2X=3$. L'insieme delle soluzioni $\{x \in \mathbb{Z} \text{ t.c. } 2x=3\} = \emptyset$

infatti sia per assurdo x soluzione di $2X=3$, allora questo vorrebbe dire $2/3$ che è impossibile

$2X=6$ $\{x \in \mathbb{Z} \text{ t.c. } 2x=6\} = \{3\}$
osserviamo infatti: (TFA) $6=2 \cdot 3$ quindi $2x=2 \cdot 3$ quindi $x=3$ \rightarrow cancellazione

In generale una soluzione di $aX=b$ ($A = \mathbb{Z}$) esiste $\Leftrightarrow a|b$. Infatti se l'insieme delle soluzioni è $\neq \emptyset$, e se x è soluzione, si ha $aX=b \Leftrightarrow a|x$.

Se $a|b$ allora $\exists k \in \mathbb{Z}$ t.c. $b=ak$ e posso prendere $x=k$

Adesso ci interessiamo al caso $A = \mathbb{Z}_{n \in \mathbb{N}^*}$ $aX=b$

Nel caso in cui A è qualsiasi e $a \in A^\times$ di inversa a^{-1}

$$\underline{\underline{a^{-1}} a X = a^{-1} b} \Rightarrow X = a^{-1} b$$

l'equazione $X = a^{-1} b$ ha l'unica soluzione $x = a^{-1} b$

se per esempio $A = K$ campo ($\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ p primo) l'equazione $aX=b$, con $a \neq 0$, ammette l'unica soluzione $x = a^{-1} b$

prop

dato $A = \frac{\mathbb{Z}}{n\mathbb{Z}}$ con $a, b \in A$ $aX = b$ ammette soluzioni $\Leftrightarrow a = \bar{a}, b = \bar{b}$ ($a, b \in \mathbb{Z}$) allora $\text{MCD}(a, n) \mid b$

dim

$$\Rightarrow ax \equiv b \pmod{n} \Leftrightarrow n \mid ax - b \Leftrightarrow ax - b \in n\mathbb{Z}$$

$$\begin{aligned} \text{sia } \bar{x} \text{ soluzione } \bar{a}\bar{x} = \bar{b} &\Leftrightarrow ax - b \in n\mathbb{Z} \Leftrightarrow ax - b = nk \quad \exists k \in \mathbb{Z} \Leftrightarrow \\ &\Leftrightarrow ax - nk = b \Rightarrow b \in a\mathbb{Z} + n\mathbb{Z} = s\mathbb{Z} \\ \delta = \text{MCD}(a, n) &\Leftrightarrow \delta \mid b \quad \text{DIMOSTRATO} \Rightarrow \end{aligned}$$

supponiamo adesso che $\delta = \text{MCD}(a, n) \mid b$ allora $b = \delta x \Rightarrow b \in a\mathbb{Z} + n\mathbb{Z} \Leftrightarrow$
 $\Leftrightarrow \exists u, v \in \mathbb{Z}$ t.c. $b = ua + vn \Leftrightarrow b - ua = vn \Leftrightarrow b \equiv ua \pmod{n} \Leftrightarrow \bar{b} = \bar{u}\bar{a}$ DIMOSTRATO \leftarrow



es

$$\bar{3} \cdot \bar{X} = \bar{0} \text{ in } A = \frac{\mathbb{Z}}{6\mathbb{Z}}$$

$$a=3 \quad b=0 \quad n=6 \quad \text{MCD}(a, n)=3 \quad \text{e } 3 \mid 0 = b \Rightarrow \text{ci sono soluzioni}$$

$x = \bar{2}$ è soluzione

$$x = \bar{4} \text{ è soluzione } \bar{3} \cdot \bar{4} = (\bar{3} \cdot \bar{2}) \cdot \bar{2} = \bar{0} \cdot \bar{2} = \bar{0}$$

$$x = \bar{0} \text{ è soluzione } \bar{3} \cdot \bar{0} = \bar{0}$$

l'insieme delle soluzioni è $\{\bar{0}, \bar{2}, \bar{4}\} \subseteq A$ infatti:

$x = \bar{1}$ non è soluzione

$$x = \bar{3} \text{ non è soluzione } \bar{3} \cdot \bar{3} = \bar{3}$$

$$x = \bar{5} \text{ non è soluzione } \bar{3} \cdot \bar{5} = \bar{3}$$

LEMMA $a, b, c \in \mathbb{Z}$ $a, b \neq 0$ e $\text{MCD}(a, b) = 1$ allora $ab \mid c$

dim

$$a, b \mid c \Leftrightarrow c = ak = bh \quad (\exists k, h \in \mathbb{Z}) \Rightarrow ab \mid c \Leftrightarrow ab \mid ak \Leftrightarrow ab \mid bh \quad (\Rightarrow ab \mid c) \rightarrow$$

infatti $\text{MCD}(a, b) = 1 \Leftrightarrow b$ è invertibile modulo a ($bb^{-1} \equiv 1 \pmod{a}$) \Leftrightarrow

$$\Leftrightarrow \exists b' \text{ t.c. } bb' \in 1 + a\mathbb{Z}$$

$$\begin{aligned} a \mid bh &\Rightarrow ab \mid bb'h = (1+ak)h \Leftrightarrow ab' = h + ahk \Leftrightarrow a(b' - hk) = h \Rightarrow \\ &\Rightarrow ab' \equiv 1 \pmod{a} \quad \text{Bézout} \Rightarrow aa' + bb' = 1 \\ &\Rightarrow bb' - 1 = -xa \end{aligned}$$

Teorema cinese dei resti

$r_1, \dots, r_s \in \mathbb{N}^*$ supponiamo che $\text{MCD}(r_i, r_j) = 1 \quad \forall i \neq j$ consideriamo inoltre $c_1, \dots, c_s \in \mathbb{Z}$
Allora il sistema

$$(*) \left\{ \begin{array}{l} X \equiv c_1 \pmod{r_1} \\ X \equiv c_2 \pmod{r_2} \\ \vdots \\ X \equiv c_s \pmod{r_s} \end{array} \right.$$

abbiamo s equazioni congruenze

ha un'unica soluzione mod $R := r_1 \dots r_s$

Ovvero l'insieme $E = \{x \text{ soluzione in } \mathbb{Z} \text{ di } (*)\}$ è della forma $x_0 + \mathbb{Z}R$

dim

Calcoliamo una soluzione particolare x_0 di $(*)$. Poniamo inoltre $R_i := \frac{R}{r_i} = r_1 \dots \check{r}_i \dots r_s = r_1 \dots r_{i-1} r_{i+1} \dots r_s$

$$\Rightarrow R = r_1 \dots r_s$$

non c'è

OSS $\text{MCD}(R_i, r_i) = 1$

Questa proprietà può essere riformulata dicendo che \bar{R}_i classe di R_i in $\mathbb{Z}_{r_i} \mathbb{Z}$ è invertibile, ovvero $\exists \bar{S}_i \in \mathbb{Z}_{r_i} \mathbb{Z}$ t.c. $\bar{R}_i \cdot \bar{S}_i = \bar{1}$ (classe inversa) \Rightarrow

$\Rightarrow \bar{R}_i \cdot \bar{S}_i \cdot \bar{c}_i = \bar{c}_i$ abbiamo costruito elementi y_1, \dots, y_s ciascuno in $\mathbb{Z}_{r_i} \mathbb{Z}$
 $= \bar{y}_i \in \mathbb{Z}_{r_i} \mathbb{Z}$

Dimostriamo che $x_0 = \sum_{i=1}^s y_i R_i$ è la soluzione $(*)$

infatti se $i \neq j$ $r_i | R_j$ $\equiv 0 \pmod{r_i}$

Quindi $x_0 = \sum_{j=1}^s y_j R_j = \sum_{\substack{j=1 \\ j \neq i}}^s y_j R_j + y_i R_i \equiv y_i R_i \pmod{r_i} \equiv c_i \pmod{r_i}$ ed è valido $\forall i = 1, \dots, s$

dunque $x_0 = \sum_{j=1}^s y_j R_j$ è una soluzione particolare del nostro sistema $(*)$

Sistema omogeneo associato

$$\left\{ \begin{array}{l} X \equiv 0 \pmod{r_1} \\ X \equiv 0 \pmod{r_2} \\ \vdots \\ X \equiv 0 \pmod{r_s} \end{array} \right. \quad (*)_H \quad X \equiv 0 \pmod{r_i} \quad i = 1, \dots, s$$

$$X \equiv 0 \pmod{r_1} \Leftrightarrow r_1 | x$$

$$X \equiv 0 \pmod{r_2} \Leftrightarrow r_2 | x \text{ ma } r_1, r_2 \text{ sono primi tra loro} \Rightarrow r_1 r_2 \mid x$$

$$X \equiv 0 \pmod{r_3} \Leftrightarrow r_3 | x \text{ ma } \text{MCD}(r_3, r_1, r_2) = 1 \Rightarrow r_1 r_2 r_3 | x$$

iterando ottengo che $R := r_1 \dots r_s | x$

Quindi l'insieme delle soluzioni di $(*)_H$ è $\mathcal{E}_H := R\mathbb{Z}$

prop

l'insieme delle soluzioni di $(*)$, \mathcal{E}_* , è dato da $x_0 + R\mathbb{Z}$

dim

$$\mathcal{E}_* \supseteq x_0 + R\mathbb{Z}$$

se $x \in x_0 + R\mathbb{Z}$ allora posso scrivere $x = x_0 + Rk \quad \exists k \in \mathbb{Z}$ ma $Rk \equiv 0 \pmod{r_i} \quad \forall i=1, \dots, s$ ($r_i | Rk$)
aggiungendo con x_0 , che è soluzione particolare ottengo $x \equiv c_i + 0 \equiv c_i \pmod{r_i}$

$$\mathcal{E}_* \subset x_0 + R\mathbb{Z}$$

sia x una soluzione di $(*)$

Allora $x - x_0 \equiv 0 \pmod{r_i} \quad \forall i=1, \dots, s \Rightarrow x - x_0 \in R\mathbb{Z}$ (lemma)

$$\Rightarrow x \in x_0 + R\mathbb{Z} \Rightarrow \mathcal{E}_* \subset x_0 + R\mathbb{Z}$$



Esercizio

Trovare X delle seguenti equazioni in $\mathbb{Z}/n\mathbb{Z}$

$$\textcircled{1} \quad 4x \equiv 7 \pmod{15}$$

$$\textcircled{2} \quad 6x \equiv 8 \pmod{9}$$

$$\textcircled{3} \quad \begin{cases} 1025x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases}$$

$$\textcircled{1} \quad 4x \equiv 7 \pmod{15}$$

$\text{MCD}(4, 15) = 1 \Leftrightarrow 4 \text{ è invertibile} \Leftrightarrow \exists n \in \mathbb{N} \text{ t.c. } 4n \equiv 1 \pmod{15} \text{ (es. } n=4)$

moltiplico per 4

congruenza è equivalente

$$\frac{4 \cdot 4 \cdot x}{\equiv 1} \equiv 28 \pmod{15}$$

alla congruenza iniziale

$$x \equiv 13 \pmod{15}$$

insieme delle soluzioni: $\Sigma = 15\mathbb{Z} + 13$

$$\textcircled{2} \quad 6x \equiv 8 \pmod{9} \Leftrightarrow 9k = 6x - 8 \Leftrightarrow 8 = 6x - 9k \Rightarrow 8 = 3(2x - 3k) \Rightarrow 3 \mid 8 \text{ impossibile}$$

$$\Sigma = \emptyset$$

$$\textcircled{3} \quad \begin{cases} 1025x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases} \quad \left. \begin{array}{l} r_1 = 8 \\ r_2 = 5 \\ r_3 = 3 \end{array} \right\} \rightarrow \text{sono a 2 a 2 primi fra loro}$$

$$1025 = 2^{\frac{10}{3}} + 1 = \overline{(2^3)^3} \cdot 2 + 1 \equiv 1 \pmod{8}$$

$$36 = 3^2 \cdot 4 \equiv 1 \pmod{5}$$

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

$$5312065$$

$$8 \mid 4 \cdot 10^6 \Rightarrow 5312065 \equiv 1312065 \pmod{8}$$

$$8 \mid 1200000 \Rightarrow 1312065 \equiv 112065 \pmod{8}$$

$$8 \mid 120000 \Rightarrow 112065 \equiv -7935 \pmod{8}$$

$$8 \mid 8000 \Rightarrow -7935 \equiv 65 \equiv 1 \pmod{8}$$

$$322 \equiv -3 \equiv 2 \pmod{5}$$

$$7 \equiv 1 \pmod{3}$$

$$\begin{cases} x \equiv 1 \pmod{8} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{3} \end{cases}$$

ci:

$$R = 8 \cdot 5 \cdot 3 = 120$$

$$\begin{aligned} R_1 &= r_2 \cdot r_3 = 15 \\ R_2 &= r_1 \cdot r_3 = 24 \\ R_3 &= r_1 \cdot r_2 = 40 \end{aligned}$$

faccio le inversioni congruenziali

R_1 invertibile modulo r_1

$$s_1 = 7 \quad \bar{7} \cdot \bar{15} = \bar{1} \pmod{8}$$

R_2 invertibile modulo r_2

$$s_2 = 4 \quad \bar{4} \cdot \bar{24} = \bar{1} \pmod{5}$$

R_3 invertibile modulo r_3

$$s_3 = 1 \quad \bar{1} \cdot \bar{40} = \bar{1} \pmod{3}$$

i	S_i	c_i	y_i
1	7	1	7
2	4	2	8
3	1	1	1

$x_0 = \sum_{i=1}^3 y_i R_i = 7 \cdot 15 + 8 \cdot 24 + 40 \cdot 1 = 217$

soluzione generale

$$E = x_0 + R\mathbb{Z} = 217 + 120\mathbb{Z} = 97 + 120\mathbb{Z}$$

Polinomi in una indeterminata a coefficiente in un campo

$$K = \mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

un polinomio in X a coefficiente in K

$$P = \sum_{i=0}^n a_i X^i$$

$a_i \in K \Rightarrow i$ coefficiente

$n \rightarrow$ un intero che dipende dal polinomio

es)

$$K = \mathbb{R} \quad 0 \quad a_i = 0 \quad \forall i$$

$$1 = 1 \cdot x^0$$

$$x = 1 \cdot x^1$$

$$K \in \mathbb{R} \quad 3x^3 + 2x + 1$$

$$\begin{aligned} K &= \mathbb{F}_2 \quad \bar{1}x^5 + \bar{0}x^4 + \bar{2}x^3 + \bar{6}x^2 + \bar{1}x + \bar{1} \\ &= x^5 + x + \bar{1} \end{aligned}$$

$A = K[x]$ è l'insieme dei polinomi (ogni $P \in A$)

$$P = \sum_{i \geq 0} a_i X^i \quad a_i = 0 \quad \forall i > 0 \quad \text{abbastanza grande}$$

c'è una struttura di anello, definiamo quindi le operazioni

$$P = \sum_{i \geq 0} a_i X^i \quad a_i = 0 \quad \forall i > 0$$

$$Q = \sum_{i \geq 0} b_i X^i \quad b_i = 0 \quad \forall i > 0$$

Somma

$$P + Q := \sum_{i \geq 0} (a_i + b_i) X^i$$

moltiplicazione

$$P \cdot Q := \sum_{K \geq 0} c_K X^K \quad \text{dove } c_K = \sum_{i+j=K} a_i b_j \quad \text{e si vede che } c_K = 0 \quad \forall K > 0$$

(es)

$$(x^3 + 5x + 1) + (x^2 + 2) = x^3 + x^2 + 5x + 3 \quad \text{somma}$$

$$(x^2 + 1)(x + 1) = x(x^2 + 1) + 1(x^2 + 1) = x^3 + x + x^2 + 1 = x^3 + x^2 + x + 1 \quad \text{moltiplicazione}$$

$$(x^3 - 2x^2 + x - 1)(-3x^5 + x^3 + x)$$

$$\begin{array}{r} x \quad x^2 \quad -3x^5 \\ \times x^7 \quad x^8 \quad x^9 \quad -3x^{12} \\ \hline -2x^3 \quad -2x^4 \quad -2x^5 \quad 6x^8 \quad -3x^{12} + x^9 \dots \\ x \quad x^2 \quad x^3 \quad -3x^6 \\ \hline -1 \quad -x \quad -x^2 \quad 3x^5 \end{array} \quad \begin{matrix} \nearrow \text{addizione} \\ \text{Cauchy} \end{matrix}$$

quindi $(A, -, +, \cdot, 0, 1)$ è un anello

Grado di un polinomio

$$P \in A[x]$$

$$P = \sum_{i \geq 0} a_i X^i \quad a_i = 0 \quad \forall i > 0 \quad P \neq 0 \quad \{j \in \mathbb{N} \text{ t.c. } a_j \neq 0\} \text{ è finito non vuoto (ammette max e min)}$$

$$\deg(P) = \max \{j \in \mathbb{N}, a_j \neq 0\}$$

grado di P

si pone $\deg(0) := -\infty$, dunque l'insieme di gradi $\mathbb{N} \cup \{-\infty\}$

$\{P \in K[x] \text{ t.c. } \deg(P) = 0\} = K^*$

$\hookrightarrow 0 \text{ non invertibile}$

$\deg: \frac{K[x]}{A} \longrightarrow \mathbb{N} \cup \{-\infty\}$

Lemma

dati $a, b \in A$

① $\deg(a) = -\infty \iff a = 0$

② $\deg(ab) = \deg(a) + \deg(b)$

③ $\deg(a+b) \leq \max(\deg(a), \deg(b))$

④ $\deg(a+b) = \max(\deg(a), \deg(b)) \iff \deg(a) \neq \deg(b)$

(es)

$$\begin{array}{l} a = x^2 + x + 1 \quad \deg 2 \\ b = x + 1 \quad \deg 1 \end{array} \longrightarrow a+b = x^2 + 2x + 2 \quad \deg(a+b) = \max(2, 1)$$

$$\begin{array}{l} a = x^5 + 6x - 3 \quad \deg 5 \\ b = -x^5 + 4x^2 + 2x - 1 \quad \deg 5 \end{array} \longrightarrow a+b = 4x^2 + 8x - 4 \quad \deg(a+b) = 2 < \max(5, 5)$$

oss può capitare $\deg(a) = \deg(b) = d$ e $\deg(a+b) = d$

Analogia tra interi e polinomi (valore assoluto e grado)

24/10

$$\mathbb{Z}, A = K[X]$$

↪ campo

$$\mathbb{Z} \xrightarrow{1.1} \mathbb{N}$$

$$a \mapsto \begin{cases} a & a \geq 0 \\ -a & a \leq 0 \end{cases}$$

$$\textcircled{1} |a| = 0 \Leftrightarrow a = 0$$

$$\textcircled{2} |ab| = |a||b|$$

$$\textcircled{3} |a+b| \leq |a| + |b|$$

↪ disegualanza triangolare

$$A \xrightarrow{\deg} \mathbb{N} \cup \{-\infty\}$$

$$\textcircled{1} \deg(a) = -\infty \Leftrightarrow a = 0$$

$$\textcircled{2} \deg(ab) = \deg(a) + \deg(b)$$

$$\textcircled{3} \deg(a+b) \leq \max(\deg(a), \deg(b))$$

vogliamo avere una struttura simile a $\mathbb{I} \cdot \mathbb{I}$ e \mathbb{P} per poter dare $\mathbb{I} \cdot \mathbb{I}$ a \mathbb{P}

Definiamo $P \in A \setminus \{0\}$ e scegliamo $c > 1$

$$|P|_c := c^{\deg(P)} \rightarrow \text{dipende da } c$$

$$|0|_c := 0 = c^\infty$$

allora $\textcircled{1} \textcircled{2} \textcircled{3}$ sono equivalenti a:

$$\textcircled{1} |a|_c = 0 \Leftrightarrow a = 0$$

$$\textcircled{2} |ab|_c = |a|_c \cdot |b|_c$$

$$|ab|_c = c^{\deg(ab)} = c^{\deg(a)} \cdot c^{\deg(b)} = |a|_c \cdot |b|_c$$

$$\textcircled{3} |a+b|_c \leq \max(|a|_c, |b|_c) \leq |a|_c + |b|_c$$

$$|a+b|_c = c^{\deg(a+b)} \leq c^{\max(\deg(a), \deg(b))} = \max(|a|_c, |b|_c)$$

Algoritmo della divisione. TEOREMA

$a, b \in A = K[X]$ con $(a, b) \neq (0, 0)$ allora esiste unica $(q, r) \in A \times A$ t.c. $a = qb+r$ dove $\deg(r) < \deg(b)$ equivalente $|r|_c < |b|_c$

divisione in colonne

$$\begin{array}{rcl} a = x^4 + x + 1 & x^4 & x + 1 & x^3 - 2 \\ b = x^3 - 2 & x^4 & -2x & x \\ \hline // & 3x + 1 & & 9 \\ & r & & \end{array}$$

Analogie

\mathbb{Z}	$A = K[X]$
intere 1.1	polinomi 1.1c, deg
\mathbb{N}^*	$A^t = \{\text{polinomi monici}\} \Rightarrow P = a_0 + a_1 X + \dots + a_n X^n \quad a_n \neq 0 \quad \begin{pmatrix} x^2+1 & \checkmark \\ x & \checkmark \\ 1 & \checkmark \\ -x+3 & \times \end{pmatrix}$ il prodotto di due monici ma nella somma si perde l'analogia
	$A^x = K^x$ $a, b \in A^x \quad \exists c \in A^x \text{ t.c. } ab = 1 \Rightarrow \deg(a) + \deg(b) = 0 \Rightarrow$ $\Rightarrow \deg(a), \deg(b) \in \mathbb{N} \Rightarrow$ $\Rightarrow \deg(a) = \deg(b) = 0 \Rightarrow a, b \in K^x$
divisibilità in \mathbb{Z} $a b \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } b = ak \Leftrightarrow b \in a\mathbb{Z} \Leftrightarrow b \mid a$	divisibilità in A $a b \Leftrightarrow \exists h \in A \text{ t.c. } b = ah \Leftrightarrow b \in aA \Leftrightarrow b \mid a$
$a, b \in \mathbb{Z}$ $a' = ba^{-1} \in \mathbb{Z}$ $a', b' \in \{1, -1\} \Rightarrow \{a, -a\} = \{b, -b\}$	proprietà di \mid su A <ul style="list-style-type: none"> • riflessiva • transitiva $x y z \Leftrightarrow z \in A \cap A \subset A \Rightarrow z \in A \subset A \Leftrightarrow x z$
$a b \wedge b a \Rightarrow b = aa', a = bb'$ $\exists a', b' \in \mathbb{Z} \quad b = bb'a' \Rightarrow 1 = a'b' \Rightarrow$ $a', b' \in \{1, -1\} \Rightarrow \{a, -a\} = \{b, -b\}$	$a, b \in A$ supponiamo che $a b \wedge b a \Rightarrow \exists u, v \in A \text{ t.c. } b = au$ $\exists v \in A \text{ t.c. } a = bv \Rightarrow a = uv \Rightarrow$ $\Rightarrow \deg(a) = \deg(u) + \deg(v) + \deg(a)$ identità in \mathbb{N} \Leftrightarrow $\Leftrightarrow \deg(u) + \deg(v) = 0 \Leftrightarrow \deg(u) = \deg(v) = 0 \Leftrightarrow$ $\Leftrightarrow u = \lambda \in K^x \wedge v = \mu \in K^x$ ho quindi dimostrato che esiste $\lambda \in K^x = A^x$ t.c. $b = \lambda a$ questa operazione è analoga alla proprietà in \mathbb{Z} a, b t.c. $a b \wedge b a$ allora $\exists \lambda \in \mathbb{Z}^x$ t.c. $b = \lambda a$
un anello si dice dominio se l'unico divisore di 0 è 0 stesso	Lemma $A = K[X]$ è un dominio di intero <u>dim</u> sia $P \in A$ un divisore di zero. $\exists Q \in A \setminus \{0\}$ t.c. $PQ = 0 \Rightarrow$ $\Rightarrow \deg(PQ) = \deg(P) + \deg(Q) = -\infty \Rightarrow \deg(P) = -\infty \Rightarrow P = 0$
$a \equiv b \pmod{n} \Leftrightarrow n a - b$	$a, b \in A \setminus \{0\}$ $a \equiv b \pmod{A}$ transitività $a \equiv b \pmod{H} \wedge b \equiv c \pmod{H} \Leftrightarrow H \mid a - b \wedge H \mid b - c \Leftrightarrow$

$$\Leftrightarrow a-b=hu \exists u \in A \wedge b-c=hv \exists v \in A \Leftrightarrow$$

addizione termine
e termine

$$a-b+b-c=h(u+v) \Leftrightarrow a-c=h(u+v) \Leftrightarrow$$

$$a \equiv c \pmod{H}$$

$\mathbb{Z}/n\mathbb{Z}$ anello commutativo unitario

$$a \in \mathbb{Z} \quad \bar{a} := a + n\mathbb{Z}$$

A/H anello commutativo unitario

$$a \in A \quad \bar{a} := a + HA \subset A$$

$$A/H = \{\bar{a} \text{ t.c. } a \in A\} = \{a + HA \text{ t.c. } a \in A \text{ t.c. } \deg(a) < \deg(H)\}$$

$\{a \in A \text{ t.c. } \deg(a) < \deg(H)\}$ è un SCR per $\equiv \pmod{H}$

Massimo comun divisore

$$a, b \in A \text{ poniamo } aA + bA = \{m \in A \text{ t.c. } \exists u, v \in A \text{ con } m = ua + vb\}$$

Lemma $a, b \in A \quad (a, b) = (0, 0) \quad aA + bA = SA \quad \exists! S \in A^+$

dim

poniamo $E = aA + bA$ e $E^+ = \{m \in E \text{ t.c. } m \in A^+\}$

per il principio del minimo E^+ contiene un elemento di grado minima che è unico

poniamo $e_0 = \min(\deg(E^+))$ ben definito in A^+

claim esiste un unico elemento $d \in E^+$, t.c. $\deg(d) = e_0$.

infatti, sia $d' \in E^+$ con $\deg(d') = e_0$

$$d = d_0 + d_1x + \dots + d_{e_0-1}x^{e_0-1} + x^{e_0}$$

$$d' = d'_0 + d'_1x + \dots + d'_{e_0-1}x^{e_0-1} + x^{e_0}$$

$d - d' \in E$ ha grado $\leq e_0$.

$$\text{Se } d - d' \neq 0 \Rightarrow d - d' = d_0'' + d_1''x + \dots + d_{e_0-1}''x^{e_0-1} + x^{e_0} \Rightarrow \deg(d - d') \leq e_0$$

calcoliamo

$$d_e''(d - d') = (d_e'')^{-1}d_0'' + (d_e'')^{-1}d_1''x + \dots + \underbrace{(d_e'')^{-1}d_{e_0-1}''x^{e_0-1}}_1 + x^{e_0} \in E^+$$

$$\deg(d_e''(d - d')) = e < e_0 = \min(\deg(E^+))$$

contraddizione

Si pone $S = d$

$$(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$$

$$(a, b) \in A^2 \setminus \{(0, 0)\}$$

prop

$$\exists! d \in A^+$$

$\exists! d \in \mathbb{N}^*$

① $d \mid a \wedge d \mid b$	① $d \mid a \wedge d \mid b$
② se $d' \in \mathbb{Z}$ t.c. $d' \mid a \wedge d' \mid b$ allora $d' \mid b$	② se $d' \in A$ t.c. $d' \mid a \wedge d' \mid b$ allora $d' \mid b$
$\text{MCD}(a,b) = d = 8$	$\text{MCD}(a,b) = d = 8$
Si dice che $a, b \in \mathbb{Z}$ sono primi tra loro se $\text{MCD}(a,b) = 1$	Si dice che $a, b \in A$ sono primi tra loro se $\text{MCD}(a,b) = 1$
<u>DEF</u>	<u>DEF</u>
$a \in \mathbb{Z} \setminus \{0\}$ è detto irriducibile se $\forall b, c \in \mathbb{Z}, a = bc$ allora $b \in \mathbb{Z}^{\times}$ o $c \in \mathbb{Z}^{\times}$	$P \in A \setminus A^{\times}$ ($\deg(P) > 0$) P è irriducibile se scrivendo $P = QR$ si ha o $Q \in K^{\times}$ oppure $R \in K^{\times}$
<u>DEF</u>	<u>DEF</u>
$a \in \mathbb{Z} \setminus \{0\}$ è primo se $\forall b, c \in \mathbb{Z}$ se $a \mid bc$ allora $a \mid b$ oppure $a \mid c$	$P \in A \setminus A^{\times}$ ($\deg(P) > 0$) P è primo se $P \mid QR$ o $P \mid Q$ oppure $P \mid R$
<u>Lema</u> a irriducibile \Leftrightarrow a primo	<u>Lema</u> P irriducibile \Leftrightarrow P primo
	$A/\langle P \rangle$ con P irriducibile è un campo

Teorema di fattorizzazione unica per i polinomi

Ogni $H \in A \setminus \{0\}$ si decomponete in modo unico come prodotto

$$H = \lambda \prod_{\substack{P \in A \\ \text{irr}}} p^{v_p(H)}$$

> irr monico

dove $v_p(H) \in \mathbb{N}$ e $\{P \text{ t.c. } v_p(H) \neq 0\}$ è un insieme finito

(es)

$$H(x) = 2x^4 - 2x^3 + 4x^2 - 8x = 2x(x^3 - x^2 + 2x - 4) = 2x(x-2)(x^2+2) = 2 \cdot x^2 \cdot (x-2)^1 \cdot (x^2+2)^1$$

$$\lambda = 2$$

polinomi irriducibili: x , $x-2$, x^2+2 e gli esponenti sono tutti 1

Il problema della fattorizzazione in $A = K[x]$

$K = \mathbb{R}, \mathbb{C} \rightarrow$ fattorizzazione "facile". È infatti facile caratterizzare i polinomi irriducibili in $\mathbb{C}[x]$. I polinomi monici e irriducibili sono tutti i polinomi $X - \alpha$ t.c. $\alpha \in \mathbb{C}$

$K = \mathbb{R}[x] \rightarrow$ se P è monico e irriducibile si ha una delle seguenti opzioni

$$\textcircled{1} \quad \deg(P) = 1 \quad (P = X - \alpha \text{ t.c. } \alpha \in \mathbb{R})$$

$$\textcircled{2} \quad \deg(P) = 2 \text{ con } P = X^2 + aX + b \text{ con } \Delta = a^2 - 4b < 0$$

$K = \mathbb{F}_p, \mathbb{Q} \rightarrow$ fattorizzazione "difficile"

Valutazione

$x \in K, F \in K[X]$ con $F = F_0 + F_1 X + \dots + F_n X^n$

la valutazione di F in x è

$$ev_x(F) := F_0 + F_1 x + \dots + F_n x^n \quad ev_x: K[X] \longrightarrow K$$

↪ morfismo di anelli

OSS ① $ev_x(F+G) = ev_x(F) + ev_x(G)$

② $ev_x(F \cdot G) = ev_x(F) \cdot ev_x(G)$

③ $\forall \lambda \in K \quad ev_x(\lambda) = \lambda$

↪ uso K e non K^* dato che 0 è costante ma non invertibile

es

$$F = X^2 + 1 \in \mathbb{R}[X] \quad x=1$$

$$ev_x(F) = 1^2 + 1 = 2$$

$K[X]$

Lemma sia $x \in K$ allora $ev_x^{-1}(\{0\}) = \{P \in A \text{ t.c. } ev_x(P) = 0\} = (X-x)A$

dim

→

sia $Q = (X-x)H$

$$ev_x(Q) = ev_x(X-x)ev_x(H) = 0 \Rightarrow Q \in ev_x^{-1}(\{0\})$$

$$X-x=0$$

c

sia $P \in A$ t.c. $ev_x(P) = 0$

applichiamo algoritmo della divisione euclidea per $X-x$

$\exists (q, r) \in A \times A$ unica t.c. $P = q(X-x) + r$ e $\deg(r) \in \{-\infty, 0\} \Leftrightarrow r \in K$

$ev_x(P) = ev_x(q(X-x) + r) = ev_x(q)ev_x(X-x) + ev_x(r) \stackrel{X-x=0}{=} ev_x(r) \Rightarrow r = ev_x(P) = 0 \Rightarrow X-x | P \Leftrightarrow P \in (X-x)A$

$\Rightarrow 0 = 0$



Si dice quindi che P ha una **radice** in $x \Leftrightarrow X-x | P$ ($ev_x(P) = 0$, quindi $R = \{x \in K \mid (x, 0) \in \Gamma\}$)

OSS $X-x$ è irriducibile $\forall x \in K \Rightarrow X-x = U \cdot V \Rightarrow \deg(X-x) = \deg(U) + \deg(V) \Rightarrow$
 $\Rightarrow \{\deg(U), \deg(V)\} = \{0, 1\} \Rightarrow \{U, V\} \cap A^x = \emptyset$

Esercizi:

Esercizio 1 Fattorizzare i seguenti polinomi. (i) $X^2 + X + 6$ in $\mathbb{R}[X]$ (ii) $X^3 - 6X^2 + 11X - 6$ in $\mathbb{R}[X]$ (iii) $X^2 - 2X + 2$ in $\mathbb{C}[X]$ (iv) $X^3 - 1$ in $\mathbb{R}[X]$, $\mathbb{C}[X]$ (v) $X^n - 1$ in $\mathbb{R}[X]$, $\mathbb{C}[X]$ ($n = 4, 5, 6$). (vi) $X^4 - 10X^2 + 1$ in $\mathbb{Q}[X]$, $\mathbb{R}[X]$.

$$1) \Delta(aX^2+bX+c) = b^2 - 4ac \Rightarrow 1-24=-23 < 0$$

essendo $\Delta < 0$ è irriducibile

$$\forall x \in \mathbb{R} \quad v_x(X^2 + X + 6) \neq 0 \Rightarrow \text{nessuna radice reale}$$

il polinomio $X^2 + X + 6$ è irriducibile in $\mathbb{R}[X] \Rightarrow$ la sua fattorizzazione è " $X^2 + X + 6$ "

OSS un polinomio in $\mathbb{R}[X]$ con $\Delta < 0$ è irriducibile

2) faccio tentativi finché non trovo una radice del polinomio
 $v_x(X^3 - 6X^2 + 11X - 6) = 12 - 6 - 6 = 0 \Leftrightarrow X-1 | X^3 - 6X^2 + 11X - 6$

$$\begin{array}{c|cc} X^3 - 6X^2 + 11X - 6 & X-1 \\ \hline X^3 - X^2 & X^2 - 5X + 6 \Rightarrow \Delta = 25 - 24 = 1 > 0 \\ // -5X^2 + 11X - 6 & \text{quindi } x_{1/2} = \frac{5 \pm \sqrt{\Delta}}{2} = \frac{5 \pm 1}{2} \\ -5X^2 + 5X & \\ \hline // 6X - 6 & \text{allora si ha} \\ 6X - 6 & X^2 - 5X + 6 = (X-3)(X-2) \\ \hline // 0 & \end{array}$$

é un resto escludo
(non ho X)

$$P = X^3 - 6X^2 + 11X - 6 = (X^2 - 5X + 6)(X-1) = (X-3)(X-2)(X-1)$$

metodo attenitivo

si comincia facendo "qualche tentativo" di valutazione

$$v_{x-1}(F) = 0 \Leftrightarrow v_{x-1}(F) > 0 \Leftrightarrow X-1 | F$$

$$v_{x-2}(F) = 0 \Leftrightarrow v_{x-2}(F) > 0 \Leftrightarrow X-2 | F$$

$$v_{x-3}(F) = 0 \Leftrightarrow v_{x-3}(F) > 0 \Leftrightarrow X-3 | F$$

$X-1, X-2, X-3$ sono monici (irriducibili) distinti sono quindi a 2 a 2 coprimi $\Rightarrow (X-1)(X-2)(X-3) | F$

$$F = \lambda \prod_p v_p(F) \Rightarrow v_{x-1}(F) = 1 \quad v_{x-2}(F) = 1 \quad v_{x-3}(F) = 1$$

$$\text{quindi } F = (X-1)(X-2)(X-3)$$

$$3) F = X^2 - 2X + 2 \in \mathbb{R}[X] \subset \mathbb{C}[X] \quad \mathbb{C} = \{x+iy \text{ t.c. } x, y \in \mathbb{R}\} \text{ i.e. } \sqrt{-1} \text{ ovvero } i^2 = -1$$

vogliamo fattorizzare in $\mathbb{C}[X]$

$$\Delta = 4 - 8 = -4 < 0 \rightarrow \text{irriducibile in } \mathbb{R}[X]$$

F si fattorizza in $\mathbb{C}[X]$ perché ammette le radici

$$x_1 = \frac{2+2i}{2} = 1+i \quad x_2 = \frac{2-2i}{2} = 1-i$$

$$F = (X - (1+i))(X - (1-i))$$

OSS ogni polinomio di grado 1 è irriducibile ma non è vero che ogni polinomio irriducibile di $K[X]$ è di grado 1. Tuttavia è vero su $K = \mathbb{C}$

$$4) F = X^3 - 1 \text{ si ha } \text{ev}_i(F) = 1 \quad (K = \mathbb{Q}, \mathbb{R}, \mathbb{C})$$

$$\begin{array}{c|cc} X^3 & -1 \\ \hline X^3 - X^2 & X^2 + X + 1 \\ \hline // X^2 & -1 \\ \hline X^2 - X & \\ \hline // X - 1 & \\ \hline X - 1 & \\ \hline // // & \end{array} \Rightarrow F = (X-1)(X^2 + X + 1)$$

$\hookrightarrow \Delta = -3 < 0 \Rightarrow$ la fattorizzazione di F in \mathbb{R} è finita

in \mathbb{C} radici $x_{1/2} = \frac{-1 \pm \sqrt{-3}}{2}$

la fattorizzazione in $\mathbb{C}[X]$ è $F = (X-1)(X-x_1)(X-x_2)$

Numeri complessi:

$\mathbb{C} = \{x+iy \text{ t.c. } x, y \in \mathbb{R}\} \text{ i.e. } \sqrt{-1} \text{ caratterizzato dalla condizione } i^2 = -1$
possiamo anche scrivere $\mathbb{C} = \mathbb{R} + i\mathbb{R}$

operazioni $z = x+iy \quad z' = x'+iy'$

$$-z := -x+(-y) \in \mathbb{C}$$

$$z+z' := (x+x') + i(y+y') \in \mathbb{C}$$

$$z \cdot z' := (x+iy)(x'+iy') = xx' + iyx' + ix'y' + i^2yy' = xx' - yy' + i(x'y + xy') \in \mathbb{C}$$

$(\mathbb{C}, -, +, \cdot, 0, 1)$ è un anello (commutativo unitario)

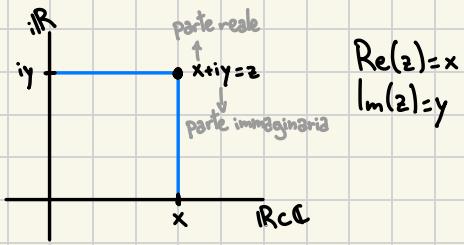
Opposto nei complessi

$$\text{se } z = x+iy$$

$$-z = -x+(-y)$$



Realizzazione cartesiana di \mathbb{C}



Esponenziale di Eulero $\theta \in \mathbb{R}$

$$e^{i\theta} := \cos \theta + i \sin \theta \in \mathbb{C} \quad \begin{matrix} \mathbb{R} & \longrightarrow & \mathbb{C} \\ \theta & \longmapsto & e^{i\theta} \end{matrix}$$

Eulero ha notato che

$$e^{i\theta} e^{i\eta} = e^{i(\theta+\eta)}$$

$$\begin{array}{c} | \\ (\cos \theta + i \sin \theta)(\cos \eta + i \sin \eta) \\ | \end{array}$$

$$(\cos \theta)(\cos \eta) - (\sin \theta)(\sin \eta) + i((\sin \theta)(\cos \eta) + (\cos \theta)(\sin \eta)) = \cos(\theta + \eta) + i \sin(\theta + \eta)$$

$$\cos \alpha \cos \beta - \sin \alpha \sin \beta = \cos(\alpha + \beta) \leftarrow$$

$$\hookrightarrow \sin \alpha \cos \beta + \sin \beta \cos \alpha = \sin(\alpha + \beta)$$

$$\text{in modo simile si trova } (e^{i\theta})^n = e^{in\theta}$$

es

$$e^{i2\pi} = \cos(2\pi) + i \sin(2\pi) = 1 + i0 = 1$$

$$e^{i0} = \cos(0) + i \sin(0) = 1$$

$$1 = e^{i2\pi} = e^{\frac{i2\pi}{3} \cdot 3} = (e^{\frac{i2\pi}{3}})^3$$

$$x = e^{\frac{i2\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$$

$$x^3 = 1 \text{ quindi } x \text{ è radice di } X^3 - 1 \text{ ev}_x(X^3 - 1) = 0$$

link

Osserviamo:

$$1 - 1^2 = \left(e^{\frac{i2\pi}{3}}\right)^2 = \left(e^{\frac{i2\pi}{3} \cdot 2}\right)^3 = \left(e^{\frac{i4\pi}{3}}\right)^3 \text{ quindi anche } x^2 \text{ è radice di } X^3 - 1$$

$$x^0 = e^{\frac{i0\pi}{3}} = \cos\left(\frac{0\pi}{3}\right) + i \sin\left(\frac{0\pi}{3}\right) = 1$$

$$x^1 = e^{\frac{i1\pi}{3}} = \cos\left(\frac{1\pi}{3}\right) + i \sin\left(\frac{1\pi}{3}\right)$$

$$x^2 = e^{\frac{i2\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$$

L'insieme $\{x^0, x^1, x^2\} = \mathbb{I}$ nei 3 elementi distinti, e $\forall y \in \mathbb{R}, \text{ev}_y(x^3 - 1) = 0 \Rightarrow x^3 - 1 = (x - x^0)(x - x^1)(x - x^2)$

$$0^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$$

$$e^{\frac{4\pi i}{3}} = \frac{-1-i\sqrt{3}}{2}$$

Punto 4
dell'esercizio

Coniugazione complessa

Si pone, per $z = x + iy \in \mathbb{C}$, $\bar{z} = x + i(-y)$

poniamo anche $h: \mathbb{C} \longrightarrow \mathbb{C}$ $h(z) := \bar{z}$

$$\bar{\bar{z}} = -z \Leftrightarrow z \in \mathbb{R}$$

infatti $\bar{\bar{z}} = -z \Leftrightarrow x - iy = -x - iy \Leftrightarrow x = 0$

Proprietà

$$\textcircled{1} h(z+z') = h(z) + h(z') \Rightarrow \overline{z+z'} = \bar{z} + \bar{z'}$$

$$h(z+z') = h(x+x'+i(y+y')) = x+x'-i(y+y')$$

$$h(z) + h(z') = x - iy + x' - iy' = x + x' - i(y+y')$$

$$\textcircled{2} h(zz') = h(z)h(z') \Rightarrow \overline{zz'} = \bar{z}\bar{z'}$$

$$h(zz') = h(xx' - yy' + i(xy' + x'y)) = xx' - yy' - i(xy' + x'y)$$

$$h(z)h(z') = (x-iy)(x'-iy') = xx' - yy' - i(xy' + x'y)$$

$$\textcircled{3} h(-z) = -h(z) \Rightarrow \overline{-z} = -\bar{z}$$

$$h(-z) = h(-x-iy) = -x+iy$$

$$-h(z) = -(x-iy) = -x+iy$$

$$\textcircled{4} h \text{ è una biezione } (h^{-1} = h)$$

$$h^{-1}(h(z)) = h^{-1}(h(x+iy)) = h^{-1}(x-iy) = x+iy = \text{id}_x$$

$$h(h^{-1}(x-iy)) = h(x+iy) = x-iy$$

Oss si dice che h è un **isomorfismo di anelli**

Relazione tra coniugazione e inverso

$$z = x+iy \in \mathbb{C}^* = \rho e^{i\theta} \quad (\rho \in \mathbb{R}_{>0}, \theta \in \mathbb{R})$$

quando avviene che $\bar{z} = z^{-1}$?

$$\bar{z} = \overline{\rho e^{i\theta}} = \bar{\rho} e^{i\theta} = \rho(\cos(\theta) - i \sin(\theta)) = \rho(\cos(-\theta) + i \sin(-\theta)) = \rho e^{-i\theta}$$

||

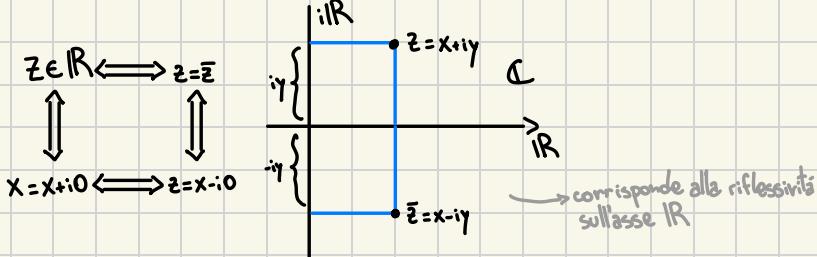
cos è pari sin è dispari

¶

$\cos(-\theta) = \cos(\theta)$ $\sin(-\theta) = -\sin(\theta)$

$$z^{-1} = (\rho e^{i\theta})^{-1} = \rho^{-1} e^{-i\theta}$$

$$\text{Quindi } z^{-1} = \bar{z} \Leftrightarrow \rho e^{-i\theta} = \rho^{-1} \bar{e}^{-i\theta} \Leftrightarrow \rho = 1$$



Formula fondamentale

$$z = x + iy \quad (x, y \in \mathbb{R})$$

$$z\bar{z} = (x+iy)(x-iy) = x^2 - ixy + ixy + y^2 = x^2 + y^2 \geq 0$$

$$x^2 + y^2 > 0 \iff x = y = 0$$

C è un campo?

$$z \in \mathbb{C} \setminus \{0\}$$

$$z\bar{z} = x^2 + y^2 > 0$$

moltiplico per $(x^2 + y^2)^{-1}$

$$\underbrace{z\bar{z}}_{z \neq 0} (x^2 + y^2)^{-1} = 1 \Rightarrow z \left(\frac{\bar{z}}{x^2 + y^2} \right) = 1$$

ogni elemento non nullo di C è invertibile $\Rightarrow C$ è un campo

es)

$$z = 2 = \begin{matrix} x \\ y \end{matrix} = \begin{matrix} 2 \\ 0 \end{matrix} \quad \bar{z} = 2 = \begin{matrix} x \\ y \end{matrix} = \begin{matrix} 2 \\ 0 \end{matrix}$$

$$z\bar{z} = x^2 + y^2 = 4$$

$$z^{-1} = \frac{\bar{z}}{z\bar{z}} = \frac{2}{4} = \frac{1}{2}$$

$$z = i = \begin{matrix} x \\ y \end{matrix} = \begin{matrix} 0 \\ 1 \end{matrix} \quad \bar{z} = -i = \begin{matrix} x \\ y \end{matrix} = \begin{matrix} 0 \\ -1 \end{matrix}$$

$$z\bar{z} = x^2 + y^2 = 1$$

$$z^{-1} = \frac{-i}{1} = -i$$

$$z = 1+i \quad \bar{z} = 1-i$$

$$z\bar{z} = x^2 + y^2 = 2$$

$$z^{-1} = \frac{1-i}{2} \Rightarrow 1+i \cdot \frac{1-i}{2} = \frac{1+i}{2} = 1$$

Valore assoluto complesso

$$|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$$

proprietà

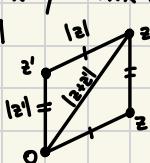
$$\textcircled{1} |z| = 0 \iff z = 0$$

$$\textcircled{2} |z\bar{z}| = |z||z|$$

$$|z\bar{z}| = |xx - yy + i(x'y + xy')| = \sqrt{(xx - yy)^2 + (x'y + xy')^2} = \sqrt{x^2x^2 + y^2y^2 - 2xy'yy' + x^2y^2 + x^2y^2 + 2xxy'yy'} = \sqrt{x^2x^2 + y^2y^2 + x^2y^2 + x^2y^2} = \sqrt{2x^2y^2} = \sqrt{2}xy$$

$$|z||z| = \sqrt{x^2 + y^2} \sqrt{x^2 + y^2} = \sqrt{x^2x^2 + y^2y^2 + x^2y^2 + x^2y^2} = \sqrt{2x^2y^2} = \sqrt{2}xy$$

$$\textcircled{3} |z+z'| \leq |z| + |z'|$$



altri proprietà $\forall \theta \in \mathbb{R}$

(1) $|e^{i\theta}| = 1$

$$e^{i\theta} = \cos \theta + i \sin \theta$$

$$|e^{i\theta}| = \sqrt{\cos^2 \theta + \sin^2 \theta} = \sqrt{1} = 1 \quad e^{i\theta} \neq 0 \text{ quindi invertibile}$$

(2) $(e^{i\theta})^{-1} = e^{-i\theta} = e^{i(-\theta)}$

$$e^{i\theta} \cdot e^{-i\theta} \Rightarrow 1 = -\theta \Rightarrow e^{i\theta} e^{i(-\theta)} = e^{i0} = 1$$

$$e^{-i\theta} = (e^{i\theta})^{-1}$$

$$\overline{e^{i\theta}} = \cos \theta - i \sin \theta$$

$$\frac{e^{i\theta}}{\cos^2 \theta + \sin^2 \theta} = \frac{(e^{i\theta})^{-1}}{\overline{e^{i\theta}}} = 1$$

La rappresentazione cartesiana è adatta a rappresentare la somma dei complessi.

Rappresentazione polare

$$z \in \mathbb{C} \quad z = x + iy$$

$$r = \sqrt{x^2 + y^2}$$

La rappresentazione polare è del tipo $z = r e^{i\theta}$

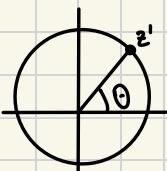
risulta essere più adatta a rappresentare il prodotto rispetto alla rappresentazione cartesiana.

Lemma: esiste $\theta \in \mathbb{R}$ t.c. $z = r e^{i\theta}$. Inoltre $\theta + 2\pi\mathbb{Z}$ è unicamente determinato

dim:

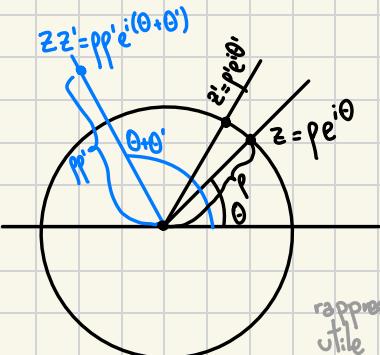
$$\begin{aligned} p &= \sqrt{z\bar{z}} \quad \text{e} \quad \sin z := p^{-1} \cdot z \\ z' \bar{z}' &= p^{-1} z \bar{p^{-1}} \bar{z} = p^{-2} p^2 \end{aligned}$$

↳ è un reale



$$z' = x' + iy' \quad \text{ma} \quad \exists \theta \text{ t.c. } x' = \cos \theta \wedge y' = \sin \theta \Rightarrow z' = e^{i\theta} \Rightarrow z = p e^{i\theta}$$

Le soluzioni di $z = p e^{i\theta}$ sono esattamente gli elementi di $\theta + 2\pi\mathbb{Z}$ per un certo $\theta \in [0, 2\pi)$



rappresentazione polare
utile per effettuare moltiplicazioni di numeri coprimi

Si può quindi dire che su \mathbb{R} c'è relazione di congruenza $(\text{mod } 2\pi)$ $\alpha, \beta \in \mathbb{R}$ $\alpha \equiv \beta \pmod{2\pi} \Leftrightarrow \alpha - \beta \in 2\pi\mathbb{Z}$ che è una relazione d'equivalenza da cui $\theta + 2\pi\mathbb{Z}$ è una classe d'equivalenza e si identifica con un elemento di $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$ (anche se non è un anello)

Alegricamente chiuso DEF

K campo è detto alegricamente chiuso se $\forall F \in K[X] \setminus K \exists x \in K$ t.c. x è radice di F ($ev_x(F) = 0$)

Lemmo K è alegricamente chiuso \Leftrightarrow polinomi irriducibili e monici sono i polinomi $X-x$, $x \in K$

dim

\Rightarrow

sia $P \in K[X]$ irriducibile e monico

siccome K è alegricamente chiuso $\exists x \in K$ t.c. $X-x \mid P \Rightarrow P = (X-x)Q$ con $Q \in K[X] \setminus \{0\}$
 $\deg(P) = 1 + \deg(Q)$

se $\deg(P) \geq 2$ allora $\deg(Q) \geq 1$

Quindi $Q \in K[X]^*$ ma $X-x \in K[X]^*$

questo contraddice il fatto che P sia irriducibile (ipotesi) quindi $\deg(P) = 1 \Rightarrow P = X-x$

\Leftarrow

supponiamo che $\{P \in K[X] \text{ t.c. } P \text{ monico irriducibile}\} = \{X-x \text{ t.c. } x \in K\}$

sia P monico di grado $n \geq 1$

$$P = \prod_{Q \in \text{irr}} Q^{v_Q(P)} = \prod_{x \in K} (X-x)^{v_{X-x}(P)}$$

sia $x \in K$ t.c. $v_{X-x}(P) \neq 0$, allora $X-x \mid P \Leftrightarrow ev_x(P) = 0 \Leftrightarrow x$ è radice di P



Corollario

K alegricamente chiuso $\Rightarrow \forall F \in K[X] \setminus \{0\}$ si scrive in modo unico come $F = \lambda \prod_{\substack{x \in K \\ K^*}} (X-x)^{v_{X-x}(F)}$

dove $v_x(F) \in \mathbb{N}$ è semplicemente $v_{X-x}(F)$ e si chiama la multiplicità di F in x

si ha che $\{x \text{ t.c. } v_x(F) \neq 0\}$

$v_x(F) = \{x \text{ t.c. } ev_x(F) = 0\} = \{\text{radici di } F\} = R$

questo insieme ha cardinalità $\leq \deg(F)$

$$\deg(F) = \sum_{x \in K} v_x(F) = \sum_{x \in R} v_x(F) \geq \sum_{x \in R} 1 = \text{Card}(R)$$

il numero di radici di un polinomio non nullo
è al massimo il grado del polinomio

Teorema

C è alegricamente chiuso

Teorema

dato un campo K esiste sempre un altro campo $L \supset K$ con L algebricamente chiuso

(es)

\mathbb{R} non è algebricamente chiuso: $X^2 + 1$ è irriducibile in \mathbb{R} e non ha grado 1 però $\mathbb{R} \subset \mathbb{C}$

Esercizio (polinomi del tipo $X^n - 1$)

$$X^n - 1 \quad (n \leq 5)$$

il polinomio $X^n - 1$ ha sempre la radice 1 quindi $X-1 | X^n - 1$

$$X^n - 1 = (X-1)Q \quad \deg(Q) = n-1$$

più precisamente $Q = X^{n-1} + X^{n-2} + \dots + X + 1 \rightarrow$ polinomio ciclotomico

$$(X-1)(X^{n-1} + X^{n-2} + \dots + X + 1) = X^n + X^{n-1} + \dots + X^2 + X - X^{n-1} - \dots - X^2 - X - 1 = X^n - 1$$

con n pari $X^n - 1$ ha anche la radice $-1 \rightarrow (-1)^n = 1$

$n=3$

$$X^3 - 1 = (X-1)(X^2 + X + 1) \quad \text{fattorizzazione in } \mathbb{R}$$

$$\text{in } \mathbb{C} \quad X^2 + X + 1 = \left(X + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(X + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$$

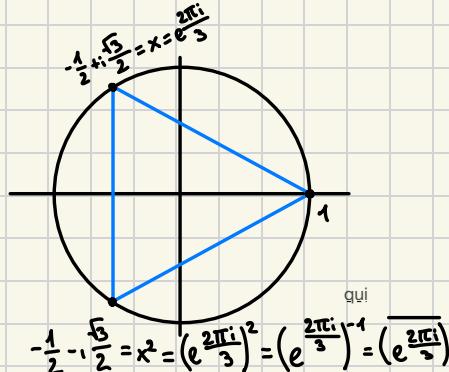
$\exists \theta$ t.c. $z = pe^{i\theta}$ in cerchio goniometrico si ha $p=1$

$$z = e^{i\theta} = \cos\theta + i\sin\theta \quad \text{quindi si ha che}$$

$$-\frac{1}{2} = \cos\theta \quad \begin{cases} \theta = \frac{2\pi}{3} + 2k\pi \\ \theta = \frac{4\pi}{3} + 2k\pi \end{cases}$$

$$\frac{\sqrt{3}}{2} = \sin\theta \quad \begin{cases} \theta = \frac{\pi}{3} + 2k\pi \\ \theta = \frac{7\pi}{3} + 2k\pi \end{cases}$$

$$\text{quindi } \theta = \frac{2\pi}{3} \Rightarrow z = e^{\frac{2\pi i}{3}}$$



$$X^3 - 1 \text{ ha le radici: } 1 = x^0, \quad x = e^{\frac{2\pi i}{3}}, \quad x = (e^{\frac{2\pi i}{3}})^2$$

$n=4$

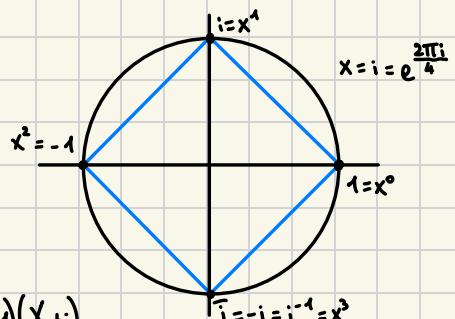
$$X^4 - 1 = (X-1)(X+1)(X^2 + 1) \quad \text{in } \mathbb{R}[X]$$

$$= (X-1)(X+1)(X-i)(X+i) \quad \text{in } \mathbb{C}[X]$$

$$X^4 - 1 = (X-x^0)(X-x^1)(X-x^2)(X-x^3)$$

$$\text{con } x = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right) = 0 = 1$$

$$X^4 - 1 = (X-i^0)(X-i^1)(X-i^2)(X-i^3) = (X-1)(X-i)(X+i)(X+i)$$



OSS se α è radice di $X^n - 1 \in \mathbb{R}[X]$ allora o $\alpha \in \mathbb{R}$ oppure $\alpha \in \mathbb{C} \setminus \mathbb{R}$ e in questo caso anche $\bar{\alpha}$ è radice di $X^n - 1$ distinta da α

$n=5$

$$X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$$

so che questo polinomio è scomponibile, infatti: lo posso scomporre in 2 polinomi di grado 2. So per certo che non sono 4 polinomi di grado 1 in quanto un polinomio ha un fattore di grado 1 \Leftrightarrow ha una radice reale

$X^5 - 1$ ha 5 radici distinte

$$(e^{\frac{2\pi i}{5}})^k \quad k=0,1,2,3,4 \Rightarrow ((e^{\frac{2\pi i}{5}})^k)^5 = (e^{\frac{2\pi i}{5}k})^5 = (e^{2\pi i k})^5 = 1$$

sono distinte perché

$$(e^{\frac{2\pi i}{5}})^k = \cos\left(\frac{2\pi k}{5}\right) + i\sin\left(\frac{2\pi k}{5}\right)$$

$$P_1 = (X-x)(X-\bar{x}) \in \mathbb{R}[X]$$

$$P_2 = (X-x^2)(X-\bar{x}^2) \in \mathbb{R}[X]$$

infatti:

$$P_1 = (X-x)(X-\bar{x}) = X^2 - (x+\bar{x})X + x\bar{x} \in \mathbb{R}$$

$$P_2 = (X-x^2)(X-\bar{x}^2) = X^2 - (x^2+\bar{x}^2)X + |x^2|^2 \in \mathbb{R}$$

$$x = \alpha + i\beta \quad \bar{x} = \alpha - i\beta \quad x + \bar{x} = 2\alpha \in \mathbb{R}$$

$$x\bar{x} = \alpha^2 + \beta^2 \geq 0 \quad \bar{x} = x^4 \Rightarrow x\bar{x} = 1$$

$$x^2\bar{x}^2 = 1$$

$$x + \bar{x} = 2\operatorname{Re}(x) = 2\cos\left(\frac{2\pi}{5}\right)$$

$$x^2 + \bar{x}^2 = 2\operatorname{Re}(x^2) = 2\cos\left(\frac{4\pi}{5}\right) \Rightarrow e^{\frac{4\pi i}{5}} = x \Rightarrow x^2 = e^{\frac{4\pi i}{5}}$$

$$P_1 = X^2 - 2\cos\left(\frac{2\pi}{5}\right)X + 1$$

$$P_2 = X^2 - 2\cos\left(\frac{4\pi}{5}\right)X + 1$$

OSS

$z \in \mathbb{C}$ è della forma $e^{i\theta} \Leftrightarrow |z|=1$

Vuol dire che z è vegole a 1
mi trovo quindi in un cerchio unitario

$$z = e^{i\theta} \Rightarrow |z| = \sqrt{\cos^2 \theta + \sin^2 \theta} = 1$$

ricerco se $|z|=1$ allora la sua distanza dall'origine è 1 quindi giace sul cerchio unitario di $\mathbb{C} \Rightarrow \exists \theta$ t.c. $z = \cos \theta + i \sin \theta = e^{i\theta}$

$$X^5 - 1 = \prod_{i=0}^4 (X-x^i) = (X-x^0)[(X-x)(X-x^4)][(X-x^2)(X-x^3)] = (X-x^0)P_1 P_2 \text{ fattorizzato in } \mathbb{R}[X]$$

$$P_1 P_2 = (X^2 - 2\cos\left(\frac{2\pi}{5}\right) + 1)(X^2 - 2\cos\left(\frac{4\pi}{5}\right) + 1) = X^4 + X^3 + X^2 + X + 1$$

si trovano in un poligono regolare di n lati: in cui sono presenti i vertici: i, 1, e -1

$$\text{OSS } \text{ le formule } (n \geq 1) \quad X^n - 1 = \prod_{i=0}^{n-1} (X-x^i) \quad x = \frac{2\pi i}{n} \text{ fattorizzato in } \mathbb{C} \quad \text{se e solo se } n \text{ è pari}$$

Dato $F = f_0 + f_1 X + \dots + f_n X^n \in \mathbb{C}[X]$

$$\underbrace{\mathbb{C}}_{\mathbb{C}} \quad \underbrace{\mathbb{C}}_{\mathbb{C}} \quad (\bar{z} := z)$$

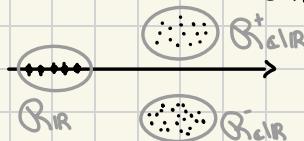
poniamo $\bar{F} = \bar{f}_0 + \bar{f}_1 \bar{X} + \dots + \bar{f}_n \bar{X}^n$

OSS $F \in \mathbb{R}[X] \Leftrightarrow \bar{F} = \bar{F}$. Inoltre se $F \in \mathbb{R}[X]$ e $\text{ev}_{\mathbb{Z}}(F) = 0$ allora $\text{ev}_{\mathbb{E}}(F) = 0$
 $\text{ev}_{\mathbb{E}}(F) = \text{ev}_{\mathbb{E}}(\bar{F}) = \overline{\text{ev}_{\mathbb{E}}(F)} = \bar{0} = 0$

Lemme Dato $F \in \mathbb{R}[X]$ detto \mathcal{R} l'insieme delle sue radici, allora $\mathcal{R} = \mathcal{R}_{\mathbb{IR}} \cup \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^+ \cup \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^-$
dove $\mathcal{R}_{\mathbb{IR}} = \mathcal{R} \cap \mathbb{R}$

$$\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^+ = \{z \in \mathcal{R} \text{ t.c. } z \in \mathbb{C} \wedge \text{Im}(z) > 0\}$$

$$\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^- = \{z \in \mathcal{R} \text{ t.c. } z \in \mathbb{C} \wedge \text{Im}(z) < 0\}$$



Inoltre posso scrivere

$$\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}} = \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^+ \cup \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^- \quad e \quad \overline{\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}} = \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^+$$

Lemme $P = X^2 + \beta X + \gamma \in \mathbb{R}[X]$ è irriducibile in $\mathbb{R}[X] \Leftrightarrow \Delta = \beta^2 - 4\gamma < 0$

dim

\Rightarrow

supponiamo P irriducibile quindi non ha radici reali (è di grado 2) $\mathcal{R}_{\mathbb{IR}} = \emptyset$

quindi $\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}} = \{z, \bar{z}\} \Rightarrow \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^+ = \{z\}$ e $\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}^- = \{\bar{z}\}$

$$P = (X-z)(X-\bar{z}) = X^2 - (z+\bar{z})X + z\bar{z}$$

$z = \begin{cases} \text{Re}(z) \\ \text{Im}(z) \end{cases}$

$$\Delta = (z+\bar{z})^2 - 4z\bar{z} = z^2 + 2z\bar{z} + \bar{z}^2 - 4z\bar{z} = z^2 - 2z\bar{z} + \bar{z}^2 = (z-\bar{z})^2$$

se scrivo $z = x+iy$ e $\bar{z} = x-iy \Rightarrow z-\bar{z} = 2iy$

$$(z-\bar{z})^2 = (2iy)^2 = 4i^2y^2 = -4y^2 < 0 \Rightarrow \Delta < 0$$

\Leftarrow

siccome $\mathbb{R} \subset \mathbb{C}$ e \mathbb{C} è algebricamente chiuso allora $\exists z \in \mathbb{C}$ t.c. $\text{ev}_z(P) = 0$

quindi $X-z \mid P$ (in $\mathbb{C}[X]$)

si ha $z \neq \bar{z}$ ($\Leftrightarrow z \in \mathbb{C} \setminus \mathbb{R}$) $\Leftrightarrow X-z \neq X-\bar{z} \Leftrightarrow X-z$ e $X-\bar{z}$ sono coprimi

Quindi $z \neq \bar{z} \Rightarrow (X-z)(X-\bar{z}) \mid P$ ma $\deg(P) = 2$ da cui P ha radici in $\mathbb{C} \setminus \mathbb{R} \Leftrightarrow P = (X-z)(X-\bar{z})$

$z \in \mathbb{C} \setminus \mathbb{R}$

Lemma ogni $F \in \mathbb{R}[X]$ si scomponga (in $\mathbb{C}[X]$) in prodotto $F = \lambda \prod_{x \in \mathbb{R}} (X-x) \prod_{z \in \mathbb{C} \setminus \mathbb{R}} [(X-z)(\bar{X}-\bar{z})]^{v_z(F)}$

dim siccome \mathbb{C} è algebricamente chiuso

$$F = \lambda \prod_{z \in \mathbb{R}} (X-z)^{v_z(F)} = \lambda \prod_{z \in \mathbb{R} \setminus \mathbb{R}} (X-z)^{v_z(F)} \prod_{z \in \mathbb{C} \setminus \mathbb{R}} (X-z)^{v_z(F)}$$

se $z \in \mathbb{R} \setminus \mathbb{R}$ si ha $\bar{z} \in \mathbb{R} \setminus \mathbb{R}$ quindi posso scegliere, senza perdita di generalità $z = x+iy$ con $y > 0$ si conclude osservando che $\mathbb{R} = \mathbb{R}_{<0} \sqcup \mathbb{R}_{>0} \sqcup \mathbb{R}_{=0}$ con ovvi significati



Lemma $\deg(P) = \#\mathbb{R}_{<0} + \#\mathbb{R}_{>0} = \#\mathbb{R}_{<0} + 2\#\mathbb{R}_{=0}^+$

prop

Sia $P \in \mathbb{R}[X]$ di grado dispari. Allora P ammette almeno una radice reale

dim

$$\text{siccome } P \text{ è di grado dispari } \deg(P) = 2n+1 = \# \mathbb{R}_{<0} + 2 \# \mathbb{R}_{=0}^+ \Rightarrow r+s = r+2s \Leftrightarrow r = 2s+1 \Rightarrow r \equiv 1 \pmod{2} \Rightarrow r \neq 0$$



Teorema dei valori intermedi (teorema dell'analisi)

sia $h: \mathbb{R} \rightarrow \mathbb{R}$ continua t.c. $\lim_{x \rightarrow -\infty} h(x) = -\infty$ e $\lim_{x \rightarrow +\infty} h(x) = +\infty$ allora $\exists x_0 \in \mathbb{R}$ t.c. $h(x_0) = 0$

$$P = X^{2n+1} + \alpha_{2n} X^{2n} + \dots + \alpha_0 \in \mathbb{R}[X]$$

sia $f: \mathbb{R} \rightarrow \mathbb{R}$ la funzione $f(x) = ev_x(P)$ è continua e soddisfa $\lim_{x \rightarrow -\infty} f(x) = -\infty$ e $\lim_{x \rightarrow +\infty} f(x) = +\infty$ da cui $\exists x_0 \in \mathbb{R}$ t.c. $f(x_0) = 0 \Leftrightarrow \exists x_0 \in \mathbb{R}$ t.c. x_0 radice di f

Esercizio

$P = X^4 - 10X^2 + 1$ fattorizzazione in $(\mathbb{Q}, \mathbb{R}, \mathbb{C})[X]$

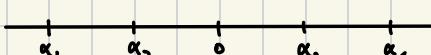
$$P = Y^2 - 10Y + 1 \quad Y = X^2$$

radici di $Y^2 - 10Y + 1$

$$\Delta > 0 \quad \text{radici } y_1 = 5 - 2\sqrt{6} > 0$$

$$y_2 = 5 + 2\sqrt{6} > 0 \Rightarrow Y^2 - 10Y + 1 = (Y - 5 + 2\sqrt{6})(Y - 5 - 2\sqrt{6}) = (X^2 - 5 + 2\sqrt{6})(X^2 - 5 - 2\sqrt{6}) = \\ = (X - \sqrt{5 - 2\sqrt{6}})(X + \sqrt{5 - 2\sqrt{6}})(X - \sqrt{5 + 2\sqrt{6}})(X + \sqrt{5 + 2\sqrt{6}}) \text{ fatt. in } \mathbb{R}[X]$$

↓



corrisponde alla fatt. in $\mathbb{C}[X]$

Esercizio

$x = \sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2}$ mostrare che $x \in \mathbb{R} > 0$ e dimostrare che $x=1$
 tip: usare che x è l'unica radice reale di $X^3 + 3X - 4$

se $\sqrt[3]{\sqrt{5} + 2} > \sqrt[3]{\sqrt{5} - 2}$ allora $\sqrt{5} + 2 > \sqrt{5} - 2$ vero $\Rightarrow x \in \mathbb{R} > 0$

$$\begin{array}{r|l} X^3 + 3X - 4 & X-1 \\ X^3 - X^2 & X^2 + X + 4 \\ \hline // X^2 + 3X - 4 & \\ X^2 - X & \\ \hline // 4X - 4 & \\ 4X - 4 & \\ \hline // // & \end{array}$$

$$X^3 + 3X - 4 = (X-1)(X^2 + X + 4) \quad \text{fattorizzazione in } \mathbb{R}[X]$$

$$X^2 + X + 4 \Rightarrow \Delta < 0$$

sapendo che x è l'unica radice reale di $X^3 + 3X - 4 \Rightarrow x = 1$

Polinomi irriducibili in $\mathbb{Q}[X]$

Possibili fattorizzazioni in polinomi irriducibili di polinomi in $\mathbb{Q}[X]$

$Q \in \mathbb{Q}[X]$ monico $\mathbb{Q} \rightarrow K$ (qualsiasi campo)

- $\deg(Q)=1$ è irriducibile
- $\deg(Q)=2$
 - è irriducibile
 - $Q = P_1 P_2$ con P_1, P_2 di grado 1
- $\deg(Q)=3$
 - Q irriducibile
 - $Q = P_1 P_2$ irriducibili con $\deg(P_1)=1$ e $\deg(P_2)=2$
 - $Q = P_1 P_2 P_3$ con P_1, P_2, P_3 di grado 1
- $\deg(Q)=4$
 - Q irriducibile
 - $Q = P_1 P_2$ con $\deg(P_1)=1$ e $\deg(P_2)=3$
 - $Q = P_1 P_2$ con $\deg(P_1) = \deg(P_2) = 2$
 - $Q = P_1 P_2 P_3$ con $\deg(P_1) = \deg(P_2) = 1$ e $\deg(P_3) = 2$
 - $Q = P_1 P_2 P_3 P_4$ con P_1, P_2, P_3, P_4 di grado 1

OSS se Q non è irriducibile su K allora ammette sempre almeno una radice

Gruppi: DEF

Sia G insieme $\neq \emptyset$, * operazione binaria su G ovvero: $G \times G \longrightarrow G$
 $(a,b) \longmapsto a * b$

seleziono $e \in G$ elemento distinto in G

L₃ terna $G = (G, *, e)$ è un gruppo se:

- ① $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$ associatività
- ② $\forall a \in G, \quad a * e = e * a = a$ elemento neutro
- ③ $\forall a \in G, \exists a' \in G$ t.c. $a * a' = a' * a = e$ inverso

inoltre se

$\forall a, b \in G \quad a * b = b * a$, allora si dice che G è un gruppo **commutativo** (o abeliano)

Gruppi in notazione additiva DEF

$(G, +, 0)$

Si scrive $+$ per l'operazione e 0 o 0_G per l'elemento neutro. Tali gruppi sono detti in notazione additiva (tipicamente sono commutativi)

In notazione additiva l'inverso di $a \in G$ si chiama opposto di a e si scrive $-a$

es

$(\mathbb{A}, -, +, \cdot, 0_A, 1_A)$ anello

Allora $(\mathbb{A}, +, 0_A)$ è un gruppo abeliano in notazione additiva

Quindi $\mathbb{Z} = (\mathbb{Z}, +, 0)$ $\mathbb{R} = (\mathbb{R}, +, 0)$ $\mathbb{C} = (\mathbb{C}, +, 0)$ o anche $\mathbb{K} = (\mathbb{K}, +, 0)$ con \mathbb{K} qualunque campo abeliano

Gruppi in notazione moltiplicativa DEF

$(G, \cdot, 1)$

Si scrive \cdot per l'operazione e 1 o 1_G per l'elemento neutro. Tali gruppi possono non essere abeliani

In notazione moltiplicativa l'inverso di $a \in G$ si scrive a^{-1}

prop

sia G un gruppo $\forall a, b \in G \quad (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ es. $(g^{-1}bg)^{-1} = g^{-1}b^{-1}g$

dim

dobbiamo verificare che $b^{-1} \cdot a^{-1}$ è l'inverso di $a \cdot b$, ovvero che $(a \cdot b)(b^{-1} \cdot a^{-1}) = e$

per associatività abbiamo $a(b \cdot b^{-1}) \cdot a^{-1} = e$ per l'inverso $b \cdot b^{-1} = e$

quindi $a \cdot e \cdot a^{-1} = e$ per elemento neutro $a \cdot e = a$

$a \cdot a^{-1} = e$ verificato

si verifica quindi che $(b^{-1} \cdot a^{-1})(a \cdot b) = e$ allo stesso modo

es

$(A, \cdot, +, \cdot, 0_A, 1_A)$ anello

Allora $(A, \cdot, 0_A)$ è un gruppo abeliano in notazione moltiplicativa

Infatti: abbiamo visto ① il prodotto di elementi invertibili è invertibile ② il prodotto è associativo
② se $a, b \in A^*$ allora $ab \in A^*$ e $(ab)^{-1} = b^{-1}a^{-1}$. Inoltre A^* è commutativo

Sottogruppo DEF

link

→ chiuso rispetto a prodotto e neutro

Dato un gruppo G (notazione moltiplicativa) e un sottoinsieme $H \subset G$ non vuoto. Si dice che H è un **sottogruppo** di G se $\forall a, b \in H$ si ha $a \cdot b^{-1} \in H$. Si scrive $H \subset G$

OSS H è un gruppo. Se $a \in H$ $a \cdot a^{-1} \in H$. Ma allora $\forall b \in H$ $1_G \cdot b^{-1} = b^{-1} \in H$ e $1_G = 1_H \in H$, $b^{-1} \in H$. Infine se $a, b \in H$, $b^{-1} \in H$ e $a(b^{-1})^{-1} = ab \in H$

es

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Omomorfismi di gruppi: DEF

Dati G_1, G_2 gruppi (in notazione moltiplicativa)

Sia $f: G_1 \longrightarrow G_2$ un'applicazione

f è un omomorfismo (di gruppi) se:

- ① $f(1_{G_1}) = 1_{G_2}$ inversione in G_1
- ② $\forall a \in G_1, f(a^{-1}) = f(a)^{-1}$ → inversione in G_2
- ③ $\forall a, b \in G_1, f(ab) = f(a)f(b)$

↳ operazione di G_2
↳ operazione di G_1

link

prop

$f: G_1 \longrightarrow G_2$ è omomorfismo $\Leftrightarrow \forall a, b \in G_1, f(ab^{-1}) = f(a)f(b)^{-1}$

dim

\Rightarrow

Sia $f: G_1 \longrightarrow G_2$ un omomorfismo allora ③ dato $a, b^{-1} \in G_1$ si ha $f(ab^{-1}) = f(a)f(b)^{-1}$

Dunque per ② $f(b^{-1}) = f(b)^{-1}$, quindi $f(ab^{-1}) = f(a)f(b)^{-1} = f(a)f(b)^{-1}$

\Leftarrow

Sia $f: G_1 \longrightarrow G_2$ t.c. $\forall a, b \in G_1, f(ab^{-1}) = f(a)f(b)^{-1}$

① $f(a \cdot a^{-1}) = f(a)f(a)^{-1} \Rightarrow f(1_{G_1}) = 1_{G_2}$

↪ immagine in G_2

↪ immagine in G_1

② $f(1_{G_1} \cdot a) = f(1_{G_1})f(a)^{-1}$ ma $a \cdot 1_{G_1} = a \Rightarrow f(a) = 1_{G_2}f(a)^{-1} \Rightarrow f(a) = f(a)^{-1}$

③ sia $\forall a, b^{-1} \in G_1, f(a(b^{-1})^{-1}) = f(a)f(b)^{-1} \Rightarrow f(ab) = f(a)f(b)^{-1} = f(ab) = f(a)f(b)$

Isomorfismo DEF

Sia $f: G_1 \longrightarrow G_2$ un omomorfismo di gruppi. Se f è biettiva allora si dice che f è un **isomorfismo**.

prop

Sia $f: G_1 \longrightarrow G_2$ isomorfismo (quindi $f \circ f^{-1} = \text{id}_{G_2}$ e $f^{-1} \circ f = \text{id}_{G_1}$) allora f^{-1} è un isomorfismo.

Inoltre $G_1 \longrightarrow G_2 \longrightarrow G_3$ con f, g omomorfismi di gruppi allora $g \circ f: G_1 \longrightarrow G_3$ è anche un omomorfismo di gruppi e in più se f, g sono isomorfismi anche $g \circ f$ lo è, anche di inverso $f^{-1} \circ g^{-1}$

es

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & m\mathbb{Z} \\ \text{---} & \text{---} & \text{---} \\ G_1 & \xrightarrow{\quad} & G_2 \end{array} \Rightarrow m\mathbb{Z} \text{ sottogruppo di } \mathbb{Z} \text{ infatti: } \forall a, b \in m\mathbb{Z} \quad a-b \in m\mathbb{Z}$$

(3) $\exists \alpha, \beta \in \mathbb{Z} \text{ t.c. } a = m\alpha \text{ e } b = m\beta \quad a-b = m(\alpha-\beta)$

notazione additiva con $f(n) := mn$ applicazione isomorfismo di gruppi, infatti:

(1) $f(n-n') = m(n-n') = mn - mn' = f(n) - f(n') \Rightarrow$ omomorfismo di gruppi

(2) f iniettiva

$$f(p) = f(q) \Leftrightarrow pm = qm \Leftrightarrow m(p-q) = 0 \Leftrightarrow p = q$$

(3) f suriettiva

sia $y \in m\mathbb{Z}$ $\exists k \in \mathbb{Z}$ t.c. $y = mk$ ponendo $x = k$ si ha $f(x) = mk = y$

Applicazioni da additiva a moltiplicativa

$G_1 = \mathbb{R}$ con $+$

$G_2 = \mathbb{R}_{>0} = \{x \in \mathbb{R} \text{ t.c. } x > 0\}$ con .

notare che $\mathbb{R}_{>0} \subset \mathbb{R}^*$ $\rightarrow \mathbb{R}$ con .

nonostante che i due gruppi sono in notazioni differenti ma posso avere un isomorfismo tra i due

poniamo $f: \mathbb{R} \longrightarrow \mathbb{R}_{>0}$

$$\begin{array}{ccc} x & \longmapsto & e^x \end{array}$$

$g: \mathbb{R}_{>0} \longrightarrow \mathbb{R}$

$$\begin{array}{ccc} y & \longmapsto & \log(y) \end{array}$$

f e g sono due isomorfismi di gruppi, l'uno l'inverso dell'altro $f^{-1} = g$ e $g^{-1} = f$ sono infatti anche omomorfismi.

$$\begin{aligned} f(0) &= e^0 = 1 = 1_{G_2} \in G_2 \\ f(-x) &= e^{-x} = (e^x)^{-1} = f(x)^{-1} \\ f(x-x') &= e^{x-x'} = e^x e^{-x'} = f(x)f(x')^{-1} \end{aligned}$$

$$\begin{aligned} g(1) &= \log 1 = 0 = 0_{G_1} \in G_1 \\ g(y^{-1}) &= \log(y^{-1}) = -\log(y) \\ g(y^{-1}) &= \log\left(\frac{1}{y}\right) = \log(y) - \log(1) = \log(y) - \log(y) = 0 \end{aligned}$$

Esercizio

Esercizio 2. \mathbb{K} è un campo qualsiasi. Dati i seguenti interi $p, q \in \mathbb{K}[x]$, calcolare il loro massimo comun divisore $d \in \mathbb{K}[x]$ e trovare $s, t \in \mathbb{K}$ tali che $ps + qt = d$. (Suggerimento: usare l'algoritmo di Euclide.)

- (i) $p = x^4 + x + 1, q = x^3 - 2$ con $\mathbb{K} = \mathbb{Q}$ PRIMI
- (ii) $p = x^5 - x^3 + x^2 - 2x + 1, q = x^4 + x^3 + 2x^2 + x + 1$ con $\mathbb{K} = \mathbb{Q}$ PRIMI
- (iii) $p = x^3 + x^2 - 6x + 1, q = x^4 - 2x^3 - 2x - 1$ con $\mathbb{K} = \mathbb{Z}/7$.

II

$\mathbb{K} = \mathbb{F}_7 = \frac{\mathbb{Z}}{7\mathbb{Z}}$ è un campo infatti: $\mathbb{F}_7^x = \mathbb{F}_7 \setminus \{0\}$ con $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ dove questi simboli rappresentano le classi corrispondenti su $\frac{\mathbb{Z}}{7\mathbb{Z}}$. Posso anche utilizzare altri interi per rappresentare elementi di \mathbb{F}_7 estraendoli dalle classi. (es. $8 \in \mathbb{F}_7, 8 \equiv 1$)

Abbiamo visto che \mathbb{F}_7 è un gruppo in notazione moltiplicativa

Tavola di moltiplicazione di \mathbb{F}_7

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

visto che \mathbb{F}_7 è abeliano questa risulta essere simmetrica rispetto alla diagonale

ogni volta che vedo un 1 vuol dire che i due numeri sono uno l'opposto dell'altro. Inoltre in ogni riga ho un 1 in quanto ogni elemento di un gruppo è invertibile.

calcolo quindi l'MCD dei polinomi

$$P = X^3 + X^2 - 6X + 1 \quad Q = X^4 - 2X^3 - 2X - 1 \quad \text{in } \mathbb{F}_7[X]$$

$\frac{1}{1}$

$$\begin{array}{r|rr}
X^4 - 2X^3 & -2X - 1 & X^3 + X^2 + X + 1 \\
X^4 + X^3 + X^2 + X & X - 3 \Rightarrow X + 4 \\
\hline
// -3X^3 - X^2 - 3X - 1 & \hookrightarrow -3+7=4 \\
-3X^3 - 3X^2 - 3X - 3 \\
\hline
// 2X^2 // +2
\end{array}$$

$$\deg(2X^2) = 2 < \deg(P) = 3$$

$$X^4 - 2X^3 - 2X - 1 = \underbrace{(X+4)}_{\text{quoziente}} \underbrace{(X^3 + X^2 + X + 1)}_P + \underbrace{2(X^2 + 1)}_{\text{resto}}$$

Attenzione a scambiare quoziente e P infatti: il polinomio è la divisione per P più il resto e non la divisione per il quoziente più il resto ($\deg(\text{resto}) > \deg(\text{quoziente})$)

$$\begin{array}{r|rr}
X^3 + X^2 + X + 1 & 2X^2 + 2 \\
X^3 + X & 4X + 4 \\
\hline
// X^2 // +1 & \hookrightarrow \text{inverso di 2, controllo} \\
X^2 + 1 & \text{la tavola di moltiplicazione} \\
\hline
// & //
\end{array}$$

$$X^3 + X^2 + X + 1 = (4X+4)(2X^2 + 2) + 0$$

il $\text{MCD}(P, Q)$ è l'unico multiplo di $2X^2+2$ (che è l'ultimo resto non nullo nell'algoritmo della divisione euclidea) per un fattore di $\mathbb{F}_7[X]$, che è monico; quindi X^2+1
 $\text{MCD}(P, Q) = X^2+1$

adesso bisogna trovare $\alpha, \beta \in \mathbb{F}_7[X]$ t.c. $\alpha P + \beta Q = S = X^2+1$

$$2(X^2+1) = Q - (X+4)P$$

$$4 \cdot 2(X^2+1) = 4Q - 4(X+4)P$$

$$X^2+1 = 4Q + (3X+5)P \quad \alpha = 4 \quad \beta = 3X+5$$

→ analogo di polinomio monico

α e β non sono unicamente determinati, infatti: sugli interi $x, y \in \mathbb{Z}$ ($x, y \neq 0, 0$) $d = \text{MCD}(x, y) \in \mathbb{N}^*$ identità di Bezout $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ t.c. $a x + b y = d$. L'insieme delle soluzioni di quest'**equazione diofantea** (a, b) è infinito in quanto è dato da

$$\left\{ \left(a_0 - K \frac{y}{d}, b_0 + K \frac{x}{d} \right) \text{ t.c. } K \in \mathbb{Z} \right\} \text{ con } (a_0, b_0) \text{ soluzione particolare}$$

$\mathbb{Z} \xrightarrow{\text{d} \mid x, y} \mathbb{Z}$

infatti:

$$(a_0 - K \frac{y}{d})x + (b_0 + K \frac{x}{d})y = a_0 x - K \frac{y}{d}x + b_0 y + K \frac{x}{d}y = a_0 x + b_0 y = d$$

torniamo alla nostra identità di Bezout

$$\underbrace{X^2+1}_{d} = \underbrace{4Q}_{a_0 x} + \underbrace{(3X+5)P}_{b_0 y}$$

tutte le soluzioni dell'equazione $AQ + BP = X^2+1$ sono date da

$$\left\{ \left(4 - M \frac{P}{X^2+1}, 3X + (5+M) \frac{Q}{X^2+1} \right) \text{ t.c. } M \in \mathbb{F}_7[X] \right\}$$

→ in $\mathbb{F}_7[X]$

Sottogruppi canonici di G_1

Sia $G_1 \xrightarrow{f} G_2$ omomorfismo (moltiplicativa)
costruzione canonica di un sottogruppo di G_1

Lemma $H = \{g \in G_1 \text{ t.c. } f(g) = 1_{G_2}\} = f^{-1}(\{1_{G_2}\}) \subset G_1$ è un sottogruppo $H \subset G_1$
questo è chiamato **nucleo di f** e si scrive $H = \text{Ker}(f)$

dim

$$a, b \in H \quad f(a) = f(b) = 1_{G_2}$$

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1_{G_2} \cdot 1_{G_2}^{-1} = 1_{G_2} \Rightarrow ab^{-1} \in H$$

$\hookrightarrow \text{Kernel}$

\Rightarrow sottogruppo di G_1

Lemma sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi si ha che $\text{Ker}(f) = \{1_{G_1}\} \iff f$ è iniettiva

dim

\Rightarrow

supponiamo che $\text{Ker}(f) = \{1_{G_1}\} (= \{x \in G_1 \text{ t.c. } f(x) = 1_{G_2}\})$

siano $x, x' \in G_1$ tali che $f(x) = f(x') \iff \underbrace{f(x) - f(x')^{-1}}_{= f(xx'^{-1})} = 1_{G_2} \iff x(x')^{-1} \in \text{Ker}(f) = \{1_{G_1}\} \iff$

$$\iff x(x')^{-1} = 1_{G_1}$$

allora $x(x')^{-1}x' = 1_{G_1}x' \iff x = x'$ quindi f iniettiva

\Leftarrow

supponiamo f iniettiva

sia $x \in \text{Ker}(f)$. Allora $f(x) = 1_{G_2}$ ma f è un omomorfismo di gruppi da cui deduco $f(1_{G_1}) = 1_{G_2}$ e f iniettiva quindi si deve avere $x = 1_{G_1}$ quindi $\text{Ker}(f) = \{1_{G_1}\}$



OSS il più piccolo sottogruppo contiene almeno l'elemento neutro

prop

link

sia $f: G_1 \longrightarrow G_2$ e $f(G_1) = \{y \in G_2 \text{ t.c. } \exists x \in G_1 \text{ con } f(x) = y\} \subset G_2$ allora $f(G_1) \subset G_2$
ovvero che se $y, y' \in f(G_1)$ allora $yy^{-1} \in f(G_1)$

dim

$$\exists x, x' \in G_1 \text{ t.c. } f(x) = y \quad f(x') = y' \Rightarrow yy^{-1} = f(x)f(x')^{-1} = f(xx'^{-1}) \in f(G_1) \quad \text{qui}$$

$$\in f(G_1) = \{z\}$$

$$\exists z \in G_1 \text{ t.c. } f(z) = yy^{-1} \in f(G_1)$$



\Rightarrow sottogruppo immagine

Sottogruppi coniugati: DEF
G gruppo e $H \triangleleft G$ (scelto)

$$H^g := \{g^{-1}h g \mid h \in H\} = g^{-1}Hg$$

qui
↳ coniugato di H per g

lo si può considerare una fabbrica di sottogruppi, infatti: preso un dato mi restituisce un sottogruppo

OSS se G è abeliano, $H^g = gHg^{-1} = gg^{-1}H = H \quad \forall g$

Lemma $H^g \triangleleft G$

dim

$a, b \in H^g$ posso scrivere per definizione

$$a = g^{-1}a'g \quad \exists a' \in H$$

$$b = g^{-1}b'g \quad \exists b' \in H$$

$$\text{quindi } b^{-1} = (g^{-1}b'g)^{-1} = g^{-1}b'^{-1}(g^{-1})^{-1} = g^{-1}b'^{-1}g$$

$$ab^{-1} = g^{-1}a'g g^{-1}b'^{-1}g = a'b'^{-1} \in H^g \quad \forall a, b \in H^g \quad \text{qui} \Rightarrow \text{visto } H^g \triangleleft H \triangleleft G \text{ abbiamo dimostrato } H^g \triangleleft H \triangleleft G$$

quindi $H^g \triangleleft G$ ■

método alternativo

diciamo, dato $g \in G$, un'applicazione

$$G \xrightarrow{fg} G$$

$$x \longmapsto f_g(x) = g^{-1}xg$$

↳ se cambia g cambia l'applicazione

per si parte da G e si arriva in G

OSS $\forall g f_g$ è un omomorfismo di gruppi (si parla di endomorfismo). Per verificarlo devo mostrare che $\forall a, b \in G \quad f_g(ab^{-1}) = f_g(a)f_g(b)^{-1}$

$$f_g(a)f_g(b)^{-1} = g^{-1}a g(g^{-1}b g)^{-1} = g^{-1}a g g^{-1}b^{-1}(g^{-1})^{-1} = g^{-1}a b^{-1}g = f_g(ab^{-1})$$

in che modo è una dimostrazione alternativa?

$H \triangleleft G_1$ e se $G_1 \xrightarrow{f} G_2$ omomorfismo allora $f(H) \triangleleft G_2$ qui

se $G_1 = G_2 = G$ e $f = fg$ otengo per ogni $H \triangleleft G$, $f_g(H) \triangleleft G \Rightarrow H^g \triangleleft G$

$$g^{-1}Hg = H^g$$

■

in generale $gH, Hg, Hg^{-1}, g^{-1}H, \dots \triangleleft G$

Gruppi di permutazioni DEF

Sia E un insieme finito

sia $S(E) := \{f: E \rightarrow E \text{ con } f \text{ biettiva}\}$

su $S(E)$ c'è l'operazione di composizione di applicazioni

$$\begin{array}{c} E \xrightarrow{f} E \xrightarrow{g} E \\ \hline E \xrightarrow{\text{fog}} E \end{array}$$

se $f, g \in S(E)$ allora $g \circ f \in S(E)$ inoltre $(g \circ f)^{-1} = f^{-1} \circ g^{-1} \Rightarrow (S(E), \circ, \text{Id}_E)$ è un gruppo

se $E = \{1, 2, \dots, n\} =: I_n$ ($n \geq 1$) allora si scrive $S_n = S(I_n)$

$f \in S_n$ $\{1, 2, \dots, n\}$ deve essere iniettiva

$$\{1, 2, \dots, n\}$$

ma questa risulta essere una rappresentazione non significativa di f

$$f \in S_n \quad \begin{pmatrix} 1 & 2 & \dots & n \\ \downarrow & \downarrow & & \downarrow \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

gli elementi di S_n si chiamano **permutazioni** (di I_n). S_n è chiamato il **gruppo simmetrico su n elementi**

es

$$\text{Id}_{I_n} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

l'ordine non conta, è uguale a $\binom{2}{2}^n$

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} = \{ \text{Id}_{I_1} \}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

Id_{S_2}

s-ciclo DEF

Una permutazione del tipo

$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{s-1} & a_s \\ a_2 & a_3 & a_4 & \dots & a_s & a_n \end{pmatrix}$$

che associa tramite Id

con $a_1, a_2, \dots, a_s \in I_n$ ($s \leq n$), che fissa quindi tutti gli elementi che non appartengono all'insieme $\{a_1, \dots, a_s\}$ si chiama **s-ciclo** e si scrive $(a_1, a_2, \dots, a_{s-1}, a_s)$

es

$$\Sigma_2 \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1 \ 2) \text{ è un 2-ciclo con } \alpha_1=1 \text{ e } \alpha_2=2$$

$$\Sigma_3 \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3) \text{ è un 3-ciclo}$$

$$\Sigma_5 \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (1 \ 3 \ 5) \text{ è un 3-ciclo } (n=5 \ s=3 \ \alpha_1=1 \ \alpha_2=3 \ \alpha_3=5)$$

oss tutti i cicli sono trasposizioni, ma non tutte le trasposizioni sono cicli:

oss l'identità è uno 0-ciclo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 4 & 1 & 3 & 7 \end{pmatrix} \in \Sigma_7 = (1 \ 6 \ 3 \ 5) \text{ è un 4-ciclo}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix} \in \Sigma_6 \text{ non è un ciclo in quanto gli elementi che non sono nel ciclo non sono fissati:}$$

Inversione

Invertire una permutazione consiste nell'invertire la direzione delle frecce al suo interno

es

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 7 & 5 & 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 6 & 7 & 5 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Composizione

Date due permutazioni la composizione consiste nell'unire le due permutazioni

es

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} = (1 \ 3 \ 4 \ 2)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix} = (1 \ 5 \ 3 \ 2 \ 4)$$

$$\sigma \circ \tau = \tau \circ \sigma = \sigma \circ \tau$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 4 \ 3)$$

$\Rightarrow \Sigma_5$ non è commutativo

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} = (1 \ 2 \ 5 \ 3)$$

Domanda

Qual è il più piccolo n tale che in S_n esiste una permutazione che non è un ciclo? $n=4$

descrizione di S_3

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \right\} = \{ \text{Id}, (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3), (1\ 3\ 2) \}$$

quindi in S_3 ogni permutazione è un s -ciclo con $s=0, 2, 3$

verifichiamo S_4

\rightarrow il prodotto di due cicli non necessariamente è un ciclo

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

verifichiamolo anche la composizione in $\{1, 2, 3, 4\}$

$$((1\ 2)(3\ 4))(1) = (1\ 2)((3\ 4)(1)) = (1\ 2)(1) = 2$$

ev₁((1\ 2)(3\ 4)) ev₂((3\ 4)) ev₁(1)

$$((1\ 2)(3\ 4))(2) = (1\ 2)((3\ 4)(2)) = (1\ 2)(2) = 1$$

$$((1\ 2)(3\ 4))(3) = (1\ 2)((3\ 4)(3)) = (1\ 2)(4) = 4$$

$$((1\ 2)(3\ 4))(4) = (1\ 2)((3\ 4)(4)) = (1\ 2)(3) = 3$$

Esercizio \rightarrow mi basta leggerlo al contrario = $(3\ 2\ 1)$

Mostrare che $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$ e che $(1\ 2\ 3)(1\ 3\ 2) = \text{Id}$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{Id}$$

Supporti disgiunti: DEF

Dati due cicli (a_1, \dots, a_s) e (b_1, \dots, b_t) di S_n si dice che sono a supporti disgiunti se $\{a_1, \dots, a_s\} \cap \{b_1, \dots, b_t\} = \emptyset$

più generalmente dati r cicli c_1, \dots, c_r di S_n sono a supporti disgiunti

es

$(1\ 2)(3\ 4)$ sono a supporti disgiunti in S_4

$(1\ 2)(3\ 4)(5\ 6)$ sono a supporti disgiunti in S_6

Teorema

Ogni $\sigma \in S_n$ può essere decomposto in prodotto di cicli a supporti disgiunti. Inoltre tali cicli sono unicamente determinati e commutano tra loro

OSS c'è un'analogia tra i cicli e i numeri nel teorema fondamentale dell'aritmetica

es

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 7 & 3 & 8 & 1 & 5 \end{pmatrix} = (1\ 2\ 4\ 7)(3\ 6\ 8\ 5) = (3\ 6\ 8\ 5)(1\ 2\ 4\ 7)$$

orbita $1 \rightarrow 2 \rightarrow 4 \rightarrow 7 \rightarrow 1$ $(1\ 2\ 4\ 7)$

$3 \rightarrow 6 \rightarrow 8 \rightarrow 5 \rightarrow 1$ $(3\ 6\ 8\ 5)$

Relazione su G

Sia G gruppo (notazione moltiplicativa) $H \subset G$. Introduciamo una relazione su G
 $x, x' \in G \quad x \sim x' \Leftrightarrow x(x')^{-1} \in H$

Lemma: \sim è d'equivalenza

dim

riflessiva $\rightarrow H \subset G \Rightarrow 1_H = 1_G \in H$. Ma $1_G = xx^{-1} \quad \forall x \in G$ da cui $x \sim x \quad \forall x \in G$

simmetrica $\rightarrow x \sim x' \Leftrightarrow x(x')^{-1} \in H$, ma $\forall a \in H, a^{-1} \in H$ quindi $(x(x')^{-1})^{-1} = x'(x)^{-1} \in H$ quindi $x' \sim x$

transitiva \rightarrow supponiamo $x \sim x'$ e $x' \sim x''$. Allora $x(x')^{-1}, x'(x'')^{-1} \in H$ ma allora (moltiplico gli elementi)

$$x(x')^{-1}x'(x'')^{-1} = x(x'')^{-1} \in H \text{ da cui } x \sim x''$$

Domanda: è possibile costruire su $\frac{G}{H}$ un'operazione binaria in modo tale che acquisisca una struttura di gruppo?

Talvolta sì, talvolta no. Quali condizioni?

Vorremmo che la seguente identità fosse valida

$$\bar{x} \cdot \bar{x}' = \bar{x} \cdot \bar{x}' \quad \text{indipendenza dei rappresentanti}$$

\downarrow operazione di G
 \downarrow nuova operazione

$$\begin{aligned} \text{Supponiamo } x \sim y &\Leftrightarrow \bar{x} = \bar{y} \Leftrightarrow xy^{-1} \in H \\ x' \sim y' &\Leftrightarrow \bar{x}' = \bar{y}' \Leftrightarrow x'(y')^{-1} \in H \end{aligned}$$

$$\star \\ \text{bisogna innanzitutto che } \bar{x} \bar{x}' = \bar{y} \bar{y}' \Leftrightarrow xx'(yy')^{-1} \in H = \underbrace{xx'}_{\in H} y^{-1} y'$$

questo suggerisce una definizione

Sottogruppo normale DEF

$$\rightarrow \forall h \exists h' \text{ t.c. } xh = h'x \Rightarrow xH = Hx$$

H è un sottogruppo normale di G se $\forall x \in G \quad xH = Hx$ si scrive $H \triangleleft G$

prop

Condizioni equivalenti:

link

- ① $H \triangleleft G$
- ② $\forall g \in G \quad \forall h \in H \quad \exists h' \in H \text{ t.c. } gh = h'g$
- ③ $\forall g \in G, H^g = H$

dim

Basta dimostrare che $\textcircled{3} \Rightarrow \textcircled{1} \Rightarrow \textcircled{2} \Rightarrow \textcircled{3}$ (si implicano ciclicamente)

$\textcircled{3} \Rightarrow \textcircled{1}$

$$H^g = g^{-1} H g$$

$$\text{se } H^g = H \Leftrightarrow g^{-1} H g = H \Leftrightarrow g g^{-1} H g = g H \Leftrightarrow H g = g H$$

$\textcircled{1} \Rightarrow \textcircled{2}$

$\forall g \in G, gH = \{x \in G \text{ t.c. } \exists h \in H \text{ con } x = gh \text{ e } Hg = \{y \in G \text{ t.c. } \exists h' \in H \text{ con } y = h'g\}$
quindi se $x \in gH = Hg$ allora $\exists h, h' \in H \text{ t.c. } x = gh = h'g$

$\textcircled{2} \Rightarrow \textcircled{3}$

$\forall g \in G \text{ e } \forall h \in H \exists h' \in H \text{ t.c. } gh = h'g$

moltiplicando per $g^{-1} \Rightarrow g^{-1}gh = g^{-1}h'g \Rightarrow h = g^{-1}h'g \forall h \in H \text{ e } \forall g \in G \Rightarrow H^g = H$



Questo consente di descrivere le classi d'equivalenza delle nostre relazioni.

Teorema

\rightarrow tutti gli elementi di G che sono multipli per un certo elemento di H

dato $g \in G$ si ha $\bar{g} = gH = Hg$. In particolare $\bar{1}_G = H$

dim



torniamo al calcolo $xx' y^{-1} y^{-1} \rightarrow$ inverti x e h

sia $H \trianglelefteq G$ allora $\underbrace{xx' (y^{-1})^{-1}}_{=: h \in H} = xhy^{-1} = hxy^{-1} \in H$

quindi $\overline{xx'} = \overline{yy'}$

In questo caso posso definire, su G/H , l'operazione $\bar{x} \cdot \bar{x}' := \overline{xx'}$

Siccome $\bar{x} = xH = Hx$ posso anche scrivere $\bar{x} \cdot \bar{x}' = xHx'H = Hx' = x'H$

$$= xx'HH = h \cdot h' \in H$$

$$= xx'H = \overline{xx'}$$

$$\hookrightarrow h' \in H \subset G$$

Teorema

sia $H \trianglelefteq G$ e \sim come prima (equivalenza) allora l'operazione su G/\sim $\bar{x} \cdot \bar{x}' := \overline{xx'}$ definisce una struttura di gruppo su G/\sim

si scrive $G/H = G/\sim$ gruppo quoziante di G per H
l'elemento neutro è $1_{G/H} = H$

Lemme l'applicazione $\begin{matrix} G & \xrightarrow{\pi_H} & G/H \\ g & \longmapsto & \bar{g} \end{matrix}$ è un omomorfismo di gruppi suriettivo



OSS G abeliano $H \triangleleft G \Rightarrow H \trianglelefteq G$ (tutti i sottogruppi sono normali in questo caso)

Per esempio \mathbb{Z} è un gruppo in notazione additiva che è abeliano

$\forall n \in \mathbb{N}^*, n\mathbb{Z}$ è un sottogruppo di \mathbb{Z} $\hookrightarrow_{a, b \in \mathbb{Z}, a - b \in \mathbb{Z}}$

$n\mathbb{Z} \triangleleft \mathbb{Z}$ e posso costruire sempre in notazione additiva $\mathbb{Z}/n\mathbb{Z}$ (sappiamo già farlo e la costruzione in questa lezione coincide con quella descritta in aritmetica modulare)

Inoltre G qualsiasi, $G \triangleleft G$, infatti $\forall x \in G \quad xG = Gx = \{G\}$ e $\{1_G\} \triangleleft G \quad \forall x \in G \quad x \cdot 1_G = 1_G \cdot x = x$

$$G/\{1_G\} = \{G\} \text{ t.c. } g \in G \}$$

dim

è suriettiva in quanto ogni classe contiene un suo rappresentante
inoltre $\pi_H(g(g')^{-1}) = \overline{g(g')^{-1}} = \overline{g} \overline{g'}^{-1} = \pi_H(g) \pi_H(g')^{-1}$ qui



OSS $\bar{g} = gh = Hg \in G$, infatti $g' \in \bar{g} \Leftrightarrow g'g^{-1} \in H \Leftrightarrow g' \in Hg$ si parla di classi laterali:

Lemma $G_1 \xrightarrow{f} G_2$ omomorfismo di gruppi: allora $\underbrace{\text{Ker}(f)}_{''H''} \triangleleft G_1$

Inoltre se $H \triangleleft G$ allora $H = \text{Ker}(\pi_H)$

dim

se $h \in G_1$ t.c. $f(h) = 1_{G_2}$ ($\Leftrightarrow h \in \text{Ker}(f)$). Mostriamo che $\forall g \in G_1$, $\text{Ker}(f)^3 = \text{Ker}(f)$

allora si ha $\forall x \in G_1$

\hookrightarrow definizione equivalente di \triangleleft

$$\begin{aligned} f(x^{-1}hx) &= f(x^{-1})f(h)f(x) = \\ &= f(x)^{-1}f(h)f(x) = \\ &= f(x)^{-1}f(x) = \xrightarrow{\hookrightarrow} 1_{G_2} \\ &= 1_{G_2} \end{aligned}$$

$$\Leftrightarrow x^{-1}hx \in \text{Ker}(f) \quad \forall h \in \text{Ker}(f), \quad \forall g \in G \Leftrightarrow \text{Ker}(f)^3 = \text{Ker}(f)$$

se $H \triangleleft G$ poniamo $f = \pi_H$, mostriamo che $H = \text{Ker}(\pi_H)$.

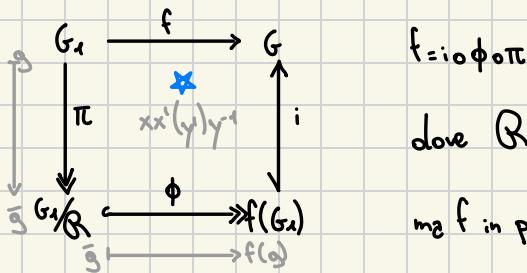
Ma se $g \in G$ soddisfa $\pi_H(g) = \overline{1_G}_H = H \Leftrightarrow gH = H \Leftrightarrow g \in H$

$$\downarrow \quad g \in \overline{1_G}_H = H = gH$$

Consideriamo un omomorfismo di gruppi $G_1 \xrightarrow{f} G$ (notazione moltiplicativa)

13/11

Allora è anche un'applicazione di insiemi non vuoti per il teorema di struttura delle applicazioni qui



$$f = i \circ \phi \circ \pi$$

dove R è la relazione $g, g' \in G_1, g R g' \Leftrightarrow f(g) = f(g')$
ma f in più è un omomorfismo di gruppi.

Verro per il primo teorema di omomorfismo

Mostriremo inoltre che tutte le 4 funzioni sono omomorfismi di gruppi

Notiamo che $g, g' \in G_1$, allora $f(g) = f(g') \Leftrightarrow f(g)f(g)^{-1} = 1_G \Leftrightarrow g(g')^{-1} \in \text{Ker}(f) \Leftrightarrow g \sim g'$

Quindi la relazione d'equivalenza su G definita da $g R g' \Leftrightarrow f(g) = f(g')$ è uguale alla relazione d'equivalenza \sim appena definita. Dunque si ha $G/\langle R \rangle \cong H$, che è un gruppo

Da questo si ha che π è un omomorfismo di gruppi come dimostrato precedentemente

Mostriamo ora che $\phi: G_1/\langle H \rangle \longrightarrow f(G_1)$ è un omomorfismo di gruppi

$$\bar{g} = gH \longrightarrow f(g)$$

$$f(g) \quad f(g)^{-1}$$

Ovvero si vuole mostrare che $\forall g, g' \in G_1$ si ha $\phi(gH)\phi((g'H)^{-1}) = \phi(g(g')^{-1}H)$ omo su f
ma $\phi(gH)(g'H)^{-1} = \phi(gHH(g')^{-1}) = \phi(gH(g)^{-1}) = \phi(g(g')^{-1}H) = f(g(g')^{-1}) = f(g)f(g)^{-1}$

$$\{g(H)^{-1}\} = \{(g^{'H})^{-1} \text{ t.c. } h \in H\} = \{h^{-1}(g')^{-1} \text{ t.c. } h \in H\} = \{h^{-1}(g)^{-1} \text{ t.c. } h \in H\}$$

sono tutti gli h in H (cambia solo la posizione)

Da cui l'identità voluta

Abbiamo dimostrato il teorema (primo teorema d'isomorfismo di gruppi)

Teorema (PRIMO TEOREMA D'ISOMORFISMO DI GRUPPI)

Dato $f: G_1 \longrightarrow G_2$ (omomorfismo di gruppi), esso si decompone in composizione $f = i \circ \phi \circ \pi$
come in $xx'(yy')^{-1}$

Altre proprietà dei gruppi

intersezione \rightarrow l'intersezione di sottogruppi di un gruppo dato è un sottogruppo

Lemme $H_1, \dots, H_n \subset G$ allora $\bigcap_{i=1}^n H_i \subset G$

dim

Siano $x, x' \in \bigcap_{i=1}^n H_i$ allora $\forall i=1, \dots, n \quad x(x')^{-1} \in H_i$ perché $H_i \triangleleft G$ ($\forall i$)
ma allora $x(x')^{-1} \in \bigcap_{i=1}^n H_i$ quindi si ha $\bigcap_{i=1}^n H_i \triangleleft G$



unione → l'unione di sottogruppi non è un sottogruppo

infatti $H_1 = \{1_G, (1\ 2)\}$, $H_2 = \{1_G, (1\ 3)\} \triangleleft G = S_3$
 $H_1 \cup H_2 = \{1_G, (1\ 2), (1\ 3)\} \subset G$

ma non è vero che $H_1 \cup H_2 \triangleleft G$, infatti $(1\ 2)(1\ 3) = (1\ 3\ 2)$ ma $(1\ 3\ 2) \notin H_1 \cup H_2$

$$\begin{matrix} \uparrow & \uparrow \\ x & (x')^{-1} \end{matrix}$$

Sottogruppo di G generato da I DEF

sia $I \neq \emptyset \subset G$

il sottogruppo di G generato da I è $\langle I \rangle := \bigcap_{\substack{H \triangleleft G \\ I \subset H}} H$

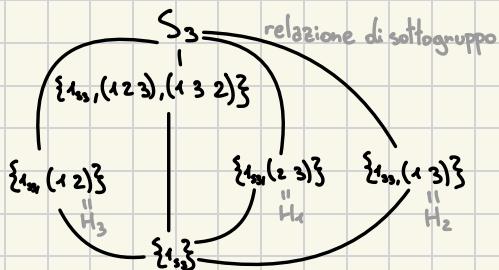
si chiama anche il più piccolo sottogruppo di G che contiene I

$I \rightsquigarrow \{\text{H} \triangleleft G \text{ t.c. } I \subset H\} \rightsquigarrow \bigcap_{i=1}^n H \triangleleft G$ (come dimostrato)

es

diagramma di Hasse di S_3

i sottogruppi di S_3 sono



$$\begin{aligned} \text{quindi } \langle (1\ 2) \rangle &= \{1_{S_3}, (1\ 2)^2\} := H_3 \\ \langle (1\ 2\ 3) \rangle &= \{1_{S_3}, (1\ 2\ 3), (1\ 3\ 2)\} \cap S_3 = \\ &= \{1_{S_3}, (1\ 2\ 3), (1\ 3\ 2)\} \\ \langle H_1 \cup H_2 \rangle &= S_3 \end{aligned}$$

Lemma dato G gruppo (notazione moltiplicativa) e $g \in G$ $\langle g \rangle = g^{\mathbb{Z}}$

dim

$$\langle g \rangle (= \langle \{g\} \rangle) = \bigcap_{\substack{H \triangleleft G \\ g \in H}} H$$

consideriamo l'insieme $\{1, g, g^2, \dots, g^{i_1}, g^{i_2}, \dots\} = \{g^n \text{ t.c. } n \in \mathbb{Z}\} = g^{\mathbb{Z}}$, dimostriamo che $g^{\mathbb{Z}} \subset G$
infatti $\forall x, x' \in g^{\mathbb{Z}} \exists n, n' \in \mathbb{Z} \text{ t.c. } x = g^n, x' = g^{n'} \Rightarrow x(x')^{-1} = g^{n-n'} \in g^{\mathbb{Z}}$

si ha che $\langle g \rangle \subset g^{\mathbb{Z}}$. D'altra parte $\langle g \rangle \subset G$ e $g \in \langle g \rangle \Rightarrow 1 = g^0 \in \langle g \rangle, g^1 \in \langle g \rangle, g^2 \in \langle g \rangle \dots g^{\mathbb{Z}} \subset \langle g \rangle$

ggⁱ gg^j

ggⁱ

gli unici sottogruppi di \mathbb{Z} sono $\{0\}$ e \mathbb{Z}

Lemma sia G un sottogruppo di \mathbb{Z} (notazione additiva), se $G \neq \{0\}$ allora $\exists n \in \mathbb{N}^*$ t.c. $G = n\mathbb{Z}$

supponiamo $G \neq \{0\}$ allora esiste un più piccolo $n \in G \cap \mathbb{N}^*$ (infatti G è stabile per $x_1 - x_2 \in G$)
sia $d \in G$ per la divisione euclidea ho $d = qn + r$ con $0 \leq r < n$
quindi $r = d - qn \in G$ come fa esserci su un gruppo in not add ??????

G
Ψ

se $r \neq 0$ si ha $r \in G$, ma $r \in \mathbb{N}^*$ contraddice la minimalità di n , quindi $r = 0$ e $d = n\mathbb{Z}$
quindi $G \subset n\mathbb{Z}$ ma $n\mathbb{Z} \subset G$ da cui $G = n\mathbb{Z}$



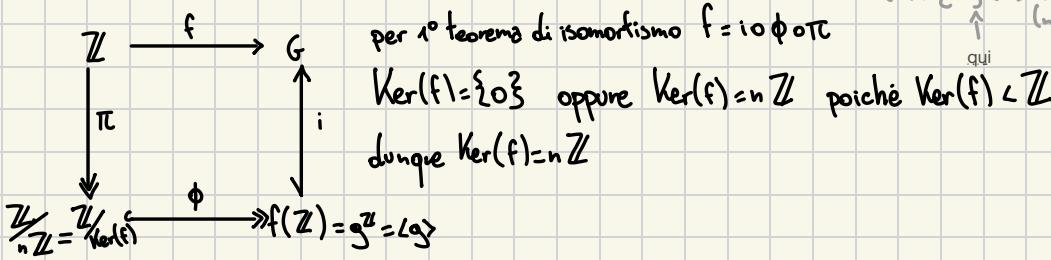
Lemma se $\#G < \infty$ (cardinalità finita) allora $\forall g \in G \exists n > 0$ t.c. $\langle g \rangle = g^{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$
l'intero n è chiamato $\text{ord}(g)$ (ordine di g)

dim

sia $\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & G \\ n \mapsto & & g^n \in g^{\mathbb{Z}} = \langle g \rangle \end{array}$ un omomorfismo di gruppi;

infatti $f(n-n') = g^{n-n'} = g^n g^{-n'} = f(n) f(n')^{-1}$

per questo lemma si ha
 $\text{Ker}(f) = \{0\} \Leftrightarrow f$ iniettiva
qui



dunque si ha che ϕ associa una classe di un multiplo di \mathbb{Z} a $g \in \{g^n \text{ t.c. } n \in \mathbb{Z}\}$
per cui ϕ risulta essere biettiva ma sapendo che ϕ è un omomorfismo allora si ha che
 $\mathbb{Z}/n\mathbb{Z}$ è isomorfa rispetto a $\langle g \rangle$



Minimo comune multiplo (mcm)

Dati: $m_1, \dots, m_k \in \mathbb{Z} \setminus \{0\}$, il minimo comune multiplo m di m_1, \dots, m_k è l'elemento intero $m \in \mathbb{N}^*$ tale che

- ① $m_1, \dots, m_k \mid m$
- ② se m' è tale che $m_1, \dots, m_k \mid m'$ allora $m \mid m'$.

Si scrive $m = \text{mcm}(m_1, \dots, m_k)$

Per calcolarlo ho due opzioni:

$$\textcircled{1} \quad m_1 \mathbb{Z} \cap m_2 \mathbb{Z} \cap \dots \cap m_k \mathbb{Z} = m \mathbb{Z}$$

$$\text{mcm}(a, b) = \frac{ab}{\text{MCD}(a, b)} \quad a, b \in \mathbb{N}^*$$

\textcircled{2} Utilizzo il teorema fondamentale dell'aritmetica

$$a = \prod_p p^{\nu_p(a)}$$

$$\Rightarrow \text{mcm}(a, b) = \prod_p p^{\max(\nu_p(a), \nu_p(b))}$$

$$b = \prod_p p^{\nu_p(b)}$$

Ordine di un elemento DEF

Sia G gruppo finito (notazione moltiplicativa) e $g \in G$

Allora $\{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\} \neq \emptyset$ infatti si ha l'omomorfismo $f: \mathbb{Z} \xrightarrow{n \mapsto g^n}$ che non può essere iniettivo essendo \mathbb{Z} infinito

non essendo iniettiva si ha $f(n_1) = f(n_2)$ ovvero $g^{n_1} = g^{n_2} \Rightarrow g^{n_1 - n_2} = 1_G$ con $d = |n_1 - n_2|$

Si pone $\text{ord}(g) := \min \{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\}$

allora $\langle g \rangle \cong \mathbb{Z}_{\text{ord}(g)} \mathbb{Z}$

$$f(n) := g^n = \begin{cases} \underbrace{1_G \dots 1_G}_{n \text{ volte}} & n \geq 0 \\ 1_G & n=0 \\ \underbrace{(g \dots g)}_{\text{In 1 volta}}^{-1} & n \leq 0 \end{cases}$$

es

$$g = (1 \ 2 \ 3) \in S_3 =: G$$

$$\mathbb{Z} \xrightarrow{n \mapsto (1 \ 2 \ 3)^n}$$

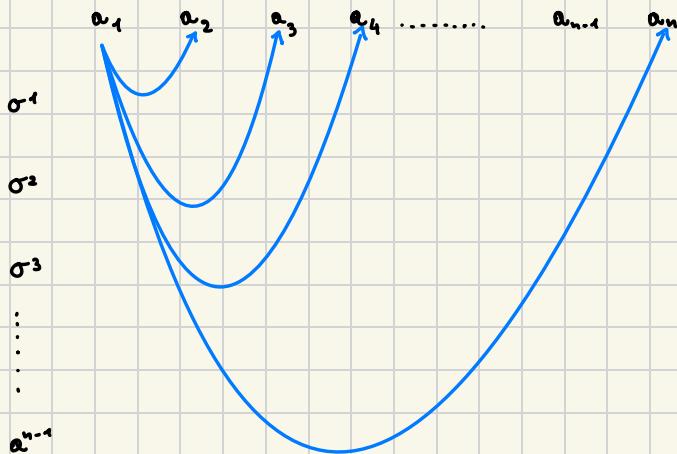
n	$(1 \ 2 \ 3)^n$
0	1_{S_3}
1	$(1 \ 2 \ 3)$
2	$(1 \ 3 \ 2)$
3	1_{S_3}
4	$(1 \ 2 \ 3)$

$$\rightarrow \text{ord}(1 \ 2 \ 3) = 3$$

$$\langle (1 \ 2 \ 3) \rangle \cong \mathbb{Z}_3 \mathbb{Z}$$

Lemma dato un n -ciclo di S_r $\sigma := (a_1 \ a_2 \ \dots \ a_n)$ $\text{ord}(\sigma) = n$ e $\langle \sigma \rangle \cong \mathbb{Z}_n$

In fatti osserviamo:



Quindi $\sigma^i \neq 1_{S_r}$ $\forall i = 1, \dots, n-1$

Inoltre $\sigma^n(a_1) = a_1$ ma $\sigma = (a_2 \ \dots \ a_n \ a_1)$ quindi $\sigma^n(a_2) = a_2$ e più generalmente $\sigma^n(a_i) = a_i$ $\forall i = 1, \dots, n$

Si come σ è un ciclo, esso fissa tutti gli elementi $b \in \{1, \dots, r\} \setminus \{a_1, \dots, a_n\}$
Quindi $\sigma^n = 1_{S_r}$ da cui $n = \text{ord}(\sigma)$

Come si calcola l'ordine di un elemento?

Se σ è un m -ciclo lo sappiamo, infatti: $\text{ord}(\sigma) = m$

Altrimenti si ha $\sigma \in S_n$. Per il teorema ^{qui} è possibile decomporlo in prodotto (commutativo) di cicli disgiunti: $\sigma = c_1 \ \dots \ c_s$

Lemma $\text{ord}(\sigma) = \text{lcm}(\text{ord}(c_1), \dots, \text{ord}(c_s))$

Esercizio calcolare $\text{ord}(\sigma)$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} \in S_n \quad n \geq 7$$

① decomponiamo σ in prodotto di cicli disgiunti.
 $(1 \ 7)(2 \ 4)(5 \ 6)$

$c_1 \quad c_2 \quad c_3$

② posso quindi calcolare $\text{ord}(\sigma)$
 $\text{ord}(\sigma) = \text{lcm}(2, 2, 2) = 2$

infatti

non metto il 3
perché fisso

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 6 & 5 & 1 \\ 1 & 2 & 4 & 5 & 6 & 7 \end{pmatrix} = 1_{S_n} \quad (n \geq 7)$$

\nearrow 2-ciclo
 $\text{ord}((5 \ 6)) = 2 \Rightarrow (5 \ 6)(5 \ 6) = 1$

alternativa $\sigma^2 = ((1 \ 7)(2 \ 4)(5 \ 6))^2 = (1 \ 7)(2 \ 4)(5 \ 6)(1 \ 7)(2 \ 4)(5 \ 6) = (1 \ 7)(2 \ 4)(5 \ 6)(6 \ 5)(2 \ 4)(1 \ 7) = 1_{S_n}$
es. $(1 \ 4 \ 7)(1 \ 3 \ 2)(1 \ 2 \ 3)(1 \ 7 \ 4) = 1_6$
 $(1 \ 3 \ 2)(1 \ 2 \ 3) = (1 \ 2 \ 3)(1 \ 2 \ 3)(1 \ 2 \ 3) = (1 \ 2 \ 3)^3 = 1_6$

Esercizio:

Trovare 2 cicli $\alpha, \beta \in S_8$ t.c. $(1 \ 2 \ 3 \ 4)(1 \ 3 \ 7) \alpha \beta = 1_{S_8}$

$$\alpha = (7 \ 3 \ 1) \quad \beta = (4 \ 3 \ 2 \ 1)$$

Esercizio

$$\text{ord}((1 \ 2)(3 \ 4 \ 5)) = \text{lcm}(2, 3) = 6$$

$$\text{ord}((1 \ 2)(2 \ 4 \ 5)) \Rightarrow \text{non sono 3 supporti disgiunti} \Rightarrow (1 \ 2)(2 \ 4 \ 5) = (1 \ 2 \ 4 \ 5) \Rightarrow \text{ord}((1 \ 2 \ 4 \ 5)) = 4$$

Esercizio

$$\text{ord}((1 \ 2)(1 \ 3)(1 \ 4)) = \text{ord}((1 \ 4 \ 3 \ 2)) = 4$$

$$1 \rightarrow 4 \rightarrow 4 \rightarrow 4$$

$$4 \rightarrow 1 \rightarrow 3 \rightarrow 3$$

$$3 \rightarrow 3 \rightarrow 1 \rightarrow 2$$

$$2 \rightarrow 2 \rightarrow 2 \rightarrow 1$$

Teorema

non necessariamente
a su perp disgiunto

Ogni permutazione si decomponе in prodotto di trasposizioni.
In generale una tale fattorizzazione è unica

15/11

Formula m-ciclo

$$\sigma = (a_1 \ a_2 \ \dots \ a_m) = (a_m \ a_{m-1}) (a_m \ a_{m-2}) \dots (a_m \ a_1)$$

(1 2)(1 2) → se lo aggiungo rimane vero

$$(a_1 \ a_2) (a_1 \ a_3) (a_1 \ a_4) = (a_1 \ a_4 \ a_3 \ a_2) = (a_1 \ a_3 \ a_2 \ a_4)$$

$$(1 \ 2 \ 3 \ 4 \ 5) = (5 \ 4)(5 \ 3)(5 \ 2)(5 \ 1)$$

Teorema "rinforzato"

Sia s il numero di trasposizioni in una fattorizzazione di $\sigma \in S_r$ allora $s \bmod 2$ è unicamente determinato (anche se se \mathbb{Z} non è unico)

La segnatura di σ è l'elemento $\varepsilon(\sigma) = (-1)^s \in \mathbb{Z}^\times$ con s il numero di trasposizioni in una tale fattorizzazione

Se ne deduce che $S_r \xrightarrow{\varepsilon} \mathbb{Z}^\times$ è un omomorfismo di gruppi:

$$\text{mostriamo che } \varepsilon(ab) = \varepsilon(a)\varepsilon(b) \quad a, b \in S_r$$

$$\text{supponiamo che } a \text{ e } b \text{ abbiano } s \text{ e } t \text{ trasposizioni} \Rightarrow \varepsilon(ab) = (-1)^{s+t} = (-1)^s(-1)^t = \varepsilon(a)\varepsilon(b)$$

C'è quindi un diagramma

$$\begin{array}{ccc} S_r & \xrightarrow{f} & \mathbb{Z}^\times \\ \downarrow \pi & \nearrow \cong & \\ S_r / \ker(\varepsilon) & \xrightarrow{\quad} & \end{array}$$

↳ infatti: $\varepsilon(S_r) = \mathbb{Z}^\times$

$$\begin{aligned} \varepsilon(\sigma) &= -1 \text{ dispari} \\ \varepsilon(\sigma) &= 1 \text{ pari} \end{aligned}$$

Come si calcola $\varepsilon(\sigma)$?

① si calcola la fattorizzazione di σ in prodotto di cicli disgiunti

$$\sigma = c_1 \dots c_k$$

$$\varepsilon(\sigma) = \varepsilon(c_1) \dots \varepsilon(c_k)$$

② si usa poi la "formula" da cui si deduce che se c è un r -ciclo, allora $E(c) = (-1)^{r-1}$

es $E((1\ 2)) = (-1)^{2-1} = -1$

altra "ricetta"

senza decomporre in prodotto di cicli disgiunti calcoliamo la segnatura di σ attraverso un procedimento grafico

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 5 & 8 & 6 & 1 & 2 \end{pmatrix} = \left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \right)$$

$$E(\sigma) = (-1)^{1^2} = -1$$

$$\left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \right) \quad E(\sigma) = (-1)^{\text{indice di incidenza invariante mod 2}} = -1$$

risolviamolo ora con l'altro metodo

Decomponiamo in cicli disgiunti

$$\sigma = (1\ 3\ 7)(2\ 4\ 5\ 8)$$

$$E(\sigma) = E((1\ 3\ 7)) \cdot E((2\ 4\ 5\ 8)) = (-1)^2 \cdot (-1)^3 = -1$$

Prodotto cartesiano di gruppi

siano G_1, G_2 gruppi (notazione additiva)
 $G_1 \times G_2 = \{(g_1, g_2) \text{ t.c. } g_1 \in G_1, g_2 \in G_2\}$

Definiamo su $G_1 \times G_2$ una struttura di gruppo nel modo seguente

$$(g_1, g_2), (g'_1, g'_2) \in G_1 \times G_2$$

$$(g_1, g_2) + (g'_1, g'_2) := (g_1 + g'_1, g_2 + g'_2)$$

operazione

verifichiamo se rispetta le proprietà dei gruppi:

$$\begin{aligned} \textcircled{1} \quad ((g_1, g_2) + (g'_1, g'_2)) + (g''_1, g''_2) &= (g_1 + g'_1, g_2 + g'_2) + (g''_1, g''_2) = (g_1 + g'_1 + g''_1, g_2 + g'_2 + g''_2) = \\ &= (g_1, g_2) + ((g'_1, g'_2) + (g''_1, g''_2)) \end{aligned}$$

$$\textcircled{2} \quad 0_{G_1 \times G_2} := (0_{G_1}, 0_{G_2})$$

$$(g_1, g_2) + (0_{G_1}, 0_{G_2}) = (g_1 + 0_{G_1}, g_2 + 0_{G_2}) = (g_1, g_2) = (0_{G_1}, 0_{G_2}) + (g_1, g_2)$$

$$\textcircled{3} \quad (g_1, g_2) - (g_1, g_2) = (0, 0) = -(g_1, g_2) + (g_1, g_2)$$

Questo definisce la struttura di gruppo (abeliano su G_1, G_2 lo sono)

OSS potremmo voler fare l'operazione su un gruppo in notazione mista, ad esempio G_1 (not +)

$$G_2 \text{ (not .)} \Rightarrow 1_{G_1 \times G_2} = (0_{G_1}, 1_{G_2})$$

Questa costruzione si estende a n gruppi G_1, \dots, G_n : si può costruire

$G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) \text{ t.c. } g_i \in G_i, \forall i = 1, \dots, n\}$ dotato di struttura di **prodotto cartesiano** o **prodotto diretto** di G_1, \dots, G_n e su G_1, \dots, G_n abeliano allora $G_1 \times \dots \times G_n$ è abeliano

$$\textcircled{4} \quad (\mathbb{R}, +)$$

possiamo costruire il gruppo $\mathbb{R}^n = \mathbb{R} \times \dots \times \mathbb{R}$: i cui elementi sono (x_1, \dots, x_n) con $x_i \in \mathbb{R} \forall i = 1, \dots, n$
 l'elemento neutro è $0 = (0, \dots, 0)$

Spazio vettoriale DEF

sia K un campo

sia V un insieme $\neq \emptyset$ munito dell'operazione binaria $V \times V \rightarrow V$ e di un'operazione $K \times V \rightarrow V$

$$(a, b) \mapsto a \cdot b$$

scalari
vettori

$$(\lambda, v) \mapsto \lambda \cdot v$$

- Si dice che V è uno spazio vettoriale su K se
- ① $(V, +)$ è un gruppo abeliano (di elemento neutro 0_V)
 - ② $\alpha(v+w) = \alpha v + \alpha w \quad \forall \alpha \in K, \forall v, w \in V$
 - ③ $(\alpha+\beta)v = \alpha v + \beta v \quad \forall \alpha, \beta \in K, \forall v \in V$
 - ④ $(\alpha\beta)v = \alpha(\beta v) \quad \forall \alpha, \beta \in K, \forall v \in V$
 - ⑤ $1 \cdot v = v \quad \forall v \in V$
 ϵK

OSS in V non ci sta elemento neutro per la moltiplicazione, quindi quello di K funge da neutro per ⑤

Le altre proprietà discendono automaticamente da queste. Per esempio $0_K \cdot v = 0_V \quad \forall v \in V$

Infatti, $0_V = 0_K \cdot v - 0_K \cdot v = (0_K + 0_K) \cdot v = 0_K \cdot v$

③

Per esempio, $V = K$ è uno spazio vettoriale su K

Più generalmente, sia K un campo, poniamo $V = K \times \dots \times K = K^n$ con l'operazione $+$ di prodotto cartesiano di gruppi; esso è un gruppo abeliano. Se 0 è elemento neutro di K , $0 = (0, \dots, 0)$ elemento neutro di K^n

Definiamo adesso una moltiplicazione $K^n \times V \longrightarrow V$

$$\begin{array}{ccc} V & & V \\ \overbrace{K \times K \times \dots \times K}^n & \longrightarrow & \overbrace{K \times \dots \times K}^n \\ (\lambda, (v_1, \dots, v_n)) & \longrightarrow & (\lambda v_1, \dots, \lambda v_n) \\ & & \downarrow \\ & & \lambda(v_1, \dots, v_n) \end{array}$$

Questa operazione soddisfa tutti gli assiomi dello spazio vettoriale dal ② fino al ⑤

infatti: $\lambda \cdot ((v_1, \dots, v_n) + (w_1, \dots, w_n)) = \lambda \cdot ((v_1 + w_1, \dots, v_n + w_n)) = (\lambda(v_1 + w_1), \dots, \lambda(v_n + w_n)) =$
 $= (\lambda v_1 + \lambda w_1, \dots, \lambda v_n + \lambda w_n) = \lambda(v_1, \dots, v_n) + \lambda(w_1, \dots, w_n)$

$$v = (v_1, \dots, v_n) \\ w = (w_1, \dots, w_n) \Rightarrow \lambda(v+w) = \lambda v + \lambda w$$

OSS La moltiplicazione di $v \in V$ per lo scalare $-1 \in K$ è l'opposto per la struttura di gruppo.
infatti, dato $v \in V$, $v + (-1) = (1 + (-1))v = 0 \cdot v = 0$

V con queste operazioni, è uno spazio vettoriale su K

Esempi di altri spazi vettoriali su K campo

① K^n , $n \in \mathbb{N}$ $K = K$ $K^0 = \{0\}$

\nwarrow spazio vettoriale
banale

② matrici m linee e n colonne a coefficiente in K

$$M_{m,n}(K) = \left\{ \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & | \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \text{ t.c. } a_{ij} \in K \forall i,j \right\} = \left\{ (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \text{ t.c. } a_{ij} \in K \forall i,j \right\}$$

con operazioni: addizione coefficiente per coefficiente e moltiplicazione per λ separatamente per ogni coefficiente

$$A = (a_{ij}), B = (b_{ij}) \in M_{m,n}(K) = K^{m \times n}$$

$$A+B = (a_{ij} + b_{ij}) \in M_{m,n}(K)$$

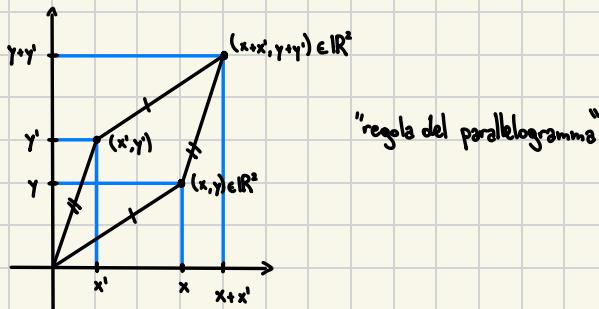
$$\lambda \in K \text{ t.c. } \lambda A = (\lambda a_{ij}) \in M_{m,n}(K)$$

\nwarrow spazio vettoriale su K

essenzialmente $M_{m,n}(K)$ è una riscrittura di $K^{m \times n}$ sottoforma di matrice. Per esempio $M_{2,3}(K) = K^{2 \times 3}$ è uguale (si dice isomorfo) a K^6 infatti

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2,3}(K) \xrightarrow[1:1]{\text{biunivoco}} (a, b, c, d, e, f) \in K^6$$

Rappresentazione grafica della somma di \mathbb{R}^2



③ polinomi a coefficienti in K campo

$$V = K[X] \quad f = f_0 + f_1 x + f_2 x^2 \dots$$

combinazioni
lineari

$$g = g_0 + g_1 x + g_2 x^2 \dots$$

$$f+g = f_0 + g_0 + (f_1 + g_1)x + \dots$$

sia $\lambda \in K \rightarrow$ costanti.

$$\lambda \cdot f = \lambda f_0 + (\lambda f_1)x + (\lambda f_2)x^2 + \dots$$

dunque dimenticandoci di un'operazione (moltiplicazione tra polinomi) ho ottenuto uno spazio vettoriale su K

? questionario?

Oss K finito (es. $K = \mathbb{F}_p$) ma $K[X]$ è infinito. Infatti contiene gli elementi: $1, x, x^2, \dots$ tutti distinti

④ $V = \mathbb{C}$ è uno spazio vettoriale su \mathbb{C}

da dove prendo gli
scalari

si ha anche che \mathbb{C} è uno spazio vettoriale su \mathbb{R} (o \mathbb{R} -spazio vettoriale)

$$\mathbb{C} = \{x+iy \text{ t.c. } x, y \in \mathbb{R}\} \quad \text{la struttura di gruppo abeliano è nota}$$

$$\lambda \in \mathbb{R}, z \in \mathbb{C} \quad z = x+iy, \quad \lambda \cdot z = \lambda(x+iy) = (\lambda x) + i(\lambda y)$$

Applicazione lineare **DEF**

Dati due spazi vettoriali V, V' su K , un'applicazione è detta **lineare** se $\forall x, y \in V$ e $\lambda \in K$

$$f(x+\lambda y) = f(x) + \lambda f(y) \quad f(\lambda x) = \lambda f(x)$$

op. su V op. su V'

Se f è biettiva si dice che f è **isomorfo**

Sia $f: V \rightarrow V'$ un isomorfismo, allora si dice che V e V' sono **isomorfi** e si scrive $V \cong V'$

Teorema di Lagrange

sia G gruppo finito e sia $H \subset G$ allora $\#H | \#G$

dim

abbiamo su G una relazione d'equivalenza associata ad H

$$x \sim y \Leftrightarrow xy^{-1} \in H$$

posso considerare l'insieme quoziente G/H allora $\#G/H < \infty$ partizionando qualcosa di finito ottenendo un numero finito di partizioni finite

Poniamo $[G:H] := \#G/H < \#G$

l'indice di H in G

Siccome G/H è una partizione di G allora $G = \bigsqcup_{c \in G/H} c$

↳ cardinalità finita

$$\text{quindi: } \#G = \sum_{c \in G/H} \#c$$

↳ numero finito di classi

claim $\#c = \#H$

se il claim è vero allora abbiamo il teorema di Lagrange

$$\text{infatti: } \#G = \sum_{c \in G/H} \#H = \#H \sum_{c \in G/H} 1 = \#H \cdot [G:H] \Rightarrow \#H | \#G$$

sommo $\#H$ per
 $\#G/H$ volte

dobbiamo dimostrare che $\forall c \in G/H \quad \#c = \#H$, per farlo ho bisogno di un secondo claim

claim 2 $\forall g \in G$ poniamo $\phi_g: G \xrightarrow{\quad} G$

$$x \mapsto xg$$

ϕ_g è una biezione

$$\text{o.s. } \phi_g(1_G) = g$$

se $g \neq 1_G$ allora ϕ_g non è un omomorfismo di gruppo $\phi_g(1_G) \neq 1_G$

Ma ϕ_g è invertibile da inversa $\phi_{g^{-1}}$. Infatti se $x \in G$ $\phi_g((\phi_{g^{-1}}(x))) = \phi_g(xg^{-1}) = xg^{-1}g = x \Rightarrow \phi_g \circ \phi_{g^{-1}} = \text{Id}_G$

$$\phi_{g^{-1}}((\phi_g(x))) = \phi_{g^{-1}}(xg) = xgg^{-1} = x \Rightarrow \phi_{g^{-1}} \circ \phi_g = \text{Id}_G$$

$$\text{Più generalmente } \phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \text{Id}_G$$

$\hookdownarrow gg^{-1}$

In particolare se $I \subset G$ allora $\#\phi_g(I) = \#I \rightarrow$ è una biezione, il numero di elementi è uguale.

Per terminare dimostriamo che $\forall c \in G/H \quad \exists g \in G$ t.c. $c = \phi_g(H) = Hg$

descriviamo una classe c

sia $x \in c$ allora $c = \{y \text{ t.c. } xy^{-1} \in H\}$ se $y \in x^{-1}H$
 $xy^{-1} \in H \Leftrightarrow x = hy \Leftrightarrow y = h^{-1}x \Leftrightarrow y \in Hx \Leftrightarrow c = Hx \Leftrightarrow c = \phi_x(H) \Rightarrow \#c = \#\phi_x(H) = \#H$

(es)

$$S_{12} \Rightarrow \#S_{12} = 12!$$

$13 \nmid 12!$ ma per il teorema di Lagrange $\exists H \subset S_{12}$ con $\#H = 13$ infatti $13 \nmid 12!$

se p primo e $p \mid \#S_{12}$ allora esiste $H \subset S_{12}$ t.c. $\#H = p$ in particolare $p = 2, 3, 5, 7, 11$

per trovare i sottogruppi basta prendere un p -ciclo

infatti se σ è un p -ciclo $\langle \sigma \rangle \cong \mathbb{Z}/p\mathbb{Z} \Rightarrow \#\langle \sigma \rangle = p$

biettiva

più generalmente $\forall n \leq 12 \exists H \subset G$ con $\#H = n$ ($\sigma = n$ -ciclo)

$$\hookrightarrow 12! = 12 \cdot 11 \cdot \dots \cdot 1$$

Sia $H \subset S_{12}$ è vero che $\#H \leq 12$? NO

$$S_{12} \xrightarrow{\epsilon} \mathbb{Z}^x = \{\pm 1\} \quad H = \ker(\epsilon)$$

per il primo teorema di isomorfismo si ha $\frac{S_{12}}{H} \cong \mathbb{Z}^x \Rightarrow \#\frac{S_{12}}{H} = 2 \Leftrightarrow [S_{12} : H] = 2$
quindi $12! = \#S_{12} = \#H \cdot 2 \Rightarrow \#H = \frac{12!}{2} \in \mathbb{N}$

$\hookrightarrow \forall c \in \frac{S_{12}}{H} \#c = \#H$ e sapendo che $\#\frac{S_{12}}{H} = 2$ allora $\#S_{12} = \sum_{c \in \frac{S_{12}}{H}} \#c = 2 \cdot \#H$

(es)

se $m \leq n$ allora c'è (almeno) un omomorfismo iniettivo $S_m \xrightarrow{f} S_n$ $f(S_m) \subset S_n$
 $\#f(S_m) = \#S_m = m!$ GIUSTO!

infatti f iniettivo $\Rightarrow S_m \cong f(S_m)$

dal teorema di isomorfismo di gruppi

$$\begin{array}{ccc}
S_m & \xrightarrow{f} & S_n \\
\downarrow & & \uparrow \\
S_m & \xleftarrow{\cong} & f(S_m) \\
\text{Ver}(f) = 1_{S_m} & \xleftarrow{\cong} & \\
\{1_{S_m}\} & & \\
\text{iff} & & \\
S_m & &
\end{array}$$

$$S_{12} \xrightarrow{f_m} \{ \sigma \in S_n \text{ t.c. } \sigma(m+1) = m+1, \sigma(m+2) = m+2, \dots, \sigma(n) = n \}$$

S_m è quindi il sottoinsieme di tutte le permutazioni in S_n che fanno oggetto degli elementi i con $i=m+1, \dots, n$

che sono $n-m$

Esercizio $m \in \mathbb{N}$

$f: S_m \longrightarrow S_n$

$$\sigma \mapsto \left(\begin{array}{c|cc} 1 & \dots & m \\ \downarrow \sigma & \downarrow \text{Id} & \downarrow \\ m+1 & \dots & n \end{array} \right)$$

è un omomorfismo iniettivo di gruppi che soddisfa quanto richiesto e $f(S_m) = S_m$

Gruppi ciclici

Sia G un gruppo e $g \in G$ di ordine $n \geq 1$, allora $\langle g \rangle \cong \frac{\mathbb{Z}}{n\mathbb{Z}}$

(es)

$$G = S_{12}$$

$$\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ \dots \ 12) \quad \text{ord}(\sigma) = 12$$

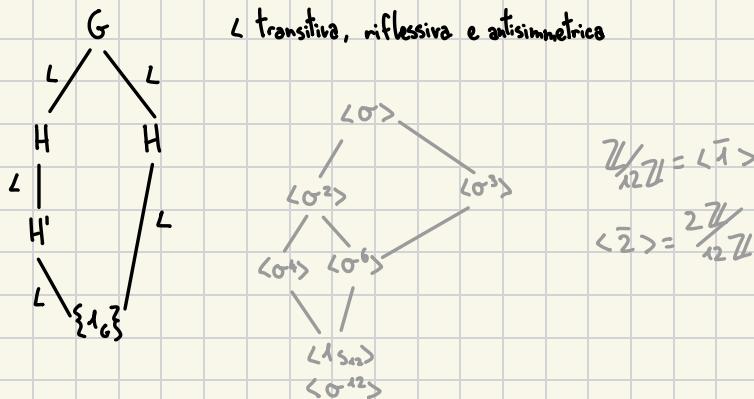
$$\text{quindi: } \langle \sigma \rangle \cong \frac{\mathbb{Z}}{12\mathbb{Z}}$$

un sottogruppo è ciclico se contiene un elemento di ordine n

$$\frac{\mathbb{Z}}{H\mathbb{Z}}$$

per ogni divisore d di 12 c'è un unico $H_d \subset G$ di cardinalità $\#H_d = d$

in più il diagramma di Hasse di un gruppo G è un grafo del tipo:



Sottospazio vettoriale DEF

21/11

dato V uno spazio vettoriale su K e $W \subset V$, $W \neq \emptyset$

W è un sottospazio vettoriale se è uno spazio vettoriale per le operazioni indotte da V . Ovvvero se, come gruppi abeliani, si ha $w \in W$ e se $w, w' \in W$ e $\lambda \in K$ si ha $\lambda w \in W$

\hookrightarrow

$\hookrightarrow W$ stabile

definizioni alternative

link

W è un sottospazio vettoriale di V se

- ① $\forall w, w' \in W$ si ha che $w + w' \in W$ (stabile per la somma)
- ② $\forall w \in W, \lambda \in K$ $\lambda w \in W$ (stabile per la moltiplicazione)

W è un sottospazio vettoriale di V se è stabile per combinazioni lineari nel senso seguente:

$\forall w, w' \in W$ e $\forall \lambda, \lambda' \in K$ si ha $\lambda w + \lambda' w' \in W$

combinazione lineare di w, w'

a coefficiente $\lambda, \lambda' \in K$

se $v_1, \dots, v_n \in V$ allora $\lambda_1 v_1 + \dots + \lambda_n v_n$ è combinazione lineare di v_1, \dots, v_n

W è un sottospazio vettoriale di V se $\forall w_1, \dots, w_n \in W$ si ha $\forall \lambda_1, \dots, \lambda_n \in K, \lambda_1 w_1 + \dots + \lambda_n w_n \in W$

W è un sottospazio vettoriale di $V \Leftrightarrow \forall w, w' \in W$ e $\lambda \in K$ si ha $w + \lambda w' \in W$

es) negativo

mostrare che $S = \{(x, y, z) \in \mathbb{R}^3 \text{ t.c. } x^2 + y^2 + z^2 = 1\}$ non è un sottospazio di \mathbb{R}^3

$$w = (1, 0, 0)$$

$$w' = (0, 1, 0) \Rightarrow w + \lambda w' = (1, 1, 0) \Rightarrow 1^2 + 1^2 + 0^2 = 2 \neq 1 \Rightarrow w + \lambda w' \notin S$$

$$\lambda = 1$$

altro modo

$0 \notin S$ ma ogni sottospazio vettoriale di \mathbb{R}^3 contiene $0 = (0, 0, 0)$

es) positivo

link

dato V spazio vettoriale su K e siano $v_1, \dots, v_n \in V$

poniamo $W = \text{Vett}_K(\{v_1, \dots, v_n\}) = \{\text{combinazioni lineari di } v_1, \dots, v_n\} = \{\lambda_1 v_1 + \dots + \lambda_n v_n \text{ t.c. } \lambda_1, \dots, \lambda_n \in K\}$

per vederlo consideriamo $w, w' \in W$ $\lambda \in W$ e $\lambda \in K$ e calcoliamo $w + \lambda w'$

$$\text{ma } w = \sum_{i=1}^n \lambda_i v_i, \quad w' = \sum_{i=1}^n \lambda'_i v_i$$

gli scalari non
necessariamente gli
stessi

$$\text{allora } w + \lambda w' = \sum_{i=1}^n (\lambda_i + \lambda \lambda'_i) v_i \Rightarrow w + \lambda w' \in W$$

K chiuso rispetto a somma e
moltiplicazione

oss $\text{Vett}(\{v_1, \dots, v_n\}) = \bigcap_{\substack{W \subset V \text{ sottospazio} \\ W \supset \{v_1, \dots, v_n\}}} W$

quindi è il più piccolo sottospazio vettoriale di V che contiene $\{v_1, \dots, v_n\}$ si chiama anche il sottospazio vettoriale generato da $\{v_1, \dots, v_n\}$ che talvolta si scrive $\langle v_1, \dots, v_n \rangle$

In particolare, l'intersezione di sottospazi vettoriali è un sottospazio vettoriale. Infatti dati W_1, W_2 sottospazi vettoriali $W_1 \cap W_2 \subset V$, sia $w \in W_1 \cap W_2$ sia $\lambda \in K$ allora $\lambda w \in W_1$ dato che W_1 è sottospazio vettoriale
l'intersezione di gruppi è un gruppo

di V (con $i=1,2$) quindi $\lambda w \in W_1 \cap W_2$

se W è sottospazio vettoriale di V allora $0 \in W$

Linearmente indipendenti DEF

dato V spazio vettoriale su K , $v_1, \dots, v_n \in V$ sono linearmente indipendenti (oppure lin. ind./l.i.) se dati $\lambda_1, \dots, \lambda_n \in K$

si ha che se $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$ allora $\lambda_1 = \dots = \lambda_n = 0 \in K$
 elemento neutro
 nei vettori elemento neutro
 negli scalari

Definizioni alternative

se l'unica combinazione lineare di v_1, \dots, v_n che è nulla è quella banale ovvero quella con $\lambda_1 = \dots = \lambda_n = 0$
 $v_1, \dots, v_n \in V$ ho quindi l'insieme di tutte le combinazioni lineari $\sum_i \lambda_i v_i \in V$. La combinazione lineare banale
 è la combinazione $\sum_i 0 \cdot v_i$:

v_1, \dots, v_n sono l.i. \Leftrightarrow l'unica combinazione lineare nulla è quella banale

se v_1, \dots, v_n non sono linearmente indipendenti allora si dice che essi sono linearmente dipendenti (lin. dip. o l.i.)
 cioè è equivalente all'esistenza di una combinazione lineare nulla che non è banale

E5

in \mathbb{R}^2 $v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ e $v_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$ sono l.i.

$$2v_1 + (-1)v_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix} - \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$$

in \mathbb{R}^2 $v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ $v_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$ sono l.i.

per vederlo consideriamo una combinazione lineare $\lambda_1 v_1 + \lambda_2 v_2 = 0$ nulli (\rightarrow nulla se sono lin. dip.)

$$\lambda_1 v_1 + \lambda_2 v_2 = 0 \Leftrightarrow \lambda_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 2 \end{pmatrix} = 0 \Leftrightarrow \begin{pmatrix} \lambda_1 \\ 2\lambda_1 \end{pmatrix} + \begin{pmatrix} 2\lambda_2 \\ 2\lambda_2 \end{pmatrix} = 0 \Leftrightarrow \begin{pmatrix} \lambda_1 + 2\lambda_2 \\ 2\lambda_1 + 2\lambda_2 \end{pmatrix} = 0 \Leftrightarrow$$

$$(\lambda_1) \text{ è soluzione del sistema lineare } \begin{cases} x_1 + 2x_2 = 0 & \text{soft termine} \\ 2x_1 + 2x_2 = 0 & 2\text{ termine} \end{cases} \Rightarrow 2x_1 - x_1 + 2x_2 - 2x_2 = 0 - 0 \Rightarrow x_1 = 0$$

sostituisco x_1 in (1) $\Rightarrow 0 + 2x_2 = 0 \Rightarrow x_2 = 0 \Rightarrow \lambda_1 = \lambda_2 = 0$

Esercizio

$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $v_2 = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}$ $v_3 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$ notare che v_1, v_2, v_3 sono l.i.

allora l'unica soluzione di $\begin{cases} \lambda_1 + 2\lambda_2 + \lambda_3 = 0 \\ 2\lambda_2 + 2\lambda_3 = 0 \\ + \lambda_3 = 0 \end{cases} \Rightarrow \begin{cases} \lambda_1 + 2\lambda_2 + 0 = 0 \\ 2\lambda_2 + 0 = 0 \\ \lambda_3 = 0 \end{cases} \Rightarrow \begin{cases} \lambda_1 + 0 = 0 \\ \lambda_2 = 0 \\ \lambda_3 = 0 \end{cases} \Rightarrow \lambda_1 = \lambda_2 = \lambda_3 = 0 \Rightarrow v_1, v_2, v_3$ sono l.i.

consideriamo adesso $v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $v_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $v_3 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$ essi sono l.d.

infatti: $2v_1 - v_2 + 0 \cdot v_3 = 0$ anche se la combinazione lineare è non banale. Quindi v_1, v_2, v_3 sono l.d.

Matrice triangolare DEF

una matrice $M \in M_{n,n}(\mathbb{R})$ è detta **triangolare** se si può scrivere come
 $\hookrightarrow M_n(\mathbb{R})$

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & \dots & \dots & m_{1n} \\ 0 & m_{22} & m_{23} & \dots & \dots & m_{2n} \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & m_{n-1,n-1} & m_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 & m_{nn} \end{pmatrix}$$

matrice triangolare (superiore)

E6

$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ è triangolare superiore

prop

link

coefficienti
diagonali

Le colonne di $M \in M_{n,n}(\mathbb{R})$ viste come vettori di \mathbb{R}^n sono lin. ind. $\Leftrightarrow m_{11}, m_{22}, \dots, m_{nn}$ sono tutti non nulli

(es)

mostrare che le colonne della matrice

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

sono l.d.

\hookrightarrow l.d. $\Leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 0 \\ 0 \end{pmatrix}$ sono l.d. (infatti $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ è l.d.)

$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}$ sono l.d. perché $\begin{cases} \lambda_1 + 2\lambda_2 + 3\lambda_3 = 0 \\ \lambda_2 + 2\lambda_3 = 0 \end{cases} \Rightarrow \begin{cases} \lambda_1 = \lambda_3 \\ \lambda_2 = -2\lambda_3 \end{cases}$ se pongo $\lambda_3 = 1$

Allora prendendo $(\lambda_1, \lambda_2, \lambda_3) = (1, -2, 1)$ si ottiene la combinazione lineare non banale ma nulla $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0$ ovvero $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = 0$

Più generalmente ho m vettori $v_1, \dots, v_m \in K^n$ e se $m > n$ allora v_1, \dots, v_m sono sempre l.d. (es. $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}$ sono 3 vettori di \mathbb{R}^2 che sono quindi l.d.)

Esercizio in K^n

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad \dots \dots \quad e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$\text{in } \mathbb{R}^3 \text{ si ha } e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Dimostrare che e_1, \dots, e_n sono l.i. e che, considerando inoltre il vettore $e_{n+1} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$ allora e_1, \dots, e_n, e_{n+1} sono l.d. e caratterizzare tutte le combinazioni lineari nulle ($\lambda_1 e_1 + \dots + \lambda_n e_n + \lambda_{n+1} e_{n+1} = 0$)

Sapendo che in e_1, \dots, e_n è presente un solo termine diverso da zero il sistema sarà del tipo

$$\begin{cases} \lambda_1 = 0 \\ \lambda_2 = 0 \\ \lambda_3 = 0 \\ \vdots \\ \lambda_n = 0 \end{cases}$$

\Rightarrow dunque l'unica soluzione di $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$ è quella banale

$$\left\{ \begin{array}{l} \lambda_1 + \lambda_{n+1} = 0 \\ \lambda_2 + \lambda_{n+1} = 0 \\ \lambda_3 + \lambda_{n+1} = 0 \\ \vdots \\ \lambda_n + \lambda_{n+1} = 0 \end{array} \right. \quad \left\{ \begin{array}{l} \lambda_1 = -\lambda_{n+1} \\ \lambda_2 = -\lambda_{n+1} \\ \lambda_3 = -\lambda_{n+1} \\ \vdots \\ \lambda_n = -\lambda_{n+1} \end{array} \right. \Rightarrow \text{risulta essere risotto } \forall \lambda_{n+1} \in K$$

tutte le soluzioni di $\{\lambda_1 v_1 + \dots + \lambda_n v_n \text{ t.c. } \forall \lambda_1, \dots, \lambda_n \in K\}$ sono del tipo

$$\lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n + \lambda_{n+1} e_{n+1} \Leftrightarrow -\lambda_{n+1} e_1 - \lambda_{n+1} e_2 - \dots - \lambda_{n+1} e_n + \lambda_{n+1} e_{n+1} \Leftrightarrow -\lambda_{n+1} (e_1 + e_2 + \dots + e_n - e_{n+1})$$

Esercizio $V = M_n(K)$

$$e_{ij} = \begin{pmatrix} & \overset{j}{\bullet} \\ \underset{i}{\bullet} & \end{pmatrix}$$

dove $e_{ii} = 1$, tutti gli altri sono zero

(es) $n=2$

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

mostrare che le matrici $(e_{ij})_{1 \leq i, j \leq n}$ sono l.i.

dovendo quindi mostrare che $\sum_i \sum_j e_{ij} \lambda_{ij} = 0$ ma poiché e_{ij} ha un solo vettore con un elemento diverso da 0 che in ogni matrice si trova in una posizione diversa della matrice, l'unica possibile soluzione è che $\lambda_{ij} = 0 \quad \forall i, j$

Prodotto di matrici

Cominciamo con diversi modi per rappresentare matrici di $M_{m,n}(K)$

sia $A \in M_{m,n}(K)$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$$

$$A = \begin{pmatrix} A_{11} \\ \vdots \\ A_m \end{pmatrix} \text{ con } A_i \text{ la } i\text{-esima riga di } A$$

$$A = (A^1, \dots, A^n) \text{ con } A^i \text{ la } i\text{-esima colonna di } A$$

es

$$A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2,3}(\mathbb{R})$$

$$A_1 = (a \ b \ c) \quad A_2 = (d \ e \ f)$$

$$A^1 = \begin{pmatrix} a \\ d \end{pmatrix} \quad A^2 = \begin{pmatrix} b \\ e \end{pmatrix} \quad A^3 = \begin{pmatrix} c \\ f \end{pmatrix}$$

Il prodotto scalare di matrice linea $U = (u_1, \dots, u_n) \in M_{1,n}(\mathbb{K})$ e matrice colonna $V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(\mathbb{K})$

$$\langle U, V \rangle = \sum_{i=1}^n u_i v_i = u_1 v_1 + \dots + u_n v_n$$

con questo prodotto scalare definiamo un'operazione $M_{m,n}(\mathbb{K}) \times M_{n,k}(\mathbb{K}) \longrightarrow M_{m,k}(\mathbb{K})$

$$A \cdot B = \left(\langle A_i, B_j \rangle \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

$$(A, B) \longmapsto A \cdot B$$

$$\downarrow$$

$$\begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} \longmapsto \begin{pmatrix} B^1 \\ \vdots \\ B^n \end{pmatrix} \in M_{n,1}(\mathbb{K})$$

$$\underbrace{A \cdot B}_{\in M_{2,2}(\mathbb{R})} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 & 1 \cdot 4 + 2 \cdot 5 + 3 \cdot 6 \\ 4 \cdot 1 + 5 \cdot 2 + 6 \cdot 3 & 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 \end{pmatrix} = \begin{pmatrix} 14 & 32 \\ 32 & 77 \end{pmatrix}$$

$$\underbrace{B \cdot A}_{\in M_{2,2}(\mathbb{R})} = \begin{pmatrix} 1 \cdot 1 + 4 \cdot 4 & 1 \cdot 2 + 4 \cdot 5 & 1 \cdot 3 + 4 \cdot 6 \\ 2 \cdot 1 + 5 \cdot 4 & 2 \cdot 2 + 5 \cdot 5 & 2 \cdot 3 + 5 \cdot 6 \\ 3 \cdot 1 + 6 \cdot 4 & 3 \cdot 2 + 6 \cdot 5 & 3 \cdot 3 + 6 \cdot 6 \end{pmatrix} = \begin{pmatrix} 17 & 22 & 27 \\ 22 & 2 & 36 \\ 27 & 36 & 49 \end{pmatrix}$$

Matrice identità $1_n, \text{Id}_n \in M_n(K)$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Quindi $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ si comporta, per il prodotto righe per colonne come elemento neutro.
Più generalmente, in $M_n(K)$, 1_n è la matrice

$$1_n := \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ 0 & & & 1 \end{pmatrix}$$

(es)

$$1_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Esercizi:

Esercizio 10. Sia G l'insieme delle matrici reali $2 \times 2 \left(\begin{array}{cc} a & b \\ c & d \end{array} \right)$, dove $ad - bc \neq 0$.
0. Dimostrare che G è un gruppo rispetto al prodotto matriciale (righe per colonne):

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \cdot \left(\begin{array}{cc} a' & b' \\ c' & d' \end{array} \right) = \left(\begin{array}{cc} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{array} \right)$$

È abeliano?

Esercizio 11. Sia G l'insieme delle matrici reali $2 \times 2 \left(\begin{array}{cc} a & b \\ 0 & d \end{array} \right)$, dove $ad \neq 0$.
Dimostrare che G è un gruppo rispetto al prodotto matriciale. È abeliano?

Esercizio 12. Sia G l'insieme delle matrici $2 \times 2 \left(\begin{array}{cc} a & b \\ c & d \end{array} \right)$, dove a, b, c, d sono interi modulo 2, e tali che $ad - bc \neq 0$. Dimostrare che G è un gruppo finito di ordine 6 rispetto al prodotto di matrici. È abeliano?

$$A, B \in M_{2,2}(K) = M_2(K) \quad A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \quad B = \begin{pmatrix} B^1 \\ B^2 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} \langle A_1, B^1 \rangle & \langle A_1, B^2 \rangle \\ \langle A_2, B^1 \rangle & \langle A_2, B^2 \rangle \end{pmatrix} \in M_{2,2}(K) = M_2(K)$$

Una matrice $A \in M_n(K)$ è invertibile se $\exists A' \in M_n(K)$ t.c. $AA' = A'A = 1_n$
 $GL_n(K) := \{A \in M_n(K) \text{ t.c. } A \text{ invertibile}\}$

↪ gruppo lineare

OSS generalmente il prodotto di matrici non è commutativo

$$K = \mathbb{R} \quad A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad B \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

\times somma

\times moltip.

Notare che $M_2(K)$, dotato delle operazioni di $+$, \cdot , con elementi neutri $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ e $1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, è un anello unitario (non commutativo)

anche se non dimostrato è anche associativo: $A(BC) = (AB)C$

$GL_2(K)$ non è abeliano

Ricapitolando A invertibile $\Leftrightarrow A \in GL_2(K) \Leftrightarrow A \in (M_2(K))^{\times}$
 ↴motto comune

determinante di una matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$

$$\det(A) := ad - bc \in K$$

Lemma $A, B \in M_2(K)$ allora $\det(AB) = \det(A) \cdot \det(B)$

K\{sos₁₁

Lemma $A \in M_2(K)$ è invertibile per la moltiplicazione di linee per colonne $\Leftrightarrow \det(A) \neq 0$ ($\Leftrightarrow \det(A) \in K^{\times}$)
 A invertibile $\Leftrightarrow \exists A' \in M_2(K)$ t.c. $A'A = AA' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_2$

dim

Mostriamo per cominciare che $\det(A) \neq 0 \Rightarrow A \in GL_2(K) \Rightarrow A$ invertibile

Poniamo $A' = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(K)$ moltiplico per ogni elemento della matrice

$$\text{Calcoliamo } A' \cdot A = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2$$

$$AA' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = Id_2$$

Scriviamo $A' = A^{-1}$: inversa di A

Mostriamo che $A \in M_2(K)^{\times} \Rightarrow \det(A) \neq 0$ utilizzando il lemma di sopra

$$\exists A' \text{ t.c. } AA' = A'A = Id_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

calcoliamo il determinante di ogni membro

$$\det(AA') = \det(A'A) = \det(Id_2) = 1 \neq 0$$

$$\det(A)\det(A') \quad \det(A')\det(A) \quad \Rightarrow \det(A), \det(A') \neq 0 \quad (K \text{ non ha divisori di } 0)$$

ne osservo che visto che $\det(A)\det(A') = 1$
 in K $\det(A) = \det(A') = 1$

Oss $\det(A) = \det(A^{-1}) = \det(A)^{-1} \Rightarrow$ il loro prodotto è l'elemento neutro di K

In particolare $\det: M_2(K)^{\times} \longrightarrow K^{\times}$ è un omomorfismo di gruppi

Sistemi lineari DEF

27/11

Dato un campo K . Un sistema lineare di m equazioni e n indeterminate a coefficienti in K è un sistema di equazioni del tipo

$$(*) \left\{ \begin{array}{l} \text{coefficiente } \in K \\ a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{array} \right.$$

termine noto/constante $\in K$

Risolvere il sistema significa descrivere l'insieme di tutti i vettori tali che le m equazioni sono

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \text{ soddisfatte simultaneamente}$$

Se il sottoinsieme $\text{Sol}(*)$ di K^n delle soluzioni del sistema $(*)$ è non vuoto, si dice che $(*)$ è **compatibile**, se $\text{Sol}(*) = \emptyset$, si dice che $(*)$ è **incompatibile**

(es)

$$\begin{cases} x_1=0 \\ x_1=0 \end{cases} \text{ è un sistema incompatibile} \quad \begin{cases} x_1=0 \\ \end{cases} \text{ è un sistema compatibile} \quad \text{Sol}(\{0\}) \subset K$$

I seguenti problemi sono importanti:

- ① Decidere se un sistema è incompatibile
- ② Descrivere tutte le soluzioni nel caso in cui sia compatibile
- ③ Nel caso sia compatibile descrivere l'insieme delle soluzioni attraverso l'insieme dei "parametri minimali"

Espressione matriciale di un sistema lineare su K

Il sistema $(*)$ si può risolvere alternativamente nel modo seguente

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} \in M_{m,n}(K)$$

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(K)$$

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in M_{n,m}(K)$$

$$AX = \begin{pmatrix} \langle A_1, X \rangle \\ \langle A_2, X \rangle \\ \vdots \\ \langle A_m, X \rangle \end{pmatrix} = \left\{ \begin{array}{l} \text{riga} \quad \text{colonna} \\ \downarrow \quad \downarrow \\ a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mm}x_m \end{array} \right.$$

quindi il sistema può essere riscritto in modo compatto attraverso l'equazione in matrice $A \cdot X = b$

es) ($m=n$)

$$A \in GL_n(K), \quad b \in M_{n,1}(K)$$

il sistema $AX=b$ è sempre compatibile e ammette un'unica soluzione (un vettore di soluzioni)

infatti sia A^{-1} l'inversa di A , allora $X \in M_{n,1}(K)$ è soluzione di (*) $\Leftrightarrow A^{-1}AX = A^{-1}b \Leftrightarrow X = A^{-1}b$

$$\text{Sol}(\ast) = \{X\} \text{ (singleton)}$$

Matrice completa associata ad un sistema lineare

Consideriamo un sistema lineare $AX=b$, tutti i dati sono contenuti nella matrice

$$(A|b) \in M_{m,n+1}(K)$$

\hookrightarrow matrice completa del sistema

La matrice completa è infatti la sovrapposizione di A e b

es)

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 1 & 5 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (A|b) = \begin{pmatrix} 1 & 2 & 3 & | & 0 \\ 2 & 3 & 4 & | & 0 \\ 1 & 5 & 1 & | & 1 \end{pmatrix}$$

se $b=0$ allora il sistema si dice **omogeneo** altrimenti è **non omogeneo**

es)

$$\begin{cases} 2x_1 + x_2 - 3x_3 + x_4 = 1 \\ x_3 + x_4 = 5 \\ x_1 - x_2 - x_3 - x_4 = 0 \end{cases}$$

$$A = \begin{pmatrix} 2 & 1 & -3 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & -2 \end{pmatrix} \quad b = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix} \quad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$(A|b) := \begin{pmatrix} 2 & 1 & -3 & 1 & | & 1 \\ 0 & 0 & 1 & 1 & | & 5 \\ 1 & -1 & -1 & -2 & | & 0 \end{pmatrix}$$

OSS $AX=b \Leftrightarrow x_1A^1 + x_2A^2 + \dots + x_nA^n = b \Leftrightarrow b$ è la combinazione lineare di $A^1, \dots, A^n \Leftrightarrow b \in \text{Vett}(A^1, \dots, A^n)$

$$\Leftrightarrow x_1 \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + x_3 \begin{pmatrix} -3 \\ 1 \\ -1 \end{pmatrix} + x_4 \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ è soluzione di (*) $\Leftrightarrow x_1A^1 + x_2A^2 + x_3A^3 + x_4A^4 = b$, ovvero (*) è compatibile $\Leftrightarrow b \in \text{Vett}_{\mathbb{R}}(A^1, A^2, A^3, A^4)$

es

$$\begin{cases} 2x_1 - x_2 - x_3 = 1 \\ x_1 + x_3 = 5 \end{cases} \Leftrightarrow x_1 \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & -1 & -1 \\ 1 & 0 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

questo sistema è compatibile $\Leftrightarrow \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix} \in \text{Vett}_{\mathbb{R}}(\begin{pmatrix} 2 & -1 & -1 \\ 1 & 0 & 1 \end{pmatrix})$

Struttura dell'insieme di soluzioni di un sistema lineare

Consideriamo il sistema $AX=b$ con $A \in M_{m,n}(\mathbb{K})$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(\mathbb{K})$, $b \in M_{m,1}(\mathbb{K})$

OSS se (*) è incompatibile poniamo $\text{Sol}(A|b) = \emptyset$

se è compatibile $\text{Sol}(A|b) = \{X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n \text{ t.c. } X \text{ è soluzione di (*)}\}$

prop

$\text{Sol}(A|b)$ è un sottospazio vettoriale di $\mathbb{R}^n \Leftrightarrow b=0$

dim

se $b \neq 0$

visto che $\text{Sol}(A|b) = \{X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ t.c. } A^1x_1 + A^2x_2 + \dots + A^nx_n = b\} \neq \emptyset$

in questo caso quindi S non è un s.v. di \mathbb{R}^n sottospazio vettoriale \Rightarrow spazio vettoriale \Rightarrow gruppo $\Rightarrow \exists 0$

supponiamo adesso che $b = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = 0$

mostriamo che $\text{Sol}(A|0)$ è sottospazio vettoriale di \mathbb{K}^n

siano $X, X' \in \text{Sol}(A|0)$ e $\alpha, \alpha' \in \mathbb{K}$, dovo mostrare che $\alpha X + \alpha' X' \in \text{Sol}(A|0)$

$X \in \text{Sol}(A|0) \Leftrightarrow AX = 0$

$X' \in \text{Sol}(A|0) \Leftrightarrow AX' = 0$

$$A(\alpha X + \alpha' X') = \alpha AX + \alpha' AX' = \alpha \cdot 0 + \alpha' \cdot 0 = 0 \Rightarrow \alpha X + \alpha' X' \in \text{Sol}(A|0)$$

Teorema

Supponiamo di avere un sistema $AX=b$ (*)
 $A \in M_{m,n}(K)$ $b \in M_{m,1}(K)$ $X \in M_{n,1}(K)$

Supponiamo inoltre che (*) sia compatibile ($\text{Sol}(A)b \neq \emptyset$), cioè è equivalente a $b \in \text{Vett}_n(A^*, A^*) \subset M_{m,n}(K)$

sia $X_0 \in \text{Sol}(A)b$, allora $\text{Sol}(A)b = X_0 + \text{Sol}(A)_{\text{0}}$

notare somiglianze con teorema cinese dei resti

dim

sia $X \in \text{Sol}(A)b$ allora $X = X_0 + X_{\text{0}}$

↑
soluzione
particolare
(non unica)

per mostrare che $\text{Sol}(A)b \subset X_0 + \text{Sol}(A)_{\text{0}}$ basta verificare che $X - X_0 \in \text{Sol}(A)_{\text{0}}$ ovvero
 che $A(X - X_0) = 0$

noi sappiamo che $\begin{array}{l} AX=b \\ AX_0=b \\ \hline A(X-X_0) \end{array} \Rightarrow \underbrace{AX-AX_0=0}_{A(X-X_0)} \Rightarrow X-X_0 \in \text{Sol}(A)_{\text{0}}$

mostreremo adesso che $\forall Y \in \text{Sol}(A)_{\text{0}}$ si ha che $X_0 + Y \in \text{Sol}(A)b$

$$A(X_0 + Y) = \underbrace{AX_0}_{b} + \underbrace{AY}_{0} \Rightarrow X_0 + Y \in \text{Sol}(A)b$$

b 0



es

$$\begin{cases} X_1 + 2X_2 + 2X_3 = 1 \\ X_2 - X_3 = 4 \\ X_3 = 5 \end{cases} \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix} \Rightarrow X_3 = 5 \quad X_2 = 9 \quad X_1 = -32$$

$$\text{Sol}(\ast) = \left\{ \begin{pmatrix} 1 \\ 9 \\ 5 \end{pmatrix} \right\}$$

equivalentemente, grazie al teorema precedente, posso scrivere $\text{Sol}(A)b = X_0 + \text{Sol}(A)_{\text{0}} =$
 $= \begin{pmatrix} -32 \\ 9 \\ 5 \end{pmatrix} + \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} \subset M_{3,1}(K)$
 $\text{Sol}(A)_{\text{0}}$

Algoritmo di Gauss

introduciamo una relazione sulle matrici complete di $M_{m,n+1}(K)$

$M, M' \in M_{m,n+1}(K)$ $M \sim M' \Leftrightarrow \text{Sol}(M) = \text{Sol}(M')$ è una relazione d'equivalenza

idea utilizzare un insieme "semplice" di trasformazioni su $M_{m,n+1}(K)$ che lascino invariate le classi di \sim + equivalenti

ogni classe ha per rappresentante una matrice a gradini (unica) nel quale la struttura delle soluzioni del sistema lineare è trasparente (si vedono subito)

operazioni elementari

- ① permutare le righe
- ② moltiplicare una riga per $\lambda \in K^*$ addizione spazi vettoriali
- ③ sostituire una riga con tale riga più un multiplo scalare di un'altra riga

Gauss ha mostrato che operando con un numero finito di operazioni ① ② ③ su una matrice M , se ne ottiene un'altra M' con $M \sim M'$

oppure

date due matrici $M, M' \in M_{m,n}(K)$ scriviamo $M \sim M' \Leftrightarrow M' \text{ si può ottenere da } M \text{ attraverso un numero finito di operazioni } ① ② ③$

rel'deq

Teorema

$M \sim M' \Rightarrow M \sim M'$ (non possiamo trovare tutte le soluzioni)

es

i sistemi lineari associati alle matrici seguenti ammetteranno lo stesso insieme di soluzioni

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 2 & 2 & 4 \end{array} \right) \xrightarrow{R_3 \rightarrow \frac{1}{2}R_3} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 1 & 1 & 1 & 2 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 1 & -1 & 1 \\ 1 & 1 & 1 & 2 \end{array} \right) \xrightarrow{R_3 \rightarrow R_3 - R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right) \xrightarrow{R_1 \rightarrow R_1 - R_2} \left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

per il teorema $\Rightarrow \text{Sol}(\begin{cases} x+2z=1 \\ y-z=1 \end{cases}) = \text{Sol}(M)$

matrice a gradini
non ridotta

matrice a gradini
ridotta

$$E = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in M_3(\mathbb{R}) \mid \text{t.c. } \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}, z \in \mathbb{R} \right\}$$

$x = 1 - 2z$ soluzione del sistema associato $\text{Vett}_{\mathbb{R}}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}\right)$
 $y = 1 + z$
 $z = z$ (indipendente)

Matrice a gradini

Il numero di zeri alla riga successiva è strettamente superiore al numero di zeri di quella attuale

$$\left(\begin{array}{cccc|cc} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & 0 & 1 & * & \dots \\ 0 & \dots & 0 & 0 & 0 & 1 & * \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 \end{array} \right)$$

casi estremi

$$\left(\begin{array}{cccc|ccccc} 1 & * & & & & \dots & * \\ 1 & * & & & & \dots & * \\ 1 & * & & & & \dots & * \\ 1 & * & & & & \dots & * \\ 1 & * & & & & \dots & * \\ 1 & * & & & & \dots & * \\ 1 & * & & & & \dots & * \end{array} \right) \quad \left(\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \right)$$

più formalmente A è a gradini

- 1) se $A_{ii}=0 \Rightarrow A_{jj}=0 \forall j > i$
- 2) se $A_{ii} \neq 0$ allora il primo coefficiente non nullo (**pivot**) è un 1
Si ha inoltre, ponendo $j = \min\{k \mid \text{t.c. } a_{ik}=0\}$ che $a_{ij}=1$
- 3) se il pivot della riga i appare nella colonna j allora allora il pivot della riga $i+1$ appare nella colonna $h > j$

matrice a gradini ridotta

$$\left(\begin{array}{cccc|ccccc} 0 & \dots & 0 & 1 & * & 0 & \dots & * \\ 0 & \dots & 0 & 0 & 1 & * & 0 & \dots & * \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & \dots & 0 \end{array} \right)$$

una matrice a gradini è detta ridotta se dato un pivot in modo tale che $a_{ij}=1$ allora $\forall k \in \{1, \dots, i-1\} \quad a_{kj}=0$

Teorema (algoritmo di Gauss)

$$\forall M \in M_{m,n+1}(K) \quad \exists \Gamma \in M_{m,n+1}(K) \quad M \sim \Gamma$$

ovvero, partendo da qualsiasi matrice, è possibile arrivare ad una matrice a gradini con le operazioni

(es)

$$(A|b) = \left(\begin{array}{cccc|c} 1 & 1 & -1 & -2 & 4 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_2 \leftrightarrow R_2 - R_1} \left(\begin{array}{cccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & -1 & 0 & 2 & -4 \\ 0 & 1 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 \cdot (-1)} \left(\begin{array}{cccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 1 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_3 \rightarrow R_3 - R_2} \left(\begin{array}{cccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 3 & -6 \end{array} \right) \sim$$

$$\xrightarrow{R_3 \rightarrow \frac{1}{3}R_3} \left(\begin{array}{cccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{array} \right)$$

Teorema (algoritmo di Gauss)

$\forall M \in M_{m,n+1}(K) \exists \Gamma \in M_{m,n+1}(K) M \sim \Gamma$

ovvero, partendo da qualsiasi matrice, è possibile arrivare ad una matrice a gradini ridotta

es) continuiamo il precedente

$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_1 - R_2} \begin{pmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix} \xrightarrow{R_2 \leftrightarrow R_2 + 2R_3} \begin{pmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

✓ 3 gradini
ridotta

$$Sol(M) = Sol\left(\begin{cases} x-2=0 \\ y=0 \\ z=-2 \end{cases}\right) = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in M_{4,1}(K) \text{ t.c. } \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + z \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + Vett_{IR} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

$$\text{ma } Sol(M) = \begin{pmatrix} -1 \\ 0 \\ -1 \\ -2 \end{pmatrix} + Vett_{IR} \left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right) \text{ infatti, per la dimostrazione del primo teorema } \begin{pmatrix} -1 \\ 0 \\ -1 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Esercizio

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 0 & 2 & 3 \end{pmatrix} \in M_{3,6+1} \sim \begin{pmatrix} 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix} \xrightarrow{R_3 \leftrightarrow R_3 - R_2} \begin{pmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_1 + R_2}$$

$$\xrightarrow{R_3 \leftrightarrow R_3 - R_2} \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix}$$

$$Sol(M) = Sol\left(\begin{cases} z = \frac{1}{2} \\ t = 0 \\ u = \frac{3}{2} \end{cases}\right) = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \\ u \\ v \end{pmatrix} \in M_{6,1}(IR) \text{ t.c. } \begin{pmatrix} x \\ y \\ z \\ t \\ u \\ v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix} + x \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\} = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix} + Vett_{IR} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)$$

→ 2 variabili indipendenti

Esercizio

Dire se il sistema seguente è compatibile e determinare tutte le soluzioni ($K = \mathbb{R}$)

$$(*) \begin{cases} 2x+3y-2z=1 \\ y-z=2 \\ x+y+z=-2 \end{cases}$$

per soluzioni di (*) si intende le matrice colonna $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ tali che le tre equazioni in (*) sono simultaneamente soddisfatte

Si ha nella notazione introdotta

$$(A|b) = \left(\begin{array}{ccc|c} 2 & 3 & -2 & 1 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right)$$

usiamo ora l'algoritmo di Gauss

$$(A|b) = \left(\begin{array}{ccc|c} 2 & 3 & -2 & 1 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right) \xrightarrow[L_2 \leftrightarrow L_3]{L_1 \rightarrow L_1 - 2L_3} \left(\begin{array}{ccc|c} 0 & 1 & -4 & 5 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right) \xrightarrow[L_1 \rightarrow L_1 - L_2]{L_3 \rightarrow L_3 - L_2} \left(\begin{array}{ccc|c} 0 & 0 & -3 & 3 \\ 0 & 1 & -1 & 2 \\ 1 & 0 & 0 & -4 \end{array} \right) \xrightarrow[L_1 \leftrightarrow L_3]{L_3 \rightarrow -\frac{1}{3}L_3} \left(\begin{array}{ccc|c} 0 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 1 & 0 & 0 & \frac{4}{3} \end{array} \right) \xrightarrow[L_2 \leftrightarrow L_3]{L_1 \rightarrow L_1 + L_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & -2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & \frac{4}{3} \end{array} \right) \xrightarrow[L_1 \rightarrow L_1 - L_2]{L_3 \rightarrow L_3 - \frac{4}{3}L_1} \left(\begin{array}{ccc|c} 1 & 0 & 2 & -4 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -\frac{4}{3} \end{array} \right) \xrightarrow[L_3 \rightarrow L_3 + 4L_1]{L_1 \rightarrow L_1 - 2L_3} \left(\begin{array}{ccc|c} 1 & 0 & 0 & -4 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -\frac{4}{3} \end{array} \right)$$

matrice 3 gradini
al contrario quindi lo scambio

$$\xrightarrow[L_2 \leftrightarrow L_3]{L_1 \rightarrow L_1 - L_2} \left(\begin{array}{ccc|c} 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right) \xrightarrow[L_1 \rightarrow L_1 - L_2]{L_1 \rightarrow L_1 - L_3} \left(\begin{array}{ccc|c} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right) \Leftrightarrow \text{Sol } (*) = \left\{ \begin{pmatrix} -2 \\ 1 \\ -1 \end{pmatrix} \right\}$$

matrice 3 gradini
ridotta

variante

determinare l'insieme Σ dei valori del parametro $z \in \mathbb{R}$ t.c. il sistema

$$(*_z) \begin{cases} 2x+3y-2z=1 \\ y-z=2 \\ x+y+z=-2 \end{cases}$$

è compatibile, e per tali valori di z determinare tutte le soluzioni. adesso abbiamo solo 2 indeterminate (2 è termine costante)

Qui, $z \in \mathbb{R}$ è un parametro quindi il sistema è da considerarsi nelle indeterminate x, y , ovvero da risolversi in \mathbb{R}^2

$$A = \begin{pmatrix} 2 & 3 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1+2z \\ 2+z \\ -2-z \end{pmatrix}$$

$$(A|b) = \left(\begin{array}{cc|c} 2 & 3 & 1+2z \\ 0 & 1 & 2+z \\ 1 & 1 & -2-z \end{array} \right) \xrightarrow[L_1 \rightarrow L_1 - 2L_3]{L_2 \leftrightarrow L_3} \left(\begin{array}{cc|c} 0 & 1 & 5+4z \\ 0 & 1 & 2+z \\ 1 & 1 & -2-z \end{array} \right) \xrightarrow[L_1 \rightarrow L_1 - L_2]{L_3 \rightarrow L_3 - L_2} \left(\begin{array}{cc|c} 0 & 0 & 3+3z \\ 0 & 1 & 2+z \\ 1 & 0 & -2-z \end{array} \right) \xrightarrow[L_1 \leftrightarrow L_3]{L_3 \rightarrow L_3 - 3L_1} \left(\begin{array}{cc|c} 1 & 1 & -2-z \\ 0 & 1 & 2+z \\ 0 & 0 & 3+3z \end{array} \right)$$

Il sistema associato è $\begin{cases} x+y=-2-2 \\ y=2+2 \\ 0=3+32 \end{cases}$, ed è compatibile $\Leftrightarrow z=-1$ (altrimenti la terza equazione è contaddetta).
Quindi $\vec{x} = \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$

Sia adesso $z=-1$, il sistema diventa $\begin{cases} x+y=-1 \\ y=1 \\ 0=0 \end{cases} \Leftrightarrow \begin{cases} x+y=-1 \\ y=1 \\ 0=0 \end{cases}$ in forma triangolare superiore di soluzione
 $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$

Rango di una matrice DEF

data $A \in M_{m,n}(K)$, il rango di A è il numero di pivot di una sua forma a gradini (ridotta o non)
notazione $rg(A) \in \mathbb{N}$. $A \in M_{m,n}(K) \quad A=(0) \Leftrightarrow rg(A)=0$

OSS per definizione se la matrice A' è ottenuta a partire dalla matrice A applicando operazioni elementari, allora $rg(A) = rg(A')$. Infatti: non si può rendere una riga nulla attraverso le operazioni di Gauss

es

$$A = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 2 & 1 & 0 & 2 \\ 1 & 0 & -1 & 2 \end{pmatrix} \quad rg(A) = rg \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & -3 & -2 & -4 \\ 0 & -2 & -2 & -1 \end{pmatrix} = rg \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & -3 & -2 & -4 \\ 0 & 0 & -2 & 5 \end{pmatrix} = 3$$

$A_1 \rightarrow A_1 - 2A_2$
 $A_3 \rightarrow A_3 - A_1$

OSS ① una matrice $A \in M_{m,n}(K)$ può avere al massimo $rg(A) = \min(m, n)$

$$\left\{ \begin{pmatrix} 1 & & * \\ & 1 & \\ 0 & & 1 \end{pmatrix} \right\} \xrightarrow{rg(A) \leq n} \left\{ \begin{pmatrix} 1 & & * \\ & 1 & \\ 0 & & 1 \end{pmatrix} \right\} \xrightarrow{rg(A) \leq m}$$

② $rg(A) \leq rg(Alb)$ qualunque sia data colonna $b \in M_{m,1}(K)$

infatti: partendo da A, applico operazioni elementari, per trasformarla in questa matrice a gradini ridotta

$$\left(\begin{array}{c|c} 1 & \\ \hline 0 & \end{array} \right)$$

se rifaccio le stesse operazioni, sulla matrice completa, permane la struttura a gradini (non riguarda b)

$$\left(\begin{array}{c|c} 1 & \\ \hline 0 & \end{array} \right) \quad \left(\begin{array}{c|c} 1 & * \\ \hline 0 & * \end{array} \right)$$

l'unica cosa che potrebbe accadere è che ci possa essere un pivot in più

aumentando la matrice il rango non può diminuire

Teatro di Rouché-Capelli:

Si consideri il sistema (*) $AX=b$ con $A \in M_{m,n}(K)$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in M_{m,1}(K)$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in M_{n,1}(K)$

① il sistema (*) è compatibile $\Leftrightarrow \text{rg}(A) = \text{rg}(A|b)$ grado di libertà del sistema

② se (*) è compatibile poniamo $s := n - \text{rg}(A) > 0$

esistono allora vettori $v_1, \dots, v_s \in \text{Sol}(A|b)$ l.i. tali che $\text{Sol}(A|b) = \text{Vett}_K(v_1, \dots, v_s)$. Quindi dato $v_0 \in \text{Sol}(A|b)$ si ha $\text{Sol}(A|b) = v_0 + \sum_{i=1}^s K v_i$

(es) su esercizio precedente

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right) \quad \text{rg}(A) = \text{rg}(A|b) \Rightarrow \text{sistema compatibile}$$

$$s = n - \text{rg}(A) = 3 - 3 = 0 \quad \text{non ha gradi di libertà}$$

quindi $\text{Sol}(A|b) = \text{Vett}_K\left(\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\right)$ infatti si vede che la soluzione è unica $\left(\begin{matrix} -2 \\ 2 \\ -1 \end{matrix}\right) + \text{Sol}(A|b) = \left(\begin{matrix} -2 \\ 0 \\ 0 \end{matrix}\right)$

$$\left(\begin{array}{cc|cc} 1 & 1 & -2 & -2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 3 & 3 \end{array} \right) \quad \text{rg}(A) = 2$$

$\text{rg}(A|b)$ dipende dal parametro z e se $z \neq -1$ allora

$$\text{rg}(A) = 2 < 3 = \text{rg}(A|b) \Rightarrow \text{sistema incompatibile}$$

Esercizio

Studiare le soluzioni del seguente sistema lineare.

$$\begin{cases} x_2 - 2x_3 + x_4 - x_5 = 6 \\ x_3 - x_4 = -2 \\ x_1 - x_2 - x_3 - x_4 = 5 \\ x_2 + x_5 = 0 \end{cases}$$

$$\left(\begin{array}{ccccc|c} 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array} \right) \xrightarrow{\text{A}_1 \leftrightarrow \text{A}_3} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array} \right) \xrightarrow{\text{A}_2 \leftrightarrow \text{A}_4} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array} \right) \xrightarrow{\text{A}_3 \rightarrow \text{A}_3 - \text{A}_2} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 2 & -1 & 2 & -6 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array} \right)$$

$$\xrightarrow{\text{A}_3 \rightarrow \text{A}_3 - 2\text{A}_4} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 2 & -2 \end{array} \right)$$

Qui si vede che $r = \text{rg}(A) = \text{rg}(A|b)$ quindi per Rouché-Capelli, il sistema originale è compatibile.

Dato V uno spazio vettoriale su K $v_1, \dots, v_n \in V$, abbiamo studiato che

$$\text{Vett}_K(v_1, \dots, v_n) = \{ \alpha_1 v_1 + \dots + \alpha_n v_n \text{ t.c. } \alpha_1, \dots, \alpha_n \in K \}$$

Più generalmente se $S \neq ScV$ (qualsiasi), si pone $\text{Vett}_K(S) = \{ \text{combinazioni lineari finite di vettori } S \}$

Ovvero: $\text{Vett}_K(S) = \bigcap_{\substack{W \text{ sottospazio di } V \\ W \subseteq S}} W$

fatto $\text{Vett}_K(S)$ è un sottospazio vettoriale di V

(es)

$W \subset V$ sottospazio, allora $W = \text{Vett}_K(W)$

Sistema di generatori DEF

Se W sottospazio e $W = \text{Vett}_K(S)$ allora ScV è un sistema di generatori per W .

Se $\exists S$ finito con $W = \text{Vett}_K(S)$ allora W è finitamente generato (f.g.)

(es)

$$V = \mathbb{R}^2 \quad K = \mathbb{R}$$

$$v = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V \quad S = \{v\}$$

$$W = \text{Vett}_{\mathbb{R}}(S) = \text{Vett}_{\mathbb{R}}(v) = W = \{ \lambda v \text{ t.c. } \lambda \in \mathbb{R} \} = \text{insieme infinito}$$

ma $W = \text{Vett}_{\mathbb{R}}(S)$
 " $\text{Vett}_{\mathbb{R}}(v)$

Dato V spazio vettoriale in modo simile, ScV è libero o l.i. se, comunque scelto un sottoinsieme finito

$$F = \{v_1, \dots, v_n\} \subset S \text{ allora } v_1, \dots, v_n \text{ sono l.i.}$$

Ogni combinazione lineare finita di vettori di S nulla è banale

Base DEF

dato W un sotto spazio, ScW è una base (o sistema di generatori libero) di W se:

① S è un sistema di generatori di W ovvero $W = \text{Vett}_K(S)$

② S è libero

prop 1

Per ogni spazio vettoriale V/K esiste una base $B \subset V$. Inoltre date due basi $B, B' \subset V$, allora esiste una funzione biettiva $f: B \rightarrow B'$

In particolare, se esiste una base finita di cardinalità n , allora ogni base è finita, di questa stessa cardinalità

Dimensione DEF

Dato uno spazio vettoriale V_K f.g. la dimensione $\dim_K(V)$ è l'intero nel \mathbb{N} tale che ogni base B di V ha cardinalità n

Oss $\dim_K(V) = 0 \Leftrightarrow V \text{ è banale } (V = \{0\})$

Prop 2

Se W è un sottospazio vettoriale di V f.g. di dimensione n allora anche W è f.g. e detta l la sua dimensione $l := \dim_K(W)$, si ha $l \leq n \Rightarrow \dim(\text{sottosp}) < \dim(\text{spazio})$

Dato $B' = \{b_1, \dots, b_l\}$ base di W esistono vettori $b_{l+1}, \dots, b_n \in V$ t.c. $B = \{b_1, \dots, b_n\}$ sia una base di $V \rightarrow$ la base di uno sp. vett. contiene almeno tutti i vettori delle basi del sottosp.

Si ha che $l = n \Leftrightarrow W = V$

InvK

Applicazione alla nozione di range

Lemma data una matrice $A \in M_{m,n}(K)$ $\text{rg}(A) = \dim_K(\text{Vett}_K(A_1, \dots, A_m))$

dim sottospazio vettoriale di $M_{1,n}(K)$

se A' è la matrice a gradiini tale che $A \sim A'$ allora ogni riga di A' è combinazione lineare delle righe di A quindi $\text{Vett}_K(A'_1, \dots, A'_m) \subset \text{Vett}_K(A_1, \dots, A_m)$

per prop 2 si ha che $\dim_K(\text{Vett}_K(A'_1, \dots, A'_m)) \leq \dim_K(\text{Vett}(A_1, \dots, A_m))$

→ il numero di righe non varia

ma ogni trasformazione elementare di Gauss è invertibile (\sim è una relazione d'equivalenza) ??

Quindi $\dim_K(\text{Vett}_K(A'_1, \dots, A'_m)) = \dim_K(\text{Vett}(A_1, \dots, A_m))$

Si vede facilmente che $\dim_K(\text{Vett}_K(A'_1, \dots, A'_m)) = \text{rg}(A)$ infatti le righe contenenti i pivot sono l.i.

Applicazione alle soluzioni di un sistema lineare

Dato un sistema lineare $AX = b$, $M := (A|b)$

Il teorema di Rouché-Capelli si riformula:

① (*) è compatibile $\Leftrightarrow \dim_K(M^1, \dots, M^{n+1}) = \dim_K(A^1, \dots, A^n)$

② $\dim_K(\text{Sol}(A|b)) = n - \text{rg}(A)$

③ $\text{rg}(A) = \dim(\text{Vett}_K(A_1, \dots, A_m)) = \dim(\text{Vett}_K(A^1, \dots, A^n))$

Esercizio

Sia $K = K_d[X]$ il sottoinsieme dei polinomi di $V = K[X]$ di grado $\leq d$. Nota che W è un sottospazio vettoriale di $K[X]$

① Mostrare che $K_d[X]$ è f.g. e calcolare una base di $K_d[X]$

② Mostrare che V non è f.g. e calcolare una base

①

sia $P \in K_d[X] =: V$ allora $P = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$ con $a_0, \dots, a_n \in K$ e se $a_n \neq 0$ allora $n \leq d$
questo perché $\deg_x(P) \leq d$

$P \in \text{Vett}_K(1, X, X^2, \dots, X^d)$ ovvero $S = \{1, X, \dots, X^d\}$ è un sistema di generatori per $K[X]$. Siccome S è finito allora se ne deduce che $K_d[X]$ è f.g.

Calcoliamo adesso una base per $K_d[X]$. Si tratta di trovare un sistema di generatori che è anche l.i.
Ma un polinomio è nullo \Leftrightarrow i suoi coefficienti sono nulli, dunque, poiché un polinomio di $K_d[X]$ è una combinazione lineare di $1, X, \dots, X^d$ è quella banale allora $\{1, t, \dots, t^d\}$ è una base quindi $\dim_K(K_d[X]) = d+1$

grado di libertà

$S = \{1, X, \dots, X^d\}$ non è l'unica base infatti con $d=1$ si ha $S = \{1, X\}$ e se sostituisco X con $X+t$ e costruisco $S' = \{1, X+t\}$. S' è un sistema di generatori

$P = a_0 + a_1 X = a_0 + a_1(X+t) - a_1 = (a_0 - a_1) + a_1(X+t) \Rightarrow \forall P \in K_1[X] \text{ si ha che } P \in \text{Vett}_K(1, X+t) \Rightarrow K_1[X] \subset \text{Vett}_K(1, X+t)$

dimostra l'aveganza
e $K_1[X]$

Sia adesso $Q \in \text{Vett}(1, X+t) \Rightarrow Q = b_0 + b_1(X+t) = b_0 + b_1 + b_1 X \in K_1[X] \Rightarrow K_1[X] = \text{Vett}_K(1, X+t) = \text{Vett}_K(1, X)$
 $1, X+t$ sono l.i. $\{1, X+t\}$ è una base di $K_1[X]$

Dato d qualsiasi $\{1, X, \dots, X^d\}$ è una base di $K_d[X]$. Se sostituisco un elemento di questa base con un polinomio di $K_d[X]$ ottenuto:

① permutando

② moltiplicando per uno scalare

③ sostituendo con lo stesso polinomio più una combinazione lineare degli altri
ne viene fuori un'altra base

Più generalmente se $B = \{b_1, \dots, b_n\}$ è base di V , allora ponendo B' un sottoinsieme di V ottenuto attraverso ①②③, B' è un'altra base

Trovare in $K_3[X]$ un sistema di generatori che non è una base. Per esempio $\{1, 1, X, X^2, X^3\}$ è un sistema di generatori ($\forall P = a_0 + a_1 X + a_2 X^2 + a_3 X^3 \Rightarrow P \in \text{Vett}_K(\{1, 1, X, X^2, X^3\}) \subset \text{Vett}_K(\{1, 1, X, X^2, X^3\})$).

In generale se $S \subset S'$ allora $\text{Vett}_K(S) \subset \text{Vett}_K(S')$

La combinazione lineare $\lambda_1 \cdot 1 + \lambda_2 \cdot 1 + \lambda_3 X + \lambda_4 X^2 + \lambda_5 X^3$ con $\lambda_1 = -\lambda_2 = 1$ e $\lambda_3 = \lambda_4 = \lambda_5 = 0$ è non banale e nulla allora $\{1, 1, X, X^2, X^3\}$ non è libero

②

$V = K[X]$. Supponiamo per assurdo che V sia f.g.

$V = \text{Vett}_K(P_0, P_1, \dots, P_n)$ $P_i \in V = K[X]$. Sia $d = \max(\deg(P_i))$ $i = 0, \dots, n$ e un $P \in V$. Allora $P = \sum_{i=0}^n \lambda_i P_i$ con $\lambda_i \in K$. Ma $\deg(P) \leq \max(\deg(\lambda_i P_i)) = \max(\deg(P_i)) = n < \infty$

Sia $Q \in V$ di grado $n+1 \Rightarrow Q \in \text{Vett}_K(P_0, \dots, P_n)$ contraddizione. $B = \{1, X, X^2, \dots, X^n, \dots\}$

V per essere f.g. vuol dire che
 $V = \text{Vett}_K(S)$ con S finito ma per come è
definito V , allora S è infinito

Esercizio 1

Calcolare il range della matrice

$$M = \begin{pmatrix} -2 & 1 & 4 & -3 & 2 \\ 3 & -1 & -1 & 3 & 1 \\ 1 & 0 & 3 & 0 & -1 \\ 4 & 5 & 5 & 6 & 0 \end{pmatrix} \xrightarrow{\text{R}_4 \rightarrow R_4 + 2R_1} \begin{pmatrix} -2 & 1 & 4 & -3 & 2 \\ 3 & -1 & -1 & 3 & 1 \\ 1 & 0 & 3 & 0 & -1 \\ 0 & 7 & 13 & -12 & 4 \end{pmatrix} \xrightarrow{\begin{array}{l} R_1 \rightarrow R_1 + 2R_3 \\ R_2 \rightarrow R_2 - 3R_3 \\ R_4 \leftrightarrow R_3 \end{array}} \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & -1 & -10 & 3 & 4 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 7 & 13 & -12 & 4 \end{pmatrix} \xrightarrow{\begin{array}{l} R_2 \rightarrow R_2 + R_3 \\ R_4 \rightarrow R_4 - 7R_3 \end{array}}$$

$$\xrightarrow{\quad} \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 0 & -57 & * & * \end{pmatrix} \xrightarrow{\begin{array}{l} R_3 \rightarrow R_2 - R_4 \\ R_4 \rightarrow R_4 - R_3 \end{array}} \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 0 & -57 & * & * \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Il range è 3, uguale alla dimensione di $W = \text{VettIR}(\text{righe di } M)$ e le righe della matrice qui sopra, l.i. costituiscono una base di W

come è stato generato l'esercizio?

Scriviamo

$$a = (1 \ 2 \ 4 \ -3 \ -1)$$

$$b = (3 \ 1 \ 0 \ 0 \ 1) \in M_{1,5}(\mathbb{R})$$

$$c = (0 \ 2 \ 1 \ -3 \ 0)$$

La matrice $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \in M_{3,5}(\mathbb{R})$ ha range 3 e $M = \begin{pmatrix} a-b \\ b-c \\ a-c \\ a+b+c \end{pmatrix}$

\rightarrow combinazioni lineari di a,b,c che $\in \text{VettIR}(a, b, c) \in M_{1,5}(\mathbb{R})$

Esercizio 2

① In funzione del parametro λ , determinare il range della matrice

$$M_\lambda = \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & -2 & \lambda & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \in M_{4,7}(\mathbb{R})$$

② Supponiamo che M_λ sia la matrice completa associata a un sistema lineare $AX \stackrel{(v)}{=} b$. Determinare in funzione di λ se il sistema è compatibile, e la dimensione di $\text{Sol}(A|b)$

①

$$M_{\lambda} = \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & -2 & \lambda & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \underset{R_2 \leftrightarrow R_3}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \underset{R_4 \leftrightarrow R_2}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \end{pmatrix}$$

Adesso ci sono due casi:

- 1) $\lambda \neq 0$
- 2) $\lambda = 0$

1) $\lambda \neq 0$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \end{pmatrix} \underset{R_3 \rightarrow \lambda R_3}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 1 & \frac{4}{\lambda} & \frac{3}{\lambda} & -2 & \frac{6}{\lambda} & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \end{pmatrix} \underset{R_3 \rightarrow R_3 - R_2}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & \frac{-2}{\lambda} & \frac{3}{\lambda} + 2 & -2 & \frac{6}{\lambda} - 1 & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \end{pmatrix}$$

non ci possono essere due righe con il pivot nella stessa posizione

Ci sono di nuovo 2 casi:

- 1.1) $\lambda \neq 2$
- 1.2) $\lambda = 2$

1.1) $\lambda \neq 0, \lambda \neq 2$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & \frac{-2}{\lambda} & \frac{3}{\lambda} + 2 & -2 & \frac{6}{\lambda} - 1 & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \end{pmatrix} \underset{R_3 \rightarrow R_3 - \frac{1}{\lambda} R_2}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3\lambda}{4-2\lambda} & \frac{2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & -3 & 3 & -2 & \lambda - 2 & 4 \end{pmatrix} \underset{R_4 \rightarrow R_4 + 3R_3}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3\lambda}{4-2\lambda} & \frac{2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{4-\lambda}{4-2\lambda} & * & * \end{pmatrix}$$

non li calcolo perché scommetto sul fatto che non mi influenzano per il rango

$\lambda = 0$ per $\lambda = 2$

$\frac{-4-\lambda}{2-\lambda}$ non si annulla per $\lambda = 7$ allora nel caso $\lambda \notin \{0, 2\}$ $\operatorname{rg}(M_{\lambda}) = 4$

mi basta calcolare questo e se non si annulla per $\lambda = 7$ allora il rango non può scendere.
Se si annullasse dovrei calcolare il successivo ma per farlo dovrei calcolare quello nella riga superiore

1.2) $\lambda = 0, \lambda = 2$

$$M_2 \underset{\substack{R_3 \rightarrow \frac{2}{3}R_3 \\ R_4 \rightarrow -\frac{1}{3}R_4 \\ R_3 \leftrightarrow R_4}}{\sim} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{5}{2} & * & * & * \\ 0 & 0 & -3 & * & * & * & * \end{pmatrix} \Rightarrow \operatorname{rang} = 4$$

2) $\lambda = 0$

$$M_{\lambda=0} \xrightarrow{R_4 \rightarrow R_4 - 4R_3} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 0 & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & -2 & 4 \end{pmatrix} \xrightarrow{\frac{1}{4}R_4} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 0 & 6 & 4 \\ 0 & 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} \end{pmatrix} \xrightarrow{-\frac{1}{3}R_3 \rightarrow R_3 - 4R_4} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \end{pmatrix}$$

$$\xrightarrow{R_3 \rightarrow \frac{1}{2}R_3} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \\ 0 & 0 & 0 & 1 & * & * & * \end{pmatrix} \xrightarrow{R_3 \leftrightarrow R_4} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & * & * & * \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \end{pmatrix}$$

(2)

In ogni range di M_λ è 4. Scriviamo $M_\lambda = \left(\underbrace{A_\lambda}_{6} \mid \underbrace{b_\lambda}_{4} \right) \Big\}^4$

Il sistema (*) è compatibile $\Leftrightarrow \text{rg}(A) = \text{rg}(B)$ → devo verificare se i ranghi dei punti 1.1, 1.2, 2
 (cioè avviene (si verifica) in tutti i casi (1.1) (1.2) (2)) senza l'ultima colonna sono uguali al range di M
 $\dim(\text{Sol}(A_\lambda | b_\lambda)) = \# \text{ indeterminate} - \text{rg}(M_\lambda) = 6 - 4$

Si verifica che prop 1, prop 2 \Rightarrow prop 3

prop 3

dato V spazio vettoriale di dim n su K e sia $S \subset V$. Allora

link

① S libero $\Rightarrow \#S \leq \infty$ e $\#S \leq n$

② S generatore $\Rightarrow S$ è infinito oppure $\#S$ è finito ma $\#S \geq n$

③ In particolare S base $\Leftrightarrow S$ è finito, $\#S = n$ e S libero $\Leftrightarrow \#S \leq \infty$, $\#S = n$ e S generatore

prop 4

dato V spazio vettoriale su K .

$\{v_1, \dots, v_n\}$ è una base \Leftrightarrow ogni vettore di V si scrive in modo unico come combinazione lineare di v_1, \dots, v_n

dim

\Rightarrow

se $\{v_1, \dots, v_n\}$ è base di V allora è anche un sistema di generatori

quindi $\forall v \in V, v \in \text{Vett}(v_1, \dots, v_n)$ allora $\exists \alpha_1, \dots, \alpha_n \in K$ t.c. $v = \sum_{i=1}^n \alpha_i v_i$
 inoltre v_1, \dots, v_n sono l.i.

Mostriamo che $(\alpha_1, \dots, \alpha_n) \in K^n$ è unicamente determinato da (*)

Supponiamo di avere $(\beta_1, \dots, \beta_n) \in K^n$ t.c. $v = \sum_{i=1}^n \beta_i v_i$

Si ha quindi: $v = \sum_{i=1}^n \beta_i v_i = \sum_{i=1}^n \alpha_i v_i$

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n$$

sottraiamo: $0 = (\beta_1 - \alpha_1) v_1 + \dots + (\beta_n - \alpha_n) v_n$ ma v_1, \dots, v_n sono l.i. allora $\beta_1 = \alpha_1, \dots, \beta_n = \alpha_n$ da cui l'unicità

\Leftarrow

Supponiamo adesso che $\forall v \in V$, si possa scrivere in modo unico $v = \alpha_1 v_1 + \dots + \alpha_n v_n$

Allora $\{v_1, \dots, v_n\}$ genera V : $V = \text{Vett}_K(v_1, \dots, v_n)$, inoltre $0 = \alpha_1 v_1 + \dots + \alpha_n v_n$ per unicità $0 = 0v_1 + \dots + 0v_n$
 quindi v_1, \dots, v_n l.i.



Dato V uno spazio vettoriale su K di dim n e data una base $B = \{b_1, \dots, b_n\}$ allora ogni vettore

$v \in V$ si scrive in modo unico
 $v = v_1 b_1 + \dots + v_n b_n$ con $\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$

Tale vettore si chiama il vettore delle coordinate di v sulla base B si scrive $[v]_B$

prop

$\dim(B) = n$
 $V = K^n$ allora $B = (e_1, \dots, e_n)$ è una base di V dove $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$

Scriviamo la matrice M che ha per righe i coefficienti dei vettori e_1, \dots, e_n . Si ha

$$M = 1_n = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in M_n(K) \text{ a gradini ridotti con } n \text{ pivot. } \text{rg}(M) = n$$

da cui B libera e siccome $W = \text{Vett}_K(B) \subset V$ ha dim n , $W = V$ e B è base di V

La base $B = \{e_1, \dots, e_n\}$ si chiama **base canonica di K^n**



qui

Esercizio 4

In $M_{m,n}(K)$, ponendo

$$e_{ij} = \begin{pmatrix} 0 & & & \\ & \ddots & & 0 \\ & & 1 & \\ 0 & & & 0 \end{pmatrix} \in M_{m,n}(K) \quad \text{con } \begin{matrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{matrix}$$

$\{e_{ij} : \begin{matrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{matrix}\}$ è una base di $M_{m,n}(K)$ detta la base canonica e che $\dim(M_{m,n}(K)) = mn$

Esercizio 5

$V = \mathbb{R}^2$. Mostrare che $B = \{(1, 1), (1, -1)\}$ è una base di V .

Usiamo la prop 3. Ci sono diverse condizioni equivalenti al punto 3. Siccome $\#B = \dim_{\mathbb{R}}(V)$ in modo

Mostriamo che $\forall \begin{pmatrix} a \\ b \end{pmatrix} \in V$, si ha che $\begin{pmatrix} a \\ b \end{pmatrix}$ è combinazione lineare dei vettori $(1, 1)$ e $(1, -1)$

Ciò è equivalente al fatto che

$\begin{pmatrix} a \\ b \end{pmatrix} \in \text{Vett}_{\mathbb{R}}(B) : x_1(1, 1) + x_2(1, -1) = \begin{pmatrix} a \\ b \end{pmatrix} \quad \exists x_1, x_2 \in \mathbb{R} \iff \text{il sistema } (*) \begin{cases} x_1 + x_2 = a \\ x_1 - x_2 = b \end{cases} \text{ è compatibile}$

Per Rouché-Capelli, il sistema $(*)$ è compatibile $\iff \text{rg}(A) = \text{rg}(A| \begin{pmatrix} a \\ b \end{pmatrix})$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

→ la scalinata finisce prima della barra verticale

$$\left(\begin{array}{ccc} 1 & 1 & a \\ 1 & -1 & b \end{array} \right) \xrightarrow{L_2 \rightarrow L_2 - L_1} \left(\begin{array}{ccc} 1 & 1 & a \\ 0 & -2 & b-a \end{array} \right) \xrightarrow{-\frac{1}{2}L_2} \left(\begin{array}{ccc} 1 & 1 & a \\ 0 & 1 & \frac{a-b}{2} \end{array} \right) \xrightarrow{L_1 \leftrightarrow L_2} \left(\begin{array}{ccc} 1 & 0 & \frac{a+b}{2} \\ 0 & 1 & \frac{a-b}{2} \end{array} \right)$$

$$\text{rg}(A) = \text{rg}(A|b) \Rightarrow \mathbb{R}^2 = \text{Vett}_{\mathbb{R}}(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix})$$

Inoltre ho la soluzione unica di (*) $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a-b}{2} \end{pmatrix}$. Allora scrivendo $v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ si ha $[v]_{\mathbb{R}^2} = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a-b}{2} \end{pmatrix}$

II modo

Possiamo anche mostrare che B è libero

prop 3 $\Rightarrow B$ base visto che $2 = \#B = \dim_{\mathbb{R}}(V)$

Ma $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ che ha rango 2.

Le righe contenenti i pivot sono l.i.
qui

Quindi B è libero, quindi è una base di V

Questo metodo appare più semplice del precedente

preparazione all'esercizio 6

Trasposizioni di matrici DEF

Sia $A \in M_{m,n}(\mathbb{K})$. La trasposta di A (notazione ${}^t A$) è la matrice di $M_{n,m}(\mathbb{K})$ ottenuta da A scambiando righe con colonne

$$A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \quad {}^t A = (a_{ji})_{1 \leq i \leq m, 1 \leq j \leq n}$$

es

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \in M_{3,2}(\mathbb{R}) \quad {}^t A = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix} \in M_{2,3}(\mathbb{R})$$

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \in M_{2}(\mathbb{R}) \quad {}^t A = \begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix} \in M_{2}(\mathbb{R})$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad {}^t A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$$

oss basta effettuare una riflessione rispetto alla "diagonale"

$$\begin{pmatrix} * & * \\ * & * \\ * & * \\ * & * \end{pmatrix} \quad \begin{pmatrix} * & * \\ * & * \\ * & * \\ * & * \end{pmatrix}$$

foto

data $A \in M_{m,n}(K)$ allora $\text{rg}(A) = \text{rg}({}^t A)$

Questo vuol dire che, per calcolare il rango di una matrice, posso "accelerare" applicando l'algoritmo di Gauss a righe e colonne simultaneamente

Proprietà delle trasposizioni di matrici

① ${}^t({}^t A) = A$

② ${}^t(\alpha A + \beta B) = \alpha {}^t A + \beta {}^t B$

③ ${}^t(AB) = {}^t B {}^t A$

Matrice simmetrica e antisimmetrica

$A \in M_n(K)$ si dice che A è simmetrica (rispettivamente antisimmetrica) se $A = {}^t A$ (rispettivamente $A = -{}^t A$)

(es)

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 4 & 1 \\ 0 & 1 & 3 \end{pmatrix} \in M_3(\mathbb{R}) \text{ è simmetrica}$$

$$A = \begin{pmatrix} 0 & 4 \\ -4 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \text{ è antisimmetrica}$$

dato K campo qualsiasi, sia $a \in K^*$ t.c. $a = -a \Leftrightarrow a + a = 2a = 0 \Leftrightarrow$ la moltiplicazione per 2 in K è 0
questo mostra che non è vero che $A = -{}^t A \Leftrightarrow$ diagonale nulla. Risulta falso in $M_n(\mathbb{F}_2)$

$$\Leftrightarrow -1 \in \mathbb{F}_2$$

Esercizio 6

Sia $M_n^+(\mathbb{R})$ l'insieme delle matrici simmetriche di $M_n(\mathbb{R})$ ($M_n^-(\mathbb{R})$ insieme delle matrici antisimmetriche)

Dimostrare che $M_n^+(\mathbb{R})$ (rispettivamente $M_n^-(\mathbb{R})$) è un sottospazio vettoriale di $M_n(\mathbb{R})$. Poniamo $M = M_n^+(\mathbb{R})$ oppure $M_n^-(\mathbb{R})$

Dobbiamo dimostrare che $A, B \in M$, $\alpha, \beta \in \mathbb{R}$ allora $\alpha A + \beta B \in M$

Cominciamo con lo studio del caso "+" \rightarrow es. per Gauss

A, B sono simmetriche: $A = {}^t A$, $B = {}^t B$. ${}^t(\alpha A + \beta B) = \alpha {}^t A + \beta {}^t B = \alpha A + \beta B$

Nel caso "-" si ottiene ... $= \alpha(-A) + \beta(-B) = -(\alpha A + \beta B)$

qui

prop 3 (versione alternativa)

sia V sp. vett. su K f.g. $B = \{v_1, \dots, v_n\} \subset V$ allora c'è equivalenza tra:

① B è una base

② \mathcal{B} è un insieme massimale di vettori l.i.

③ B è un insieme minimaile di generatori

dim ② \Rightarrow ①

sia $B = \{v_1, \dots, v_n\}$ libero massimale e sia $v \in V$, allora $B' = \{v_1, \dots, v_n, v\}$ è un insieme di vettori l.d.

quindi $\exists \lambda, \lambda_1, \dots, \lambda_n \in K$ non tutti zero t.c. $\lambda v + \lambda_1 v_1 + \dots + \lambda_n v_n = 0 \Rightarrow \lambda v = -\lambda_1 v_1 - \dots - \lambda_n v_n$

necessariamente λ deve essere $\neq 0$ poiché v_1, \dots, v_n sono l.i. mg $\{v_1, \dots, v_n, V\}$ l.d. È quindi possibile

moltiplicare (*) per λ^i per $X^i \Rightarrow V = \frac{\lambda^1}{\lambda} V_1 + \dots + \frac{\lambda^n}{\lambda} V_n \Rightarrow V \in \text{Vect}_{\mathbb{K}}(B) \quad \forall v \in V \Rightarrow V \subset \text{Vect}_{\mathbb{K}}(B) \subset V \Rightarrow V = \text{Vect}_{\mathbb{K}}(B) \Rightarrow$

\Rightarrow B è un sistema di generatori per V

Teorema

sia V sp. vett. su K f.g. allora due basi hanno lo stesso numero di elementi:

1
dim

$B = \{b_1, \dots, b_r\}$ e $B' = \{b'_1, \dots, b'_{r'}\}$ due basi. Posso supporre $r' \geq r$

In particolare $\text{Vett}_K(\mathcal{B}) = \text{Vett}_K(\mathcal{B}') = V$

Posso scrivere in modo unico $\forall i: 1 \leq i \leq r$ $b'_i = \sum_{j=1}^r u_{ij} b_j$ \hookrightarrow posso scrivere gli elementi di $Vet_k(\mathbb{R})$ come combinazione lineare di \mathbb{R}

$$M = \left(\begin{array}{c|c|c} r' & \text{(coeffienti che formano gli elementi di } V_{\mathbb{K}}(S) \text{)} & r' \\ \hline (M_{ij})_{\substack{1 \leq i \leq r' \\ 1 \leq j \leq r}} & & A_{r'} \\ \hline & & r' \end{array} \right) \in M_{r', r+r'}(\mathbb{K})$$

Applico le operazioni di Gauss, che non modificano la proprietà di essere una base (mandano basi di V su basi di V)

Riduciamo quindi M a gradini relativamente al primo blocco $r'xr$

$$\Sigma \left(\begin{array}{c} r^1 \\ 1 \\ r^2 \\ 1 \\ r^3 \\ 1 \\ \hline 0 \end{array} \right) \quad * \quad \left(\begin{array}{c} c^1 \\ c^2 \\ c^3 \end{array} \right)$$

Ad ogni tappa le matrici intermedie hanno il primo blocco costituito da coordinate nella base di vettori di una base di V con r' elementi. Ma una base non contiene mai 0 cosa che avviene se $r' > r$ quindi $r' = r$

Analisi

con $r = r'$

$$r \left(\begin{array}{c|c} A & 1_r \\ \hline \end{array} \right) \quad r$$

Sia C una base qualsiasi di V $C = \{v_1, \dots, v_n\}$

$$[v_i]_C = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} \xrightarrow{\text{base canonica}} e_i \quad v_i = 0 \cdot v_1 + 0 \cdot v_2 + \dots + 1 \cdot v_i + \dots + 0 \cdot v_n$$

Si verifica che alla fine dell'algoritmo (portandola fino a una matrice a gradini ridotta) si ottiene:

$$\left(\begin{array}{c|c} 1_r & A' \\ \hline \end{array} \right)$$

dove le righe di A' sono le coordinate dei vettori della base
 \otimes nella base $\otimes \rightarrow A'$ rimane $[v]$ con \otimes base, ma diversa da quella
 (A era il contrario) di origine

E si osserva che A' è invertibile di inversa A

es

Mostriamo che U è invertibile e calcoliamo l'inversa

$$U = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 2 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{\substack{R_2 \rightarrow R_2 - 3R_1 \\ R_3 \rightarrow R_3 - R_1}} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -4 & -2 & -3 & 1 & 0 \\ 0 & -2 & -2 & -1 & 0 & 1 \end{array} \right) \xrightarrow{R_3 = -\frac{1}{2}R_3} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -4 & -2 & -3 & 1 & 0 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \end{array} \right) \xrightarrow{\substack{R_2 \rightarrow R_2 + 4R_3 \\ R_1 \rightarrow R_1 - 2R_2}}$$

$$\xrightarrow{\substack{R_1 \rightarrow R_1 - 2R_2 \\ R_3 \rightarrow \frac{1}{2}R_3}} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & -1 & 1 & -2 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \end{array} \right) \xrightarrow{\substack{R_2 \rightarrow R_2 - R_3 \\ R_1 \rightarrow R_1 - R_2}} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array} \right) \xrightarrow{\substack{R_1 \rightarrow R_1 - 2R_2 \\ R_2 \rightarrow R_2 - R_3}} \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & \frac{3}{2} & -\frac{1}{2} & 1 \\ 0 & 1 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array} \right) \xrightarrow{\quad}$$

$$\xrightarrow{R_1 \rightarrow R_1 - 2R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 1 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array} \right) \rightarrow \text{inversa}$$

Teorema

link

C'è equivalenza tra:

- ① $A \in GL_n(K)$ (A invertibile)
- ② $\text{rg}(A) = n \rightarrow$ trasformabile in gradini ridotta senza zeri (base)
- ③ le righe di A sono una base di K^n
- ④ le colonne di A sono una base di $K^n \rightarrow$ base mantenuta in A^T

oss esiste una nozione di determinante $\det: M_n(K) \rightarrow K$ (che abbiamo descritto solo nel caso $n=2$)
si dimostra che $A \in M_n(K)$ è invertibile $\Leftrightarrow \det(A) \in K^\times$

formula universale

$$A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(K) \Rightarrow \det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

Applicazioni lineari DEF

dati V, V' due spazi vettoriali su K un'applicazione $V \xrightarrow{f} V'$ è detta lineare se
 $\forall u, v \in V$ e $\forall \alpha, \alpha' \in K$ $f(\alpha u + \alpha' v) = \alpha f(u) + \alpha' f(v)$

Se inoltre f è biettiva allora si dice che è un isomorfismo di spazi vettoriali (se f è isomorfismo allora anche f^{-1} è isomorfismo)

prop

sia V sp. vett. su K f.g.

$\mathcal{B} = \{b_1, \dots, b_n\}$ base di V

V' sp. vett. qualsiasi su K

$f: \mathcal{B} \rightarrow V'$

Allora $\exists!$ applicazione lineare $\tilde{f}: V \rightarrow V'$ t.c. $\tilde{f}|_{\mathcal{B}} = f$

dm

siccome \mathcal{B} è una base allora $\forall v \in V \exists! (k_1, \dots, k_n) \in K^n$ t.c. $v = \sum_{i=1}^n k_i b_i$ ($[v]_{\mathcal{B}} = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$)

poniamo $\tilde{f}(v) = \sum_{i=1}^n k_i f(b_i)$ $V \xrightarrow{\tilde{f}} V'$

restrizione del dominio su

Mostriamo che \tilde{f} è lineare

siano $v, v' \in V$ e $\alpha, \alpha' \in K$ $\tilde{f}(\alpha v + \alpha' v') = ?$

calcoliamo

$$[v]_{\mathcal{B}} = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \quad [v']_{\mathcal{B}} = \begin{pmatrix} k'_1 \\ \vdots \\ k'_n \end{pmatrix}$$

$$[\alpha v + \alpha' v']_{\mathcal{B}} = ?$$

$$v = \sum_{i=1}^n k_i b_i, \quad v' = \sum_{i=1}^n k'_i b_i \Rightarrow \alpha v + \alpha' v' = \sum_{i=1}^n (\alpha k_i + \alpha' k'_i) b_i$$

$$\tilde{f}(\alpha v + \alpha' v') = \sum_{i=1}^n (\alpha k_i + \alpha' k'_i) f(b_i)$$

$\in K$

$$\alpha \tilde{f}(v) + \alpha' \tilde{f}(v') = \alpha \sum_{i=1}^n k_i f(b_i) + \alpha' \sum_{i=1}^n k'_i f(b_i) = \sum_{i=1}^n (\alpha k_i + \alpha' k'_i) f(b_i)$$

Quindi \tilde{f} è lineare

Mostriamo ora l'unicità di \tilde{f}

perché sono uguali su B

Supponiamo che $\exists \hat{f}: V \rightarrow V'$ lineare t.c. $\hat{f}(b_i) = \tilde{f}(b_i) = f(b_i)$ e mostriamo che $\hat{f} = \tilde{f}$

ovvero $\hat{f} - \tilde{f} = 0$

Poniamo $g = \hat{f} - \tilde{f}$

linearità in quanto differenza
di applicazioni lineari

$$g(v) = g\left(\sum_{i=1}^n k_i b_i\right) = \sum_{i=1}^n k_i g(b_i) = \sum_{i=1}^n k_i (\tilde{f}(b_i) - \hat{f}(b_i)) = 0 \Rightarrow g \equiv 0 \Rightarrow \hat{f} = \tilde{f}$$

■

per definizione
dimostrato che sono uguali ovunque

es)

sia V sp.vett. su \mathbb{R} di base $B = \{b_1, \dots, b_n\}$ e $V' = \mathbb{R}^n \Rightarrow \dim(V) = \dim(V') = n$

dato $v \in V$ posso scrivere $v = \sum k_i b_i$ (unica)

$$\text{poniamo } f(b_i) = e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$$

$$\tilde{f}(v) = \sum_i k_i f(b_i) = \sum_i k_i e_i = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \quad \text{quindi: } \tilde{f}(v) = [v]_B$$

$$\text{Notare che } \tilde{f} \text{ è un isomorfismo di spazi vettoriali: } \tilde{f}^{-1}\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} := \sum_{i=1}^n k_i b_i$$

abuso di notazione se \tilde{f} prolunga $f: B \rightarrow V$ allora scriviamo $f = \tilde{f}$

corollario

Se $\dim_K(V) = n$ allora $f: V \rightarrow K^n$ è un isomorfismo

Immagine e nucleo

Sia $f: V \rightarrow V'$ applicazione lineare

Poniamo $\text{Ker}(f) = \{v \in V \text{ t.c. } f(v) = 0\} (= f^{-1}\{\{0\}\})$

$\text{Im}(f) = \{v' \in V' \text{ t.c. } \exists v \in V \text{ f}(v) = v'\}$

Lemme $\text{Ker}(f)$ e $\text{Im}(f)$ sono sottospazi vettoriali di V e V' rispettivamente

dim

Chiaro che si tratti di sottogruppi quindi f è anche omomorfismo di gruppi.

Rimane da mostrare che $\text{Ker}(f)$ e $\text{Im}(f)$ sono stabili rispetto alla moltiplicazione scalare

sia $\alpha \in K$

$\xrightarrow{\alpha \in K, \text{lo posso portare fuori}}$

$f(v) = 0 \Rightarrow f(\alpha v) = \alpha f(v) = \alpha 0 = 0 \Rightarrow v \in \text{Ker}(f) \Rightarrow \alpha v \in \text{Ker}(f) \Rightarrow \text{Ker}(f)$ è sottospazio vettoriale di V

sia adesso $v' \in \text{Im}(f)$ e $\alpha \in K \Rightarrow \exists v \in V$ t.c. $f(v) = v'$ $\Rightarrow \alpha f(v) = \alpha v' \Rightarrow \alpha v' \in \text{Im}(f)$ ma $\alpha f(v) = f(\alpha v) \Rightarrow$ il vettore $\alpha v \in V$ è tale che $f(\alpha v) = \alpha v' \Rightarrow \alpha v' \in \text{Im}(f) \Rightarrow \text{Im}(f)$ è sottospazio vettoriale di V

in particolare $\text{Ker}(f) = 0 \Leftrightarrow f$ iniettiva

$\text{Im}(f) = V \Leftrightarrow f$ suriettiva



Somma di sottospazi vettoriali:

siano V_1, V_2 sottospazi vettoriali di V

definiamo $V_1 + V_2 = \{v \in V \text{ t.c. } \exists_{\substack{v_1 \in V_1 \\ v_2 \in V_2}} \text{ t.c. } v = v_1 + v_2\}$ che è un sottospazio vettoriale di V

proprietà

$$V_1 + V_2 = \bigcap_{\substack{W \text{ s.s. di } V \\ W \supseteq V_1 \cup V_2}} W$$

il più piccolo sottospazio vettoriale che contiene $V_1 \cup V_2$

Supponiamo che V f.g. e siano V_1, V_2 due sottospazi vettoriali allora V_1, V_2 sono anch'essi finitamente generati, come anche i sottospazi $V_1 \cap V_2$ e $V_1 + V_2$

Lemma data un'applicazione lineare $f: V \rightarrow V'$ con $\dim(V) = n$ allora $\dim(\text{Ker}(f)) + \dim(\text{Im}(f)) = n$

Teorema formula di Grassmann

$$\dim(V_1) + \dim(V_2) = \dim(V_1 \cap V_2) + \dim(V_1 + V_2)$$

Esercizio

Esercizio 2. Dati i seguenti insiemi di vettori, si dica in ciascun caso, motivando la risposta, se essi sono:

- linearmente indipendenti
- generatori di V
- una base di V .

$$\begin{matrix} \vec{v}_1 \\ \vec{v}_2 \\ \vec{v}_3 \end{matrix}$$

$$(a) V = \mathbb{R}^4, \quad T = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \right\};$$

$$(b) V = \{ \text{matrici simmetriche reali } 2 \times 2 \}, \quad T = \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\};$$

$$(c) V = \mathbb{R}_2[t] (\text{i polinomi di grado al più 2 a coefficienti reali}), T = \{1+t, 1-t, t^2, 1-t^2\}.$$

② Vediamo se T è l.i.

$$x \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + y \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

metto $(A|0)$
poiché lo zero
non potrebbe cambiare

$$rg(A) = 3 = rg(A|0) \Rightarrow \text{il sistema è compatibile}$$

$$\text{il numero di indeterminate}$$

$$\text{e il numero di equazioni} \Leftrightarrow \text{Sol}(A|0) = \{(0, 0, 0)\} \text{ ovvero } \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow$$

$$\Leftrightarrow \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0 \Leftrightarrow v_1, v_2, v_3 \text{ sono l.i.}$$

Ma $\{v_1, v_2, v_3\}$ non è base di \mathbb{R}^4 , infatti abbiamo osservato $\dim(\mathbb{R}^4) = 4$ qui

Mostriamo ora che v_1, v_2, v_3 non generano $V = \mathbb{R}^4$ ovvero che $\text{Vett}_{\mathbb{R}}(v_1, v_2, v_3) \subsetneq \mathbb{R}^4$

Io potrei anche dimostrare dicendo che v_1, v_2, v_3 è una base $\Leftrightarrow v_1, v_2, v_3$ l.i. e generatore. Non essendo una base ma essendo l.i. allora necessariamente non è un generatore

dovrò mostrare che $\exists v \in \mathbb{R}^4$ t.c. il sistema completo associato è incompatibile

$$(A|b) = \begin{pmatrix} 1 & 1 & 0 & a \\ 0 & 1 & 1 & b \\ 1 & 0 & 1 & c \\ 1 & 1 & 1 & d \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 1 & 0 & a \\ 0 & 1 & 1 & b \\ 0 & -1 & 1 & c-a \\ 0 & 0 & 1 & d-a \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 1 & 0 & a \\ 0 & 1 & 1 & b \\ 0 & 0 & 1 & d-a \\ 0 & 0 & 2 & c-a+b \end{pmatrix} \begin{array}{l} \\ \curvearrowleft \\ \curvearrowleft \\ \curvearrowleft \end{array} \begin{pmatrix} 1 & 1 & 0 & a \\ 0 & 1 & 1 & b \\ 0 & 0 & 1 & d-a \\ 0 & 0 & 0 & c-a+b-d \end{pmatrix}$$

$\text{rg}(A) \neq \text{rg}(A| \begin{smallmatrix} b \\ c \\ d \end{smallmatrix})$ se $a=1$ e $b=c=d=0$ il rango sarebbe 4
da ciò si capisce che il sistema non è compatibile $\Rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \notin \text{Vett}_{\mathbb{R}}(v_1, v_2, v_3) \Rightarrow \exists v \in \text{Vett}_{\mathbb{R}}(v_1, v_2, v_3)$

⑥ poiché è simmetrica allora sono del tipo $\begin{pmatrix} a & b \\ c & a \end{pmatrix}$ da cui si nota che il grado di libertà è 3 (tre distinte incognite possono assumere qualsiasi valore $\Rightarrow \dim_{\mathbb{R}}(V)=3$)

$$T = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \subset V = M_2^+(\mathbb{R})$$

per verificare che T è libero si studia il sistema $x \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + y \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + z \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$(A|0) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{array}{l} L_3 \rightarrow L_3 - L_2 \\ L_3 \leftrightarrow L_4 \end{array} \sim \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{array}{l} L_2 \rightarrow L_2 - L_3 \\ L_3 \rightarrow L_3 - L_4 \\ L_3 \rightarrow L_3 - L_2 \end{array} \sim \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{rg}(A) = \text{rg}(A|0) = 3$$

inoltre $s := n - \text{rg}(A) = 3 - 3 = 0 \Rightarrow \text{Sol}(A|0) \xrightarrow{\text{R}^{2,3}} \mathbb{R}^0 \Leftrightarrow \text{Sol}(A|0) = \{0\}$ ovvero $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow$
 ⇒ le matrici $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ sono l.i.

Ma $M_2^+(\mathbb{R}) = V$ ha dim 3, quindi $\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right)$ è una base di $M_2^+(\mathbb{R})$

⑦ $T = \{1+t, 1-t, t^2, 1-t^2\} \subset \mathbb{R}_2[t]$

$\mathbb{R}_2[t]$ è il sottospazio vettoriale di $\mathbb{R}[t]$ generato da $\{1, t, t^2\}$ che ne è una base.

Ovvero $\dim(\mathbb{R}_2[t]) = 3$. Ricordiamo che, se V è f.g., $\dim(V) = n$ e se $B \subseteq V$ finito, allora B libero $\Rightarrow \#B \leq n$ e B generatore $\Rightarrow \#B \geq n$

Osserviamo che $T \subseteq \mathbb{R}_2[t]$ quando $\text{Vett}_{\mathbb{R}}(T) \subseteq \mathbb{R}_2[t]$. Ma T non è libero infatti $\#T = 4 > \dim_{\mathbb{R}}(\mathbb{R}_2[t]) = 3$

Ne consegue che non è neanche una base

Verifichiamo ora se è una base. Osserviamo che $\mathbb{R}_2[t] = \text{Vett}_{\mathbb{R}}(1, t, t^2)$

① $t^2 \in T$

② $1 = \frac{1}{2}(1+t+1-t) \in \text{Vett}_{\mathbb{R}}(T)$

③ $t = \frac{1}{2}(1+t-(1-t)) \in \text{Vett}_{\mathbb{R}}(T)$

Quindi $\text{Vett}_{\mathbb{R}}(1, t, t^2) = \mathbb{R}_2[t] \subseteq \text{Vett}_{\mathbb{R}}(T) \Rightarrow T$ è sistema di generatori

Esercizio 3. (a) Si determini una base per il sottospazio S di \mathbb{R}^4 generato dai vettori $v_1 = (1, 1, 0, 1)$, $v_2 = (1, 0, 1, 1)$, $v_3 = (1, -1, 1, -1)$, $v_4 = (2, 2, 1, 4)$.

(b) Si dica se il vettore $v = (0, 3, -2, 2)$ appartiene al sottospazio S .

(c) Si dica (motivando la risposta) se i vettori $\{v_1, v_2, v_3, v\}$ formano una base di \mathbb{R}^4 .

(d) Dopo aver verificato che l'insieme $B = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} \right\}$

è una base di \mathbb{R}^4 , si determinino le coordinate del vettore v nella base B .

① Calcolare una base di $\text{Vett}_{\text{IR}}(v_1, v_2, v_3, v_4) = W$

Data A' ottenuta applicando ad A delle trasformazioni elementari sulle righe, $W = \text{Vett}_{\text{IR}}(\text{righe di A}')$

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 2 & 2 & 1 & 1 \end{pmatrix} \xrightarrow{\substack{R_2 \rightarrow -(R_2-R_1) \\ R_3 \rightarrow R_3 - R_1 \\ R_4 \rightarrow R_4 - 2R_1}} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -2 & 1 & -2 \\ 0 & 0 & 1 & 2 \end{pmatrix} \xrightarrow{R_3 \rightarrow R_3 + 2R_2} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{pmatrix} \xrightarrow{\substack{R_1 \rightarrow R_1 + R_3 \\ R_3 \rightarrow -R_3}} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

quindi $\text{rg}(A) = 3$ $W = \text{Vett}_{\text{IR}}\left(\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}\right)$ le righe sono una base di S

In una matrice a gradini, i vettori dei pivot sono l.i. quindi $\{(1, 1, 0, 1), (0, 1, -1, 0), (0, 0, 1, 2)\}$ è un insieme linearmente indipendente ed è una base di S ovvero $\dim_{\mathbb{R}}(S) = 3$ (ma non è una base di S)

② Si tratta ora di risolvere il sistema

$$x \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \\ 2 \\ 2 \end{pmatrix} \quad (*)$$

si ha che (*) è compatibile $\Leftrightarrow \begin{pmatrix} 3 \\ -2 \\ 2 \\ 2 \end{pmatrix} \in S$

La matrice completa associata al sistema è

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 3 \\ 0 & -1 & 1 & -2 \\ 1 & 0 & 2 & 2 \end{pmatrix} \xrightarrow{\substack{R_2 \rightarrow R_2 - R_1 \\ R_3 \rightarrow R_3 - R_1}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & -1 & 1 & -2 \\ 0 & 0 & 2 & 2 \end{pmatrix} \xrightarrow{\substack{R_3 \rightarrow R_3 + R_2 \\ R_4 \rightarrow \frac{1}{2}R_4}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \xrightarrow{R_4 \rightarrow R_4 - R_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

dunque $\text{rg}(A) = \text{rg}(A|b) = 3 \Rightarrow v \in \text{V}(v_1, v_2, v_3) = S$

③ poiché $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = v$ e sapendo che v_1, v_2, v_3 sono l.i. è evidente che v è l.d. infatti

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 - v = 0$$

$$\Leftrightarrow \lambda_4 = -1 \neq 0$$

④

I modo

Verifico prima di tutto che è l.i.

$$x \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\left(\begin{array}{cccccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \end{array} \right) \underset{\substack{R_1 \leftrightarrow R_2 \\ R_2 \rightarrow R_2 - R_1 \\ R_4 \rightarrow \frac{1}{2}(R_4 - R_1)}}{\sim} \left(\begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{array} \right)$$

$\text{rg}(A) = \text{rg}(A|0) = 4 \Rightarrow$ è compatibile

$$\begin{aligned} \dim_{\mathbb{R}}(\text{Sol}(A|0)) &= n - \text{rg}(A) = 4 - 4 = 0 \Rightarrow \\ \Rightarrow \text{Sol}(A|0) &= \{0\} \text{ ovvero } \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \text{sono l.i.} \end{aligned}$$

Verifichiamo che B è un generatore

$$\left(\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right) \underset{\substack{R_1 \leftrightarrow R_2 \\ R_2 \rightarrow R_2 - R_1 \\ R_4 \rightarrow \frac{1}{2}(R_4 - R_1)}}{\sim} \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$\begin{aligned} \Rightarrow \text{rg}(A) &= \text{rg}(A|b) = 4 \Rightarrow \text{è compatibile} \Rightarrow \\ &\Rightarrow \text{è un generatore} \end{aligned}$$

Da ciò si conclude che B è una base

II modo

Verificare che B è una base di \mathbb{R}^4 è calcolare le coordinate di v in questa base

B è base di $\mathbb{R}^4 \Leftrightarrow \text{rg}(M) = 4$ con qui lavoriamo sulle righe

$$M = \left(\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right) \underset{R_3 \rightarrow R_2 - R_1}{\sim} \left(\begin{array}{cccc} 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array} \right) \underset{R_2 \rightarrow R_2 + R_1}{\sim} \left(\begin{array}{cccc} 0 & 0 & 1 & -1 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array} \right)$$

Da qui si vede che il range della matrice iniziale, preservato da tutte queste operazioni, è uguale a 4 quindi B è una base di \mathbb{R}^4 dove

Troviamo adesso $[v]_B$. Bisogna quindi trovare x, y, z, t tali che
 $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} + t \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \\ 0 \\ -2 \end{pmatrix}$

$$\text{quindi: } \begin{pmatrix} 0 \\ 3 \\ -2 \\ 2 \end{pmatrix} = \begin{pmatrix} x+y \\ x \\ z+3 \\ z-t \end{pmatrix} \Rightarrow \begin{cases} x+y = 0 \\ x = 3 \\ z+3 = -2 \\ z-t = 2 \end{cases} \quad \begin{cases} y = -3 \\ x = 3 \\ t = -2 \\ z = 0 \end{cases} \Rightarrow [v]_B = \begin{pmatrix} 3 \\ 3 \\ 0 \\ -2 \end{pmatrix}$$