Lezione 01 - 29/09/2022

Operazione binaria

Un'operazione binaria $*$ su un insieme S è un'applicazione:

$$\begin{gathered} * : S \times S \to S \\ (a, b) \mapsto a * b \end{gathered}$$

Monoide

Un insieme S dotato di **un'operazione binaria** in cui valgono le proprietà di **associatività** e **esistenza dell'elemento neutro** si dice **MONOIDE**.

- **Proprietà associativa**

$$(a * b) * c = a * (b * c) \; \forall a, b, c \in S$$

- **Esistenza elemento neutro**

$$\exists e \in S : e * a = a * e = a \; \forall a \in S$$

Es.:

- $(\mathbb{N}, +)$, con elemento neutro $e = 0$
- $(\mathbb{N}, \cdot)$, con elemento neutro $e = 1$

Più in generale ogni insieme X nella lista

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

rispetto a $+$ o rispetto a $\cdot$ è un monoide.

Lemma - L'elemento neutro è unico

In un monoide S l'elemento neutro è unico

Dimostrazione: Siano e_1, e_2 due elementi neutri

$$e * a \overset{(1)}{=} a * e \overset{(2)}{=} a$$
$$e_1 \overset{(1)}{=} e_1 * e_2 \overset{(2)}{=} e_2$$

Dove, nella seconda equazione:

- Nel primo passaggio vengono posti: $a = e_1$ e $e = e_2$
- Nel secondo passaggio vengono posti: $a = e_2$ e $e = e_1$

Monoide commutativo

Un monoide si dice **commutativo** se

$$a * b = b * a, \forall a, b \in S$$

Es.:

X insieme, $F_X = \{f : X \to X\}$ e $f * g = f \circ g$ si ha che

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

F_X è un **monoide** perché la composizione di funzioni è associativa. L'elemento neutro è:

$$\mathrm{Id}_x(x) = x, \forall x \in X$$

Infatti:

$$f \circ \mathrm{Id}_x = \mathrm{Id}_x \circ f = f$$

Es.:

$$(f \circ \mathrm{Id}_x)(x) = f(\mathrm{Id}_x(x)) = f(x)$$
$$(\mathrm{Id}_x \circ f)(x) = \mathrm{Id}_x(f(x)) = f(x)$$

Gruppo e gruppo abeliano

Un **monoide** $(G, *)$ si dice **GRUPPO** se

$$\forall g \in G \; \exists g' \in G : g * g' = g' * g = e$$

Ovvero g' è l'**elemento inverso** di g.

Se G è **commutativo**, diciamo anche che è un **GRUPPO ABELIANO**.
Es.:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$

Esempio: Sia $F_x \supset S_x = \{f : X \to X, \text{ f biiettiva}\}$

Biiettiva siginifica che: $\exists g : X \to X \text{ t.c. } f \circ g = g \circ f = \mathrm{Id}_X$

$$f^{-1}(B) = \{x \in X | f(x) = B\}$$

Prendiamo:

- f biunivoca
- $B = \{y\}$

Si ha che $f^{-1}(y)$ ha un solo elemento.

Notazione - gruppo simmetrico

S_n è un gruppo simmetrico su $X = \{1, 2, ..., n\}$, dove X indica le permutazioni su $\{1, 2, ..., n\}$

Lemma - Inverso unico

In un gruppo G l'inverso di ogni elemento è unico

Dimostrazione: supponiamo che g_1, g_2 siano entrambi inversi di g, per ipotesi

$$g * g_1 = g_1 * g = e$$
$$g * g_2 = g_2 * g = e$$

Si avrà la seguente cosa:

$$g_1 = g_2 * e = g_1 * (g * g_2) \overset{assoc.}{=} (g_1 * g) * g_2 = e * g_2 = g_2$$

Anello, anello commutativo con unità e campo

Un anello con unità R è un insieme dotato di due operazioni binarie $+$ e $\cdot$ tali che:

1. $(R, +)$ è un **gruppo abeliano**,
2. $(R, \cdot)$ è un **monoide**

Valgono le proprietà distributive:

$$(a+b)c = ac + bc, \forall a, b, c \in R$$
$$a(b+c) = ab + ac, \forall a, b, c \in R$$

Se $(R, \cdot)$ è un **monoide commutativo**, diciamo che R è un **anello commutativo con unità**.
Es.:

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

Se $(R \setminus \{0\}, \cdot)$ è un **gruppo abeliano**, diciamo che R è un **campo**.
Es.:

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

In un anello $0 \cdot a = 0, \forall a \in R$, infatti:

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

Lezione 02 - 30/09/2022

Relazione

Sia X insieme, $X \times X = \{(a, b) | a, b \in X\}$

Esempio:

$$X = \{1, 2\}$$
$$X \times X = \{(1,1), (1,2), (2,1), (2,2)\}$$

Definizione

Una relazione su X è un sottoinsieme R di $X \times X$. Diremo che $x \in X$ è in relazione con $g \in X$ se $(x, g) \in R$

Esempio:

$$X = \{1, 2, 3\}$$
$$R = \{(1,2), (1,3), (3,3)\}$$

- 1 è in relazione con 2
- 2 non è in relazione con 1

Notazione

Se R è una relazione e x è in relazione con y, scriveremo $x \sim y$.

Definizione - Relazione di equivalenza

Una relazione R su X si dice di **equivalenza** se valgono le 3 seguenti proprietà:

1. **Riflessiva**: $x \sim x, \forall x \in X$
2. **Simmetrica**: $x \sim y \Rightarrow y \sim x$
3. **Transitiva**: $x \sim y, y \sim z \Rightarrow x \sim z$

Esempi:

- R è la relazione di eguaglianza
- X = rette nel piano, R = relazione di parallelismo
- Congruenza modulo n, $n \in \mathbb{N}$

Osservazione

$\mathbb{Z}$ non è una campo in quanto non si può fare la divisione, ma si può comunque fare la divisione con resto. Verrà dimostrato che dati

$$a, b \in \mathbb{Z}, b \neq 0\ \exists! q, r \in \mathbb{Z} \text{ t.c.}$$
$$a = bq + r,\ 0 \leq r < |b|$$

Esempio: $17 = 4 * 4 + 1$

Fissato n, si pone

$$a \equiv_n b$$
$$\text{oppure}$$
$$a \equiv b \mod n$$

se a, b hanno lo stesso resto nella divisione per n. Quindi $a \equiv_n b$ se

$$a = q_1 n + r$$
$$b = q_2 n + r$$

e varrà la seguente regola

$$b - a = q_2 n + r - (q_1 n + r) = (q_2 - q_1)n$$

ovvero che $b - a$ è un multiplo di n, quindi

$$b \equiv_n a \Leftrightarrow \text{b-a è multiplo di n}$$

Verifichiamo che $\equiv_n$ è una **relazione di equivalenza**

- **Riflessiva**: $a \equiv_n a,\ a - a = 0 = 0 \cdot n$ ✓
- **Simmetrica**: $a \equiv_n b \Rightarrow b \equiv_n a$
    - Ipotesi: $b - a = kn$
    - Tesi: $\exists h$: $a - b = hn$, cioè $a - b = (-k)n$, quindi $h = -k$ ✓
- **Transitiva**: $a \equiv_n b, b \equiv_n c \Rightarrow a \equiv_n c$
    - Ipotesi:
        1. $b - a = hn$
        2. $c - b = kn$
    - Tesi: $\exists s$: $c - a = sn$. Sommando 1. con 2. si ottiene

$$c - a = c - b + b - a = hn + kn = (h+k)n \checkmark$$

Classi di equivalenza

Se R è un'equivalenza su X, poniamo per $x \in X$

$$[x] = \{y \in X | y \sim x\}$$

e la chiamiamo **classe di equivalenza di x.**

Osservazione

$$x \sim y \Leftrightarrow [x] = [y]$$

Dimostrazione:

- $\Rightarrow$

  Supponiamo $x \sim y$ e facciamo vedere che $[x] = [y]$, ovvero $[x] \subseteq [y]$ e $[y] \subseteq [x]$.

    1. $z \in [x]$

$$z \sim x, \overbrace{x \sim y}^{\text{ipotesi}} \overset{\text{TRA.}}{\Rightarrow} z \sim y \Rightarrow z \in [y]$$

    2. $t \in [y]$

$$t \sim y, \overbrace{x \sim y}^{\text{ipotesi}} \overset{SIM.}{\Rightarrow} y \sim x \overset{TRA.}{\Rightarrow} t \sim x \Rightarrow t \in [x]$$

- $\Leftarrow$

  Supponiamo $[x] = [y]$, allora $x \in [y]$, quindi $x \sim y$.

Costruzione dell'insieme quoziente

Siano X inseme e $\sim$ relazione di equivalenza

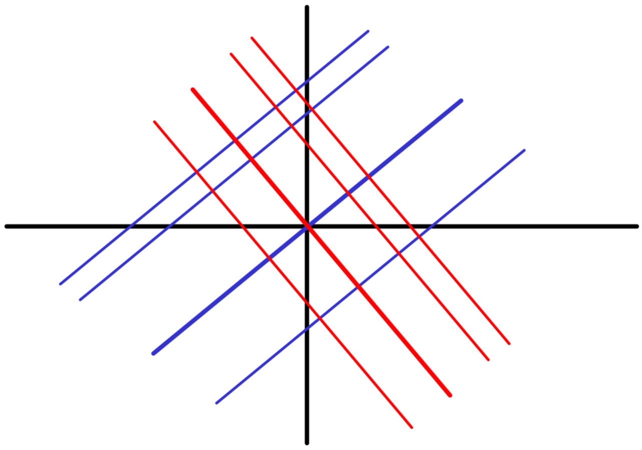
$$X/\sim = \{[x] | x \in X\}$$

e si chiama **insieme quoziente di x modulo $\sim$.**

<u>Esempi</u>:

- $[x] = [y] \Leftrightarrow x = y$

  $X/_{=} = X$
- $X/_{\sim} = \text{direzioni nel piano} \leftrightarrow \text{rette che passano per l'origine}$



  Vengono scelte come rappresentanti solo quelle che passano per l'origine.

- $a \equiv_n b \Leftrightarrow a, b \text{ hanno lo stesso resto nella divisione per } n \leftrightarrow$
  $\text{un insieme di rappresentanti è dato dai resti della divisione per } n$

$$\mathbb{Z}/\equiv_n = \{[0], [1], ..., [n-1]\}$$

  <u>Esempi</u>:

- $\mathbb{Z}/\equiv_2 = \{[0],[1]\}$ che stanno ad indicare rispettivamente i **numeri pari** e i **numeri dispari**.
- $\mathbb{Z}/\equiv_3 = \{[0],[1],[2]\}$

> Di solito si scrive $\mathbb{Z}_n$ per indicare $\mathbb{Z}/\equiv_n$.

Definizione di anello su Zn

Si vuole definire una struttura di anello su $\mathbb{Z}_n$:

- $+\ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

  $([a],[b]) \mapsto [a+b]$
- $\cdot\ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

  $([a],[b]) \mapsto [ab]$

Esempio: $n = 4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$
$[2]$	$[2]$	$[0]$	$[2]$
$[3]$	$[3]$	$[2]$	$[1]$

> ⚠️ Negli anelli si toglie lo 0 per l'operazione $\cdot$

> ⚠️ 2 non ha inversi quindi non è un campo. In quanto non ha inversi si dice che 2 è un **divisore dello 0**.

Spiegazione: a differenza di 2, tutti gli altri hanno inverso:

- $[1] \cdot [1] = [1]$
- $[3] \cdot [3] = [1]$

Mentre per $[2]$ non c'è nessuna classe $[b]$ tale che $[2] \cdot [b] = [1]$.

Problema teorico

Quando si definisce una funzione su un insieme quoziente, bisogna assicurarsi che la definizione sia **ben posta**, ovvero non dipenda dal **rappresentante scelto**.

Esempio: $\mathbb{Z}_{21}$

$$[18] + [8] = [26] = [5]$$

Ma in $\mathbb{Z}_{21}$ si ha anche $[18] = [-3]$ e $[8] = [50]$, quindi analogamente

$$[-3] + [50] = [47] = [5]$$

I risultati sono gli stessi, ma andrebbe dimostrato!

Verifichiamo che la $+$ in $\mathbb{Z}_n$ non dipenda dai rappresentanti. Bisogna vedere che:

$$[a] = [a'], [b] = [b'] \Rightarrow [a + b] = [a' + b']$$

Ipotesi:

1. $a' - a = kn$, ovvero è un multiplo di n
2. $b' - b = hn$

Verifichiamo che $(a' + b') - (a + b)$ è un multiplo di n:

$$a' + b' - a - b = \underbrace{(a' - a)}_{1.} + \underbrace{(b' - b)}_{2.} = kn + hn = (k + h)n \checkmark$$

Facciamo la stessa cosa per il prodotto:

$$[a] = [a'], [b] = [b'] \Rightarrow [ab] = [a'b']$$

Ipotesi:

1. $a' - a = hn$
2. $b' - b = kn$

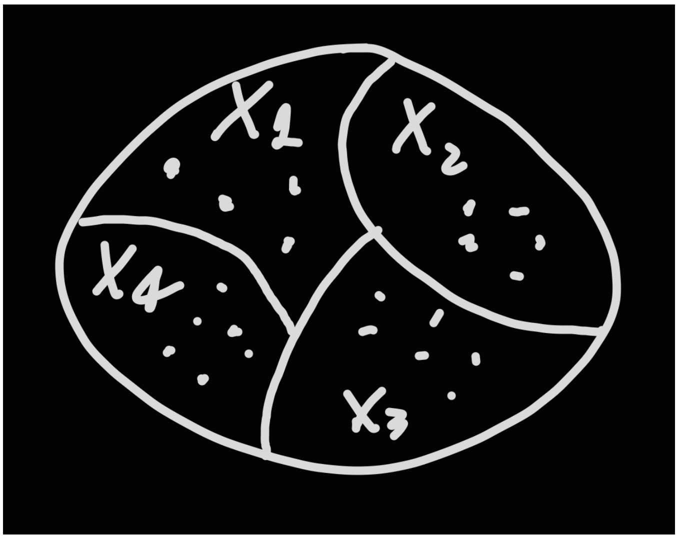
$$a'b' - ab = (a + hn)(b + kn) - ab = ab + hnb + akn + hkn^2 - ab =$$
$$= (hb + ak + hkn)n \checkmark$$

Entrambe le operazioni son **ben poste**.

Partizione

Sia X un insieme. Una famiglia $\{X_\alpha\}_{\alpha \in I}$ sottoinsiemi non vuoti di X si dice **partizione** di X se:

1. $X = \bigcup_{\alpha \in I} X_\alpha$
2. $X_\alpha \cap X_\beta = \emptyset \text{ se } \alpha \neq \beta$



$$X = X_1 \cup X_2 \cup X_3 \cup X_4$$
$$X_i \cap X_j = \emptyset \text{ se } i \neq j$$

Proposizione

Esiste una corrispondenza biunivoca tra paritzioni di X e relazioni di equivalenza su X.

<u>Dimostrazione</u>: sia $\sim$ una relazione di equivalenza. Poniamo

$$X_\alpha = \{x \in X | x \sim \alpha\} \alpha \in X$$

Dico che $\{X_\alpha\}_{\alpha \in X}$ è una partizione di X.

Dato $\alpha \in X$, allora $\alpha \in X_\alpha$ poichè $\alpha \sim \alpha$ per la **relazione riflessiva**. Quindi $X = \bigcup X_\alpha$.

Devo ora vedere che se X_α e X_β si intersecano, allora $\alpha = \beta$:
Sia $z \in X_\alpha \cap X_\beta$

$$\begin{aligned} & z \in X_\alpha, z \sim \alpha \overset{SIM.}{\Longrightarrow} \alpha \sim z \\ & z \in X_\beta, z \sim \beta \\ & \overset{TRA.}{\Longrightarrow} \alpha \sim \beta \Rightarrow X_\alpha = X_\beta \end{aligned}$$

<u>Viceversa</u>: sia $X = \bigcup_{\alpha \in I} X_\alpha$ una partizione. Definisco la relazione

$$x \sim y \Leftrightarrow \exists \delta \in I : x, y \in X_\delta$$

Verifico che $\sim$ è di **equivalenza**:

- **Riflessiva**: $x \sim x$, devo vedere che esiste

$$\alpha \in I \text{ t.c. } x \in X_\alpha$$

  Ma questo segue dall'ipotesi che $X = \bigcup_{\alpha \in I} X_\alpha$.

- **Simmetrica**:

$$\begin{aligned} & x \sim y \Rightarrow \exists \alpha \in I \text{ t.c. } x, y \in X_\alpha \\ & \Rightarrow y \sim x \ (\text{poichè entrambe appartengono a } X_\alpha) \end{aligned}$$

- **Transitiva**:

$$x \sim y, y \sim z \Rightarrow x \sim z$$

  Ipotesi:

$$\begin{aligned} & \exists \alpha_1 \in I : x, y \in X_{\alpha_1} \\ & \exists \alpha_2 \in I : x, y \in X_{\alpha_2} \end{aligned}$$

  quindi $y \in X_{\alpha_1} \cap X_{\alpha_2} \Rightarrow \alpha_1 = \alpha_2$ e di conseguenza $x, z \in X_{\alpha_1} \Rightarrow x \sim z$.

  Si verifica facilmente che le corrispondenze costruite sono una l'inversa dell'altra.

Lezione 04 - 07/10/2022

Relazione d’ordine (parziale)

Definizione: una relazione d’ordine $\leq$ su X è un sottoinsieme **non vuoto** di $X \times X$ che verifica le seguenti proprietà:

- **Riflessiva**: $x \leq x, \ \forall x \in X$
- **Antiriflessiva**: $x \leq y, \ y \leq x \Rightarrow x = y$
- **Transitiva**: $x \leq y, \ y \leq z \Rightarrow x \leq z$

Esempi:

1. Usuale $\leq$ su $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
   Nota: In questo caso, dati due elementi x, y risulta

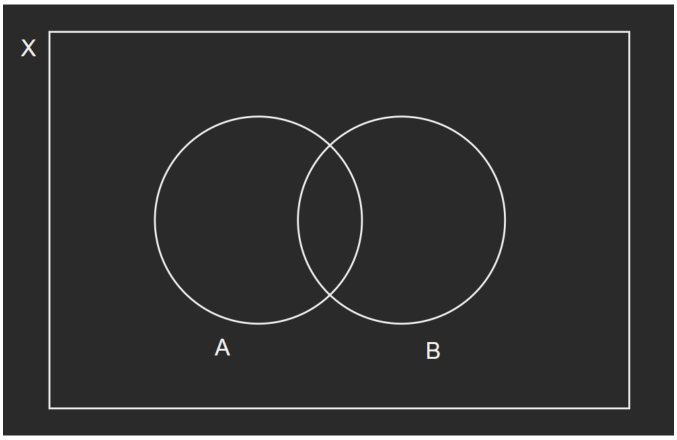
$$x \leq y \text{ oppure } y \leq x$$

   Una relazione d’ordine con questa proprietà si dice **totale**.

2. Sia X insieme, $\mathcal{P}(X)$ l’insieme delle parti di X e $A, B \in \mathcal{P}(X)$

$$A \leq B \text{ se } A \subseteq B$$

   Guardando il seguente diagramam di Venn



Si ha che $A \not\subseteq B$ e $B \not\subseteq A$, quindi **non è una relazione d'ordine**.

3. Sia $X = \mathbb{N}$ e la relazione $\leq = |$ "divide"

$$a \mid b \Leftrightarrow b \text{ è un multiplo di } a, \text{cioè } \exists c \in \mathbb{N} \text{ t.c. } b = ac$$

Esempi: $2 \nmid 5, 2 \mid 6$

- **Riflessiva**:

$$a \mid a, \;\; a = 1a \checkmark$$

- **Antisimmetrica**:

$$\begin{aligned} a \mid b, b \mid a \\ b = ca \\ a = db \\ (b \neq 0) \; 1 = cd \Rightarrow c = d = 1, \;\; \text{quindi } a = b \checkmark \end{aligned}$$

> ⚠️ In $\mathbb{Z}$, $cd = 1 \not\Rightarrow c = 1 = d$, in quanto potrebbe anche essere che $c = d = -1$, quindi la divisibilità non è una **relazione d'ordine** su $\mathbb{Z}$.

- **Transitiva**: $a \mid b, b \mid c \Rightarrow a \mid c$

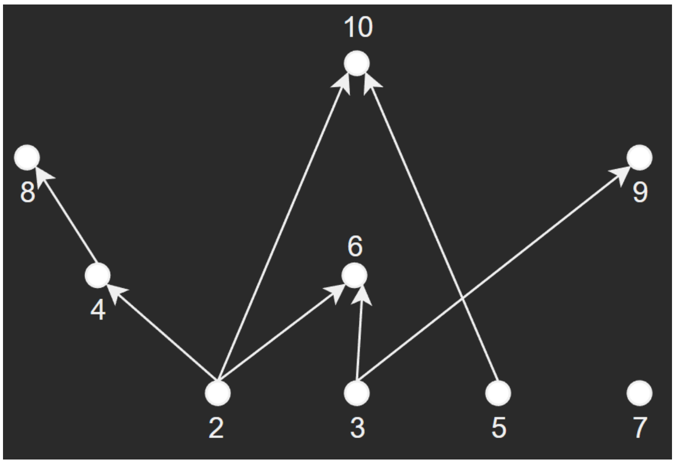
$$\begin{aligned} a \mid b \Rightarrow b = ka \\ b \mid c \Rightarrow c = hb \\ c = hb = hka = (hk)a \Rightarrow a \mid c \checkmark \end{aligned}$$

Grafo di Hasse

Un insieme X dotato di una **relazione d'ordine parziale** è usualmente chiamato **POSET** (Partially - Ordered - Set). Spesso quando X è un insieme finito, un POSET viene rappresentato tramite il suo **grafo di Hasse**:

- **Vertici**: elementi di X
- **Lati orientati**: x → y se $x \leq y$ e $x \leq t \leq y \Rightarrow x = t \text{ oppure } y = t$, ovvero **non ci sono altri nodi di mezzo**.

<u>Esempio</u>: $X = \{2, 3, ..., 10\}$, con la relazione $\leq = |$



Costruzione di Z a partire da N

Siano $X = \mathbb{N} \times \mathbb{N}$ e ρ è la seguente relazione

$$(n, m)\rho(n', m') \iff n + m' = m + n'$$

Verifichiamo che si una relazione d'equivalenza:

- **Riflessiva**: $(n, m)\rho(n, m)$ vera in quanto $n + m = m + n$✓
- **Simmetrica**:

$$(n, m)\rho(n', m') \text{ ipotesi } n + m' = m + n'$$
$$(n', m')\rho(n, m) \text{ tesi } n' + m = m' + n \ ✓$$

- **Transitiva**:

$$(n,m)\rho(n'm') \text{ e} \tag{1}$$
$$(n',m')\rho(n",m") \tag{2}$$
$$\text{tesi } (n,m)\rho(n",m") \tag{3}$$

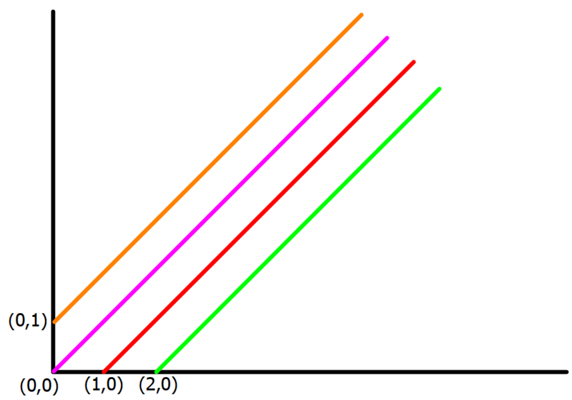
Da (1), (2) e (3) seguono le seguenti cose:

1. $n+m'=m+n'$
2. $n'+m"=m'+n"$
3. $n+m"=m+n"$

Dimostriamo che $n+m"=m+n"$

$$\begin{aligned} n+m" &= \underbrace{n+m'}_{1.}-m'+m" = \\ &= m+n'-m'+m" = \\ &= m-m'+\underbrace{n'+m"}_{2.} = \\ &= m-m'+m'+n" = \\ &= m+n" \end{aligned}$$

<u>Definizione</u>: $\mathbb{Z}=\mathbb{N}\times\mathbb{N}_{/\rho}$



<u>Esempi</u>:

$$\begin{aligned} [(1,0)] &= \{(n,m):(n,m)\sim(1,0)\} \\ &= \{(n,m):m+1=n\} \end{aligned}$$

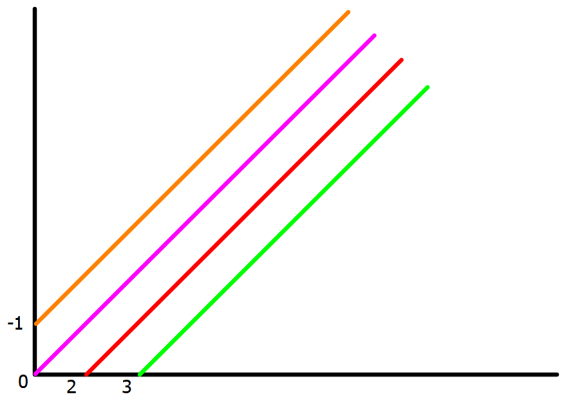
$$
\begin{aligned}
[(0,0)] &= \{(n,m) : (n,m) \sim (0,0)\} \\
&= \{(n,m) : (n,m)\}
\end{aligned}
$$

Poniamo

$$
\begin{aligned}
\mathbb{Z}_+ &= \{[(n,0)] : n \neq 0\} \\
\mathbb{Z}_- &= \{[(0,n)] : n \neq 0\} \\
0 &= [(0,0)]
\end{aligned}
$$

e

$$
\begin{aligned}
\mathbb{Z} &= \mathbb{Z}_+ \cup \mathbb{Z}_- \cup \{0\} \\
n &= [(n,0)] \\
-n &= [(0,n)] \\
0 &= [(0,0)]
\end{aligned}
$$



Definiamo le operazioni su $\mathbb{Z}$:

- Operazione $+$:

$$
[(n,m)] + [(n',m')] = [(n+n', m+m')]
$$

<u>Osservazione</u>:

$$
\begin{aligned}
2+3 &= [(2,0)] + [(3,0)] = [(5,0)] = 5 \\
2+(-2) &= [(2,0)] + [(0,2)] = [(2,2)] = [(0,0)] = 0 \\
2+(-3) &= [(2,0)] + [(0,3)] = [(2,3)] = [(0,1)] = -1
\end{aligned}
$$

- Operazione $\cdot$:

$$[(n,m)][(n',m')] = [(nn' + mm', n'm + m'n)]$$

Osservazione:

$$n \cdot m = [(n,0][(m,0)] = [(nm,0)] = nm,\ n,m > 0$$
$$n \cdot 0 = [(n,0)][(n,n)] = [(n^2,n^2)] = [(0,0)] = 0$$

Verifica che la definizione dell'addizione è ben posta, cioè che non dipende dal rappresentante scelto:

$$[(m,n)] + [(m',n')] = [(m+n', n+m')]$$
$$[(m,n)] = [(a,b)],\ [(m',n')] = [(a',b')]$$
$$\Rightarrow [(m+m', n+n')] = [(a+a', b+b')]$$

Ipotesi:

1. $m + b = n + a$
2. $m' + b' = n' + a'$

Tesi:

3. $m + m\text{'} = b + b',\ n + n' = a + a'$

Sommando membro a membro 1. e 2. si ottiene 3.

Proposizione

$(\mathbb{Z}, +, \cdot)$ è un **annello commutativo con unità**.

Lemma

Sia A un anello commutativo con unità:

1. $a \cdot 0 = 0 \cdot a = 0,\ \forall a$
2. $(-a)b = -ab$
3. $(-a)(-b) = ab$

Dimostrazione:

1. $0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$

$$
\begin{aligned}
& (0 + a \cdot 0) + (-a \cdot 0) = (a \cdot 0 + a \cdot 0) + (-a \cdot 0) \\
\text{(assoc.) } & 0 + (a \cdot 0 + (-a \cdot 0)) = a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) \\
& 0 + 0 = a \cdot 0 + 0 \\
& 0 = a \cdot 0
\end{aligned}
$$

2. $0 \overset{1.}{=} 0 \cdot b = (a + b(-a)b = ab + (-a)b$

   Che è quello che si vuole: $(-a)b$ è l'elemento che devo sommare ad ab per ottenere 0. $-ab = (a)b$

3. $(-a)(-b) \overset{2.}{=} -(a(-b)) \overset{2.}{=} -(-ab) = ab$

Proposizione

Se $a, b \in \mathbb{Z}, ab = 0$ se e solo se $b = 0$ oppure $a = 0$

Dimostrazione: Si usa il fatto che gli interi hanno un segno

$$\mathbb{Z} = \mathbb{Z}_+ \cup \mathbb{Z}_- \cup \{0\}$$

Se $a, b > 0$ per la definizione di prodotto $ab > 0$

Se $a, b < 0$ per il lemma:

$$ab = \overset{>0}{(-a)}\overset{>0}{(-b)} > 0$$

Se $a > 0, b < 0$ allora $-b > 0$ e per il lemma

$$0 < a(-b) = -ab \Rightarrow ab > 0$$

Costruzione di Q a partire da Z

Siano $X = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ e ρ una relazione di equivalenza su X definita nel seguente modo:

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

Idea:

$$\frac{n}{m} = \frac{n'}{m'}$$

Bisogna dimostrare che:

1. ρ è una relazione di equivalenza
2. $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}_{/\rho}$
3. $\mathbb{Q}$ è un campo, quindi vanno definite le operazioni

$$[(m,n)] + [(m',n')] = [(mn' + nm', nn')]$$

questo perché

$$\frac{n}{m} + \frac{n'}{m'} = \frac{nm' + n'm}{mm'}$$

Poi

$$\begin{aligned} [(m,n)][(m',n')] &= [(mm', nn')] \\ -[(m,n)] &= [(-n,m)] \\ [(m,n)]^{-1} &= [(n,m)] \\ 0 &= [(0,1)] \\ 1 &= [(1,1)] \end{aligned}$$

Lezione 05 - 10/10/2022

Esercizio operazioni ben poste

$$\begin{aligned} \mathbb{R} \quad & x \sim_1 y \text{ se } [x] = [y] \\ & x \sim_2 y \text{ se } \{x\} = \{y\} \end{aligned}$$

Dove con:

- $[x] = \text{parte intera } \leq x$
- $\{x\} = \text{parte frazionaria } x - [x]$

$\sim_1$ e $\sim_2$ sono relazioni di equivalenza in quanto sono definite in **termini di uguaglianza**.

Chiamiamo:

- $\bar{x} = x \mod \sim_1 \qquad (\bar{x} = \{y \in \mathbb{R} : y \sim_1 x\})$
- $\tilde{x} = x \mod \sim_2$

Definiamo

$$\begin{aligned} \bar{x} +_1 \bar{y} &= \overline{x + y} \\ \tilde{x} +_2 \tilde{y} &= \widetilde{x + y} \end{aligned}$$

Sono ben poste?

$+_1$ **non è ben posta**. Vengano presi $\overline{0.2} = \overline{0.8}$

$$\begin{aligned} \overline{0.2} + \overline{0.2} = \overline{0.2 + 0.2} = \overline{0.4} = 0 \\ \overline{0.8} + \overline{0.8} = \overline{0.8 + 0.8} = 1.6 \end{aligned}$$

Ma $0 \neq 1.6$ anche se abbiamo posto $\overline{0.2} = \overline{0.8}$. Questo significa che l'operazione **dipende** dai rappresentanti che vengono scelti.

$+_2$ invece è **ben posta**. Per dimostrarlo si osserva che

$$x \sim_2 y \Leftrightarrow x - y \in \mathbb{Z} \quad (\text{differiscono per un intero})$$

È facile vedere che $+_2$ è ben posta:

$$\widetilde{x} = \widetilde{x_1}, \tilde{y} = \widetilde{y_1} \text{ allora } \widetilde{x+y} = \widetilde{x_1 + y_1}$$

<u>Ipotesi</u>:

$$x - x_1 = n, y - y_1 = m$$
$$x + y - (x_1 + y_1) = x - x_1 + y - y_1 = n + m \in \mathbb{Z}$$

Definizioni: divisore dello zero, dominio di integrità, elemento invertibile, elementi associati, elemento irriducibile, elemento primo

Sia A un **anello commutativo con unità**:

1. Un elemento $a \in A, a \neq 0$ si dice **divisore dello zero** se esiste $b \in A, b \neq 0 : ab = 0$
2. Un **dominio di intregrità** è un anello commutativo con unità **privo** di divisori dello 0
3. Se $a, b \in A$ diciamo che $a \mid b$ se $\exists c \in A : b = ac$
4. Un elemento $a \in A : a \mid 1$ si dice **invertibile**
5. Due elementi $a, b \in A : a \mid b \wedge b \mid a$ si dicono **associati**
6. Un elemento $a \in A, a \neq 0, a$ non invertibile si dice **irriducibile** se

$$a = bc \Rightarrow b \text{ invertibile o } c \text{ invertibile}$$

7. Un elmento $a \in A, a \neq 0, a$ non invertibile si dice **primo** se

$$a \mid bc \Leftrightarrow a \mid b \text{ oppure } a \mid c$$

Commenti ed esempi

- In $\mathbb{Z}_6, \overline{2} \cdot \overline{3} = \overline{0}$

  Per lo stesso motivo, se $n = ab \text{ con } a, b \neq 1$ allora $\mathbb{Z}_n$ non è un domino di integrità

- È stato già dimostrato che $\mathbb{Z}$ è un dominio di integrità

- Dire che $a \mid 1$ significa dire che $\exists b \in A : ab = 1$

- È immediato osservare che in $\mathbb{Z}$ gli unici elementi invertibili sono ± 1 perchè la relazione in $\mathbb{Z}$

  $$ab = 1$$

  è possibile solo quando $a = b = 1$ oppure $a = b = -1$

Proposizione

In un dominio di integrità

$$a \text{ primo} \Rightarrow a \text{ riducibile}$$

<u>Dimostrazione</u>: Supponiamo $a \text{ primo}$ e facciamo vedere che se $a = bc$ allora b è invertibile o c è invertibile.

Se $a = bc$, in particolare $a \mid bc$, quindi per ipotesi $a \mid b$ oppure $a \mid c$.

Se $a \mid b$ significa che $b = ad$, quindi $a = bc$ diventa

$$a = adc$$
$$a(1 - dc) = 0$$

Poichè $a \neq 0$ per l'ipotesi, $1 - dc = 0$ ovvero $dc = 1$ ovvero c è **invertibile**.

Se $a \mid c$ si procede allo stesso modo: $c = af$, allora

$$a = bc$$
$$a = baf$$
$$a(1 - bf) = 0$$
$$\Rightarrow bf = 1 \Leftrightarrow b \text{ è invertibile}$$

MCD e algoritmo euclideo in Z

Definizione: $a, b \in \mathbb{Z}$. Un numero $d \in \mathbb{Z}$ si dice un MCD(Massimo Comun Divisore) tra a e b se:

1. $d \mid a, \quad d \mid b$
2. $d' \mid a, \quad d' \mid b \Rightarrow d' \mid d \text{ } (d \text{ è il più grande})$

Nomenclatura: due interi a, b tali che $\text{MCD}(a, b) = 1$ si dicono **coprimi**, ovvero non hanno divisori comuni.

Proposizione

Dati $a, b \in \mathbb{Z}, b \neq 0 \ \exists! q, r \in \mathbb{Z} : a = bq + r, \ 0 \leq r < |b|$.

Esempi:

$$\begin{aligned} 29, 7 &\rightsquigarrow 29 = 7 \cdot 4 + 1 \\ -29, 7 &\rightsquigarrow -29 = 7 \cdot (-5) + 6 \\ 29, -7 &\rightsquigarrow 29 = (-7) \cdot (-4) + 1 \\ -29, -7 &\rightsquigarrow -29 = (-7) \cdot 5 + 6 \\ 6, 7 &\rightsquigarrow 6 = 7 \cdot 0 + 6 \end{aligned}$$

Dimostrazione: Ricordiamo che dati a, b dobbiamo trovare q, r tali che

$$a = bq + r, \quad 0 \leq r < |b|$$

Vanno dimostrate **esistenza** e **unicità** di questi due elementi

- **Esistenza**:

  Sia $a > 0$. Procediamo per induzione su a.

  Se $a = 0$, poniamo $q = 0$ e $r = 0$ (base)

  Se $|b| > a$, posso porre $q = 0$ e $r = a$

  Quindi posso supporre $|b| \leq a$, cioè $a - |b| \geq 0$ e $a > a - |b|$, per induzione esistono q' e r' tali che

$$\begin{aligned} a - |b| &= q'b + r', \quad 0 \leq r' < |b| \\ a &= |b| + q'b + r' \end{aligned}$$

Se $b > 0$

$$a = \underbrace{b(1+q')}_{=q} + \underbrace{r'}_{=r} \quad 0 \le r < |b|$$

Se $b < 0$

$$\begin{aligned} a &= -b + q'b + r' \\ &= \underbrace{b(q'-1)}_{=q} + \underbrace{r'}_{=r} \quad 0 \le r < |b| \end{aligned}$$

Se $a < 0,\ -a > 0$ posso quindi usare la prima parte con $-a$. Per i dettagli, vedere sul libro di testo.

- **Unicità**

$$a = \overbrace{bq + r}^{(1)} = \overbrace{bq' + r'}^{(2)} \quad \begin{aligned} 0 \le r < |b| \\ 0 \le r' < |b| \end{aligned}$$

Possiamo assumere $r' \ge r$. Sottraiamo (1) da (2)

$$\begin{aligned} &0 \le r' - r = b(q - q') \\ &|b||q - q'| = |r' - r| = r' - r \le r' < |b| \end{aligned}$$

Siccome $b \neq 0$, da $|b||q-q'| < |b|$ segue che $|q - q'| < 1 \Rightarrow q = q'$.

Ma se $q = q'$

$$bq + r = bq' + r' = bq + r'$$

Quindi bq ha come resti sia r che r', che deve significare che $r = r'$.

Teorema - Identità di Bezout

Dati $a, b \in \mathbb{Z}$ non entrambi 0, esiste $d = \mathrm{MCD}(a, b)$. Inoltre esistono interi $s, t \in \mathbb{Z}$ tali che:

$$d = sa + tb$$

tale espressione viene chiamata **identità di Bezout** e ne esistono infinite.

Dimostrazione: ricordiamo che il principio di induzione è equivalente al principio del minimo: ogni sottoinsieme $S \neq \emptyset, S \subseteq \mathbb{N}$, ha minimo.

Poniamo $S = \{xa + yb > 0 | x, y \in \mathbb{Z}\}$:

- $S \neq \emptyset$: supponiamo $a \neq 0$. Se $a > 0, a \in S$. Se $a < 0, -a \in S$. Per costruzione $S \subseteq \mathbb{N}$.

  Per il principio del minimo esiste $d = \min S$. Dico che $d = \mathrm{MCD}(a, b)$. Dimostro che $d \mid a$ facendo la divisione con resto di a per d e mostrando che il resto è 0.

$$\begin{gathered} a = qd + r, \quad 0 \leq r < d \\ 0 \leq r = a - qd \stackrel{*}{=} a - q(x_0 a + y_0 b) = \\ = (1 - x_0 q)a - q y_0 b \leq d \end{gathered}$$

  $*$: $d = x_0 a + y_0 b$ in quanto $d \in S$ siccome abbiamo detto che $d = \min S$ e gli elementi di S sono della forma $xa + yb$.

  Se $r \neq 0$, ho dimostrato che $r \in S$, $r < d = \min S$ (contraddizione, in quanto risulta che r è minore di d).

  Questo significa che $r = 0$ e quindi abbiamo dimostrato che $d \mid a$ e similmente $d \mid b$. Inoltre è chiaro che se $d' \mid a$ e $d' \mid b$ allora $d' \mid d$.

  Infatti se $a = hd', b = kd'$ allora

$$d = x_0 a + y_0 b = x_0 h d' + y_0 k d' = (x_0 h + y_0 k) d'$$

  e qunque $d' \mid d$.

Lezione 06 - 13/10/2022

Algoritmo euclideo

Notazione: Si chiama $(a,b) = \mathrm{MCD}$ positivo di a, b.

Nel seguito vediamo come:

1. Calcolare algoritmicamente (a,b)
2. Trovare un’identità di bezout per (a,b)

Esempio:

- $(3522, 321)$

$$\begin{aligned} 3522 &= 321 \cdot 10 + 312 \\ 321 &= 312 \cdot 1 + 9 \\ 312 &= 9 \cdot 34 + 6 \\ 9 &= 6 \cdot 1 + \underline{3} \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Dove l’ultimo resto non nullo nella catena di divisioni è il risultato, in questo caso $(3522, 321) = 3$.

Vediamo l’dentità di bezout: cerchiamo un’espressione del tipo $3 = x \cdot 321 + y \cdot 3522$

$$
\begin{aligned}
3 &= 9 - 6 \\
&= 9 - (312 - 9 \cdot 34) \\
&= 9 \cdot 35 - 312 \\
&= (321 - 312) \cdot 35 - 312 \\
&= 321 \cdot 35 - 312 \cdot 36 \\
&= 321 \cdot 35 - (3522 - 321 \cdot 10) \cdot 36 \\
&= -3522 \cdot 36 + 321 \cdot 35 + 321 \cdot 360 \\
&= -3522 \cdot 36 + 321 \cdot 395
\end{aligned}
$$

quindi abbiamo che $3 = -3522 \cdot 36 + 321 \cdot 395$.

- $(57, 23)$

$$
\begin{aligned}
57 &= 23 \cdot 2 + 11 \\
23 &= 11 \cdot 2 + \underline{1} \\
11 &= 1 \cdot 11 + 0
\end{aligned}
$$

Quindi $(57, 23) = 1$ (sono coprimi)

Vediamo l'identità di bezout: cerchiamo un'espressione del tipo $1 = x \cdot 23 + y \cdot 57$

$$
\begin{aligned}
1 &= 23 - 11 \cdot 2 \\
&= 23 - (57 - 23 \cdot 2) \cdot 2 \\
&= 23 - 57 \cdot 2 + 23 \cdot 4 \\
&= 23 \cdot 5 - 57 \cdot 2
\end{aligned}
$$

quindi abbiamo che $1 = 23 \cdot 5 - 57 \cdot 2$.

Proposizione - Soluzioni di ax+by=c

L'equazione $(1) ax + by = c,\ a, b, c \in \mathbb{Z}$ possiede una soluzione intera

$$(x, y) \in \mathbb{Z} \text{ sse } (a, b) \mid c$$

Esempi:

- $2x + 2y = 5$ non ha soluzione intere perche $(2, 2) \nmid 5$

- $2x + 2y = 4$ ha soluzioni intere, ad esempio $x = y = 1$

Dimostrazione: supponiamo che l'equazione (1) abbia soluzione $(\bar{x}, \bar{y})$. Allora vale

$$a\bar{x} + b\bar{y} = c$$

Sia $d = (a, b)$ con $d \mid a$ e $d \mid b$, quindi $d \mid a\bar{x}, d \mid b\bar{y}$, quindi $d \mid a\bar{x} + b\bar{y} = c$ come vogliamo.

Viceversa, supponiamo che $d \mid c$. Scriviamo l'**identità di bezout** per d:

$$d = \alpha a + \beta b$$

Poichè $d \mid c, c = hd$

$$c = hd = \underbrace{h\alpha}_{x} a + \underbrace{h\beta}_{y} b$$

Proposizione - In Z ogni irriducibile è primo

In $\mathbb{Z}$ ogni **irriducibile** è **primo**.

Dimostrazione: Supponiamo p **irriducibile** e $p \mid ab$. Dobbiamo far vedere che se $p \nmid a$ allora $p \mid b$.

Siccome $p \mid ab,\ ab = ph \Rightarrow (a, p) = 1$.

Dunque esistono $s, t \in \mathbb{Z}$ t.c. $as + tp = 1$. Moltiplico questa relazione per b

$$b = bas + btp = \overbrace{abs}^{p|} + \overbrace{pbt}^{p|} \Rightarrow p \mid b$$

Teorema fondamentale dell'aritmetica

Sia $n > 1$ un intero. Allora n è prodotto di un numero finito di potenze di primi:

$$n = p_1^{h_1} ... p_s^{h_s} \quad h_i > 0,\ p_i \neq p_j,\ i \neq j$$

Inoltre tale fattorizzazione è unica nel senso che se

$$n = q_1^{k_1} ... q_t^{k_t} \quad k_i > 0,\ q_i \neq q_j, i \neq j, q_i \text{ primi}$$

allora $s = t$ a meno di **rioridinamenti $p_i = q_i$ e $h_i = k_i$.**

Dimostrazione:

- **Esistenza**: per induzione su n, con base ovvia $n = 2$.

  Supponiamo di avere dimostrato l'esistenza della fattorizzazione per ogni intero $k,\ 2 \leq k < n$ e dimostriamola per n.

  Se n è **primo** non c'è **nulla da dimostrare**.

  Altrimenti **non è irriducibile**, quindi può scriversi come

$$
\begin{aligned}
n = n_1 n_2, \quad & 2 \leq n_1 < n \\
& 2 \leq n_2 < n
\end{aligned}
$$

  Per induzione n_1, n_2 hanno fattorizzazione e quindi anche n ce l'ha

$$
n_1 = p_1^{a_1} ... p_s^{a_s} \ , \quad n_2 = q_1^{b_1} ... q_s^{b_s}
$$
$$
n = p_1^{a_1} ... p_s^{a_s} q_1^{b_1} ... q_s^{b_s} = t_1^{c_1} ... t_n^{c_n} \text{ con i } t_i \ \underline{\text{primi}}
$$

  Esempio:

$$
\begin{aligned}
n_1 &= 2^3 \cdot 3^4 \cdot 5 \\
n_2 &= 2^3 \cdot 3 \cdot 5 \cdot 7 \\
n_1 n_2 &= 2^6 \cdot 3^5 \cdot 5^2 \cdot 7
\end{aligned}
$$

- **Unicità**: Si consideri $n = p_1^{h_1} ... p_s^{h_s} \ (*)$

  Procediamo per induzione su $m = h_1 + ... + h_s$

  - Caso base: $m = 1$; la $(*)$ ci dice che n è primo. **Supponiamo** che ci sia **un'altra fattorizzazione in primi**. Sia p

$$
\begin{aligned}
p = n = q_1^{k_1} ... q_t^{k_t} \\
\implies p \mid q_1^{k_1} ... q_t^{k_t}
\end{aligned}
$$

    Poichè p è primo, p **divide uno dei** q_i

$$
p \mid q_i
$$

    ma q_i è primo, quindi $p = q_i$. Allora

$$p = q_1^{k_1} ... p^{k_i} ... q_t^{k_t}$$

implica

$$\begin{aligned} 1 &= q_1^{k_1} ... p^{k_i - 1} ... q_t^{k_t} \\ \implies k_1 &= ... = k_{i-1} = k_{i+1} = ... = k_t = 0 \quad k_i = 1 \end{aligned}$$

Quindi la seconda fattorizzazione è proprio $n = q_i = p$.

- Caso $m > 1$: **supponiamo** che n abbia **due fattorizzazioni.**

$$(**) n = p_1^{h_1} ... p_s^{h_s} = q_1^{k_1} ... q_t^{k_t}$$

con $h_1 + ... + h_s = m_i$ come prima

$$p_1 \mid q_1^{k_1} ... q_t^{k_t}$$

quindi come prima $p_1 \mid q_i$ e quindi $p_1 = q$.

Allora $(**)$ diventa

$$\begin{aligned} p_1^{h_1} ... p_s^{h_s} &= q_1^{k_1} ... p_1^{k_i} ... q_t^{k_t} \\ p_1^{h_1 - 1} ... p_s^{h_s} &= q_1^{k_1} ... p_1^{k_i - 1} ... q_t^{k_t} \end{aligned}$$

Al primo membro la somma degli esponenti è $m - 1$. Per induzione ho l'unicità della fattorizzazione, quindi $h_i - 1 = k_i - 1$ e gli altri fattori coincidono a meno di riordinamento. Quindi la **fattorizzazione di n è unica**.

> ⚠️ Si noti come nel corso della dimostrazione si sia utilizzata pesantemente l'equivalenza in $\mathbb{Z}$ tra l'essere **primo** e l'essere **irriducibile**.

Proposizione - I numeri primi sono infiniti

Dimostrazione: supponiamo il viceversa, ovvero che $p_1 ... p_N$ sia la lista **finita** di tutti i numeri primi. Sia

$$M = p_1 \cdot ... \cdot p_N + 1$$

Osserviamo che M da resto 1 quando è diviso per ogni numero primo, quindi M **non è divisibile** per nessun primo, **contro il teorema fondamentale dell'aritmetica**$\blacksquare$

Congruenze e sistemi di congruenze

Vogliamo risolvere equazioni del tipo

$$ax = b \text{ in } \mathbb{Z}_n$$

ovvero **congruenze** del tipo

$$ax \equiv b \mod n$$

e anche sistemi del tipo

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ ... \\ a_k x \equiv b_k \mod n_k \end{cases}$$

Proprietà fondamentali delle congruenze

Ricordiamo che $a \equiv b \mod n$ se $n \mid b - a$

$$\begin{aligned} a &= xn + r \\ b &= yn + r \\ b - a &= (x - y)n \Rightarrow n \mid b - a \end{aligned}$$

viceversa se $n \mid b - a,\ b - a = hn$, se

$$\begin{aligned} a &= xn + r_1 \\ b &= yn + r_2 \\ b - a &= (x - y)n + r_1 - r_2 \\ &= hn \Rightarrow r_1 = r_2 \end{aligned}$$

> ⚠️ Il fatto che $r_1 = r_2$ segue dal fatto che n divide $a - b$, quindi il resto deve essere 0. Questo accade solo se $r_1 = r_2$.

Sia $a \equiv_n b$; allora

1. $a + c \equiv_n b + c$
2. $ac \equiv_n bc$
3. $a^i \equiv_n b^i,\ i \geq 0$
4. $ac \equiv_n bc,\ (c, n) = 1 \Rightarrow a \equiv_n b$

$$\begin{aligned} n \mid bc - ac = (b - a)c \\ (c, n) = 1 \Rightarrow \exists s, t : cs + tn = 1 \\ b - a = (b - a)cs + (b - a)tn \\ = ns + (b - a)tn \\ = n(s + (b - a)t) \end{aligned}$$

   Dunque $n \mid b - a$, ovvero $a \equiv_n b$.

5. $ac \equiv bc \mod n \Rightarrow a \equiv b \mod \dfrac{n}{(n, c)}$

> ⚠️ Nota: **non** è vero che $ac \equiv_n bc \Rightarrow a \equiv_n b$, ovvero non è vero che si può dividere per c. Esempio:
>
> $$\begin{aligned} 3 \cdot 5 \equiv 3 \cdot 8 \mod 9 \\ 15 \equiv 24 \mod 9 \\ 6 \equiv 6 \mod 9 \checkmark \end{aligned}$$
>
> Ma $5 \not\equiv 8 \mod 9$.

Lemma

Sia p primo e $x, y \in \mathbb{Z}$,

$$(x + y)^p = x^p + y^p \mod p$$

Dimostrazione:

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

Ma $p \mid \binom{p}{k}$ se $k \neq 0, p$, quindi nella somma restano solo il primo e l'ultimo termine $\bmod p$

$$(x+y)^p = \underbrace{\binom{p}{0}}_{=1} x^0 + y^{p-0} + \underbrace{\binom{p}{p}}_{=1} x^p y^{p-k} = x^p + y^p$$

Teorema - Piccolo teorema di Fermat

Sia $a \in \mathbb{Z}$, p un **numero primo**, allora

$$a^p \equiv a \mod p$$

Dimostrazione: Se $a \geq 0$, **procediamo per induzione** su a

- $a = 0$

  Non c'è niente da dimostrare

- $a > 0$

  Assumiamo $a^p \equiv a \mod p$ sia vero e dimostriamo che $(a+1)^p \equiv a+1 \mod p$.

  $$(a+1)^p \equiv a^p + 1^p \equiv a^p + 1 \equiv a+1 \mod p$$

- $a < 0$

  $$0 = 0^p = (a + (-a))^p \equiv a^p + (-a)^p \equiv a^p - a \Rightarrow a^p \equiv a \mod p$$

  Nota: dato che $-a > 0$, per quanto provato nel punto precedente si ha che $(-a)^p \equiv -a$.

Corollario

Se $(a, p) = 1$, allora $a^{p-1} \equiv 1 \mod p (*)$.

Dimostrazione: Se $(a,p)=1$, posso semplificare a nella relazione $a^p \equiv a \mod p$, ottenendo $(*)$

Lezione 07 - 14/10/2022

Ripasso - Elementi invertibili

Ricordiamo che se A è un **anello commutativo con unità**, un elemento $a \in A$ si dice **invertibile** se

$$\exists b \in A : ab = 1$$

Esempio: In $\mathbb{Z}$ gli elementi invertibili sono ± 1.
Osserviamo inoltre che gli elementi invertibili di A **formano un gruppo rispetto al prodotto**. Infatti basta verificare che il prodotto di elementi invertibili è invertibile: Se a, b sono invertibili, esistono

$$c, d \in A : ac = 1 \quad bd = 1$$

ma allora

$$(ab)(cd) = acbd = 1 \cdot 1 = 1$$

Osservazione: $\{\pm 1\}$ è un gruppo rispetto al prodotto. La tabella moltiplicativa è:

	1	-1
1	1	-1
-1	-1	1

Proposizione

$\bar{a} \in \mathbb{Z}_n$ è invertibile se e solo se $(a, n) = 1$

Corollario

$\{\bar{a} \in \mathbb{Z}_n : 0 < a < n,\ (a, n) = 1\}$ è un gruppo (che spesso viene denotato con $\mathbb{U}_n$)

Dimostrazione: supponiamo che $(a, n) = 1$. Scriviamo l'**identità di bezout**:

$$ab + ns = 1$$

prendiamo le classi resto $\bmod n$

$$\begin{aligned} \overline{ab + ns} &= \overline{1} \\ \overline{a}\overline{b} + \underbrace{\overline{ns}}_{=\overline{0}} &= \overline{1} \\ \overline{a}\overline{b} &= \overline{1} \end{aligned}$$

Dunque $\overline{a}$ è invertibile e $\overline{b}$ è l'**inverso**.
Viceversa, se $\overline{a}$ è **invertibile**, esiste $\overline{b} \in \mathbb{Z}_n$ con $\overline{a}\overline{b} = \overline{1}$, cioè

$$\begin{aligned} &ab \equiv 1 \quad \bmod n \\ &ab - 1 = kn \\ &\underbrace{ab - kn = 1}_{\text{identità di bezout}} \ \Rightarrow (a, n) = 1 \end{aligned}$$

Esempi esercizi:

1. Trovare gli **elementi invertibili** in $\mathbb{Z}_{42}$

$$42 = 2 \cdot 3 \cdot 7$$
$$\{\overline{1}, \overline{5}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{37}, \overline{41}\}$$

   Procedimento:

   - Si prende il modulo
   - Si fattorizza
   - Si prendono i fattori che non hanno multipli in comune

2. Trovare l'inverso di $\overline{31}$ in $\mathbb{Z}_{42}$

$$
\begin{aligned}
42 &= 31 + 11 \\
31 &= 11 \cdot 2 + 9 \\
11 &= 9 \cdot 1 + 2 \\
9 &= 2 \cdot 4 + 1
\end{aligned}
$$

Scriviamo ora l'identità di bezout

$$
\begin{aligned}
1 &= 9 - 2 \cdot 4 \\
&= 9 - (11 - 9) \cdot 4 \\
&= 9 \cdot 5 - 11 \cdot 4 \\
&= (31 - 11 \cdot 2)5 - 11 \cdot 4 \\
&= 31 \cdot 5 - 11 \cdot 14 \\
&= 31 \cdot 5 - (42 - 31) \cdot 14 \\
&= 31 \cdot 19 - 42 \cdot 14
\end{aligned}
$$

Quindi l'inverso di $\overline{31}$ è $\overline{19}$ in $\mathbb{Z}_{42}$ in quanto $\overline{31} \cdot \overline{19} = \overline{1}$.

Spoiler - la cardinalità di Un

Definizione: funzione ϕ di Eulero

$$\phi(n) = |\{a \in \mathbb{N}, 1 \leq a <, (a, n) = 1\}|$$

Teorema: $\phi(n)$ si calcola a partire dalla fattorizzazione di n usando le due segenti regole:

1. Se p **primo**, $\phi(p^n) = p^n - p^{n-1}$
2. Se $(r, s) = 1$, $\phi(rs) = \phi(r) \cdot \phi(s)$

Esempio:

- Calcolo di $\phi(42)$

$$
\begin{aligned}
\phi(42) = \phi(2 \cdot 3 \cdot 7) &\overset{(2)}{=} \phi(2)\phi(3)\phi(7) \\
&\overset{(1)}{=} (2-1)(3-1)(7-1) = 1 \cdot 2 \cdot 6 = 12
\end{aligned}
$$

- Calcolo di $\phi(100)$

$$
\begin{aligned}
\phi(100) = \phi(2^2 \cdot 2^5) &= \phi(2^2)\phi(2^5) \\
&= (2^2 - 2)(5^2 - 2) = (4-2)(25-5) = 40
\end{aligned}
$$

Congruenze lineari

Una **congruenza lineare** è un'equazione della forma

$$ax \equiv b \mod n$$

con $a, b \in \mathbb{Z},\ n \in \mathbb{N}$.

> ⚠️ Può essere pensata come l'equazione $\bar{a}\bar{x} = \bar{b}$ in $\mathbb{Z}_n$

Proposizione

Una congruenza $ax \equiv b \mod n$ ha soluzione se e solo se $(a, n) \mid b$.

Dimostrazione:

$$ax \equiv b \mod n \iff ax - b = kn \iff ax - kn = b$$

ovvero, la congruenza $ax \equiv b \mod n$ ha soluzione se e solo se l'**equazione diofantea** $ax - kn = b$ **ha soluzione**, che accade se e solo se $(a, n) \mid b$.

Proposizione

Sia $ax \equiv b \mod n$ una **congruenza lineare** con $(a, n) \mid b$. Se x_0 è una soluzione, **tutte le soluzioni** sono del tipo

$$x_0 + h \cdot \underbrace{\frac{n}{(a,n)}}_{\text{è un intero}}, \quad h \in \mathbb{Z}$$

tra queste le soluzioni con $0 \leq h < (a, n)$ sono **a due a due non congruenti** e **ogni altra soluzione è congruente a una di esse**.

Esempio: $2x \equiv 4 \mod 8$ con $d = (a, n) = 2$.

Le soluzioni fondamentali sono: $x_0,\ x_0 + 4$. Ad esempio:

- $x_0 = 2$

- $x_0 = 4$

Proviamo che $x_0 + h \cdot \frac{n}{d}$ (abbiamo posto $d = (a,n)$) è una soluzione:

$$\begin{aligned} a(x_0 + h \cdot \frac{n}{d}) &= ax_0 + ah \cdot \frac{n}{d} \\ &\equiv b + \underbrace{\text{m.c.m}(a,n) \cdot h}_{\text{è un multiplo di n}} \\ &\equiv b \mod n \end{aligned}$$

Proviamo ora che **ogni soluzione è di questo tipo**: siano x_0, x_0' due soluzioni, allora

$$\begin{aligned} &ax_0 = b + hn,\ ax_0' = b + kn \\ &a(x_0 - x_0') = (h-k)n \\ &\frac{a}{d}(x_0 - x_0') = (h-k)\frac{a}{d} \end{aligned}$$

$$(\frac{a}{d}, \frac{n}{d}) = 1 \quad \begin{aligned} &\frac{n}{d} \mid x_0 - x_0' \\ &x_0 - x_0' = h \cdot \frac{n}{d} \\ &x_0 = x_0' + h \cdot \frac{n}{d} \end{aligned}$$

Resta da vedere che le soluzioni $x_0 + h \cdot \frac{n}{d} \quad 0 \le h < d$

1. Sono **a due a due non congruenti**
2. Che **ogni altra soluzione è congruente a una di loro**

<u>Dimostrazione per 1.</u>: Supponiamo per assurdo che

$$x_0 + h_1 \cdot \frac{n}{d} \equiv x_0 + h_2 \cdot \frac{n}{d} \mod n, \quad 0 \le h_1 < h_2 < d \ (1)$$

allora

$$h_1 \cdot \frac{n}{d} \equiv h_2 \cdot \frac{n}{d} \mod n$$

dunque

$$h_1 \equiv h_2 \mod \frac{n}{n/d}$$

e qundi $h_1 \equiv h_2 \mod d$ che è **assurdo** per (1).

> ℹ️ Si ricorda che per la proprietà 5 delle congruenze
>
> $$ac \equiv bc \mod n$$
> $$a \equiv b \mod \frac{n}{(n,c)}$$

Dimostrazione per 2: prendiamo una soluzione $x_0 + h \cdot \frac{n}{d}$ e dividiamo h per d:

$$h = dq + r \quad 0 \leq r < d$$
$$x_0 + h \cdot \frac{n}{d} = x_0 + (dq + r)\frac{n}{d} = x_0 + nq + r\frac{n}{d} \equiv x_0 + r\frac{n}{d} \mod n$$

Corollario

Se $(a, n) = 1$, la congruenza $ax \equiv b \mod n$ **ammette soluzione unica** $\mathrm{mod}\ n$.

Esempio:

$$5x \equiv 16 \mod 7$$
$$\overline{5}\overline{x} = \overline{16} = \overline{2} \text{ in } \mathbb{Z}_7$$

L'inverso di $\overline{5}$ in $\mathbb{Z}_7$ è $\overline{3}$

$$\overline{3} \cdot \overline{5}\overline{x} = \overline{3} \cdot \overline{2}$$
$$\overline{x} = \overline{6}$$
$$x = 6 + 7k, \ k \in \mathbb{Z}$$

> ⚠️ Devo trovare l'inverso di $\overline{5}$ per isolare la $\overline{x}$.

Sistemi di congurenze lineari

Vogliamo ora risolvere sistemi di congruenze lineari del tipo

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ ... \\ a_s x \equiv b_s \mod n_s \end{cases}$$

Supponiamo dapprima $(n_i, n_j) = 1, \ i \neq j$.

Supponiamo inoltre $d_i = (a_i, n_i) \mid b_i$.

Se divido per d_i ciascuna equazione, ottengo un sistema del tipo:

$$\begin{cases} a_1' x \equiv b_1' \mod n_1' \\ a_2' x \equiv b_2' \mod n_2' \\ ... \\ a_s' x \equiv b_s' \mod n_s' \end{cases}$$

con $a_i = \dfrac{a_i}{d_i}$, $b_i = \dfrac{b_i}{d_i}$ e $n_i = \dfrac{n_i}{d_i}$.

Ma allora $(a_i', n_i') = 1$ quindi a_i' è invertibile in $\mathbb{Z}_n$ e quindi il sistema può riscriversi nella forma

$$\begin{cases} x \equiv c_1 \mod n_1' \\ ... \\ x \equiv c_s \mod n_s' \end{cases}$$

con $c_i = a_i'^{-1}, \ (n_i', n_j') = 1, \ i \neq j$.

<u>Esempio</u>:

$$\begin{cases} 1025x \equiv 5312065 \mod 8 \\ 36x \equiv 322 \mod 5 \\ 4x \equiv 7 \mod 3 \end{cases}$$

si trasforma in

$$\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 3 \end{cases}$$

soluzione

$$\begin{aligned} x &= 1 + 8n \\ 1 + 8n &\equiv 2 \mod 5 \\ 8n &\equiv 1 \mod 5 \\ 3n &\equiv 1 \mod 5 \\ n &\equiv 2 \mod 5 \end{aligned}$$

$$\begin{aligned} n &= 2 + 5m \\ x &= 1 + 8n = 1 + 8(2 + 5m) = \\ &= 17 + 40m \end{aligned}$$

$$\begin{aligned} 17 + 40m &\equiv 1 \mod 3 \\ 2 + m &\equiv 1 \mod 3 \\ m &\equiv -1 \mod 3 \\ m &\equiv 2 \mod 3 \\ m &= 2 + 3s \end{aligned}$$

$$\begin{aligned} x &= 17 + 40m = 17 + 40(2 + 3s) = \\ &= 97 + 120s \end{aligned}$$

Lezione 09 - 20/10/2022

Teorema cinese del resto

Il sistema di congruenze

$$\begin{cases} x \equiv c_1 \mod r_1 \\ x \equiv c_2 \mod r_2 \\ ... \\ x \equiv c_s \mod r_s \end{cases}$$

con $(r_i, r_j) = 1,\ i \neq j$, **ha soluzione unica** $\mod r_1 \cdot r_2 \cdot ... \cdot r_s$.

Dimostrazione: poniamo $R = r_1 \cdot r_2 \cdot ... \cdot r_s,\ R_k = \dfrac{R}{r_k}$.

Ovviamente si ha che $(R_k, r_k) = 1$, quindi la congruenza

$$R_k x \equiv c_k \mod r_k$$

ammette un'unica soluzione $\bar{x}_k \mod r_k$. Pongo

$$\bar{x} = R_1\bar{x}_1 + R_2\bar{x}_2 + ... + R_s\bar{x}_s$$

e dico che $\bar{x}$ risolve il sistema di congruenze. Infatti la **k-esima equazione** è

$$\begin{aligned} x &\equiv c_k \mod r_k \\ \bar{x} &= R_1\bar{x}_1 + R_2\bar{x}_2 + ... + R_s\bar{x}_s \\ &\equiv R_k\bar{x}_k \equiv c_k \mod r_k \end{aligned}$$

Per provare l'unicità $\mod r_1 \cdot ... \cdot r_s$, supponiamo che $\bar{y}$ sia un'altra soluzione:

$$\bar{x} \equiv c_k \equiv \bar{y} \mod r_k,\ \forall k$$

quindi

$$\begin{aligned} \bar{x} - \bar{y} &\equiv 0 \mod r_k,\ \forall k \\ \text{ovvero } \bar{x} - \bar{y} &\equiv 0 \mod r_1 \cdot ... \cdot r_s \end{aligned}$$

ovvero $\bar{x} \equiv \bar{y} \mod r_1 \cdot ... \cdot r_s$.

Esempio:

$$\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 3 \end{cases}$$

si ha che:

- $R = 5 \cdot 8 \cdot 3 = 120$
- $R_1 = 15$
- $R_2 = 24$
- $R_3 = 40$

che forma il seguente sistema

$$\begin{cases} R_1 x \equiv c_1 \mod r_1 \\ R_2 x \equiv c_2 \mod r_2 \\ R_3 x \equiv c_3 \mod r_3 \end{cases}$$

ovvero

$$\begin{cases} 15x \equiv 1 \mod 8 \\ 24x \equiv 2 \mod 5 \\ 40x \equiv 1 \mod 3 \end{cases}$$

ricaviamo ora le $\overline{x}_k$

$$\begin{array}{lllll} 15x \equiv 1 \mod 8 & \rightarrow & -x \equiv 1 \mod 8 & \rightarrow & x \equiv -1 \equiv 7 \mod 8 & \overline{x}_1 = 7 \\ 24x \equiv 2 \mod 5 & \rightarrow & -x \equiv 2 \mod 5 & \rightarrow & x \equiv -2 \equiv 3 \mod 5 & \overline{x}_2 = 3 \\ 40x \equiv 1 \mod 3 & \rightarrow & x \equiv 1 \mod 3 & & & \overline{x}_3 = 1 \end{array}$$

quindi

$$\begin{aligned} \overline{x} &= R_1\overline{x}_1 + R_2\overline{x}_2 + R_3\overline{x}_3 \mod 120 \\ &= 15 \cdot 7 + 24 \cdot 3 + 40 \cdot 1 = 105 + 72 + 40 \\ &= 217 \equiv 97 \mod 120 \end{aligned}$$

e quindi tutte le soluzioni sono del tipo $x = 97 + 120k$.

Proposizione

Siano r, s interi ≥ 2, $(r, s) = 1$. Allora la corrispondenza

$$f : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$$

data da

$$f(x \bmod rs) = (x \bmod r, x \bmod s)$$

è **biunivoca** e **rispetta le operazioni**.

> ⚠️ Più avanti diremo che f è un **isomorfismo di anelli**.

Esempio:

$$\begin{aligned} \mathbb{Z}_6 &\to \mathbb{Z}_3 \times \mathbb{Z}_2 \\ \bar{0} &\mapsto (\bar{0}, \bar{0}) \\ \bar{1} &\mapsto (\bar{1}, \bar{1}) \\ \bar{2} &\mapsto (\bar{2}, \bar{0}) \\ \bar{3} &\mapsto (\bar{0}, \bar{1}) \\ \bar{4} &\mapsto (\bar{1}, \bar{0}) \\ \bar{5} &\mapsto (\bar{2}, \bar{1}) \end{aligned}$$

Dove quello che si trova prima di '$\mapsto$' è inteso in $\bmod 6$, mentre quello che si trova nelle parentesi è inteso rispettivamente alle posizioni nella coppia $\bmod 3$ e $\bmod 2$.

Esempio:

$$\bar{3} + \bar{5} = \bar{8} = \bar{2}$$
$$(\bar{0}, \bar{1}) * (\bar{2}, \bar{1}) = (\bar{2}, \bar{0})$$

Dimostrazione di f biunivoca: Poichè $|\mathbb{Z}_{rs}| = |\mathbb{Z}_r| \times |\mathbb{Z}_s| = rs$, basta vedere che f è **suriettiva**.

Dire che f è suriettiva significa dire che dato $\bar{a} \in \mathbb{Z}_r$, $\bar{b} \in \mathbb{Z}_s$, esiste $x \in \mathbb{Z}_{rs}$ tale che

$$\begin{cases} x \equiv a \mod r \\ x \equiv b \mod s \end{cases} \tag{1}$$

ma questo è garantito dal **teorema cinese dei resti**: il sistema (1) ha soluzione **unica** $\bmod rs$.

Esempio:

$$\begin{cases} 2x \equiv 8 \mod 9 \\ 2x \equiv 6 \mod 15 \end{cases}$$
$$\begin{cases} x \equiv 40 \mod 9 \\ x \equiv 48 \mod 15 \end{cases}$$
$$\begin{cases} x \equiv 4 \mod 9 \\ x \equiv 3 \mod 15 \rightarrow \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 3 \mod 3 \ (*) \end{cases} \end{cases}$$

Sia ha che $x \equiv 0 \mod 3 \Rightarrow 0, 3, 6$ e $(*)$ si può riscrivere come $x = 3k$. Il sistema però non è risolubile.

Teorema di Eulero-Fermat

Ricordiamo prima la **funzione di Eulero**:

$$\phi(n) = |\{x \in \mathbb{N} : 1 \leq x < n,\ (x, n) = 1)\}|$$
$$\phi(rs) = \phi(r)\phi(s) \quad \text{se } (r, s) = 1$$
$$\phi(p^k) = p^k - p^{k-1}$$

e ricordiamo il **piccolo teorema di Fermat**:

$$a^p \equiv a \mod p$$
$$\text{se } (a, p) = 1 \quad a^p \equiv 1 \mod p$$

Teorema: **Teorema di Eulero-Fermat**

Sia $(a, n) = 1$

$$a^{\phi(n)} = 1 \mod n$$

> ⚠️ Se p è **primo**, $\phi(p) = p - 1$, quindi il **piccolo teorema di Fermat** è un caso speciale di **teorema di Eulero-Fermat**

Dimostrazione: per prima cosa proviamo che se p è **primo** e $p \nmid a$ allora

$$a^{\phi(p^k)} \equiv 1 \mod p^k$$

Procediamo per **induzione su k**:

- $k = 1$, si ottiene il **piccolo teorema di Fermat**
- Supponiamo la tesi vera per k e dimostriamola per $k+1$

$$\begin{aligned} &a^{\phi(p^k)} \equiv 1 \mod p^k, \text{ ovvero} \\ &a^{\phi(p^k)} = 1 + hp^k \\ &\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p \cdot \phi(p^k) \end{aligned}$$

dunque

$$\begin{aligned} a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} = (1 + hp^k)^p = \\ &= 1 + \binom{p}{1} hp^k + \binom{p}{2} (hp^k)^2 + ... + \binom{p}{p-1} (hp^k)^{p-1} + (hp^k)^p \equiv 1 \end{aligned}$$

dove tutti gli $hp^k \equiv 0 \mod p^{k+1}$.

In generale, $n = p_1^{h_1} ... p_s^{h_s}$

$$\phi(n) = \phi(p_1^{h_1})...\phi(p_s^{h_s}) \ (*)$$

Da quanto già visto risulta

$$a^{\phi(p_i^{h_i})} \equiv 1 \mod p_i^{h_i} \ (\blacksquare)$$

Inoltre da $(*)$ si ha che $\phi(p_i^{h_i}) \mid \phi(n)$.

Elevando ambo i membri per $(\blacksquare)$ alla $\dfrac{\phi(n)}{\phi(p_i^{h_i})}$ otteniamo

$$a^{\phi(n)} \equiv 1 \mod p_i^{h_i}$$

Ma allora $a^{\phi(n)} \equiv 1 \mod \underbrace{p_1^{h_1} ... p_s^{h_s}}_{=n}$.

Lezione 12 - 27/10/2022

Definzione - Spazio vettoriale

Uno spazio vettoriale su $\mathbb{K}$ (campo) è un **insieme non vuoto** V dotato di un'**operazione binaria** $+$ rispetto alla quale V è un **gruppo abeliano** e di un'applicazione

$$\begin{gathered} \mathbb{K} \times V \to V \\ (\alpha,\ v) \mapsto \alpha v \end{gathered}$$

tale che

$$\begin{array}{cl} (\alpha+\beta)v = \alpha v + \beta v & \forall \alpha, \beta \in \mathbb{K},\ \forall v \in V \\ (\alpha\beta)v = \alpha(\beta v) & \forall \alpha, \beta \in \mathbb{K},\ \forall v \in V \\ \alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2 & \forall \alpha \in \mathbb{K},\ \forall v_1, v_2 \in V \\ 1v = v & \forall v \in V \end{array}$$

Nomenclatura

- Gli elementi di V si chiamano **vettori**
- Gli elementi di $\mathbb{K}$ si chiamano **scalari**

Esempi

1. Sia $\mathbb{K}$ un campo e $V = \mathbb{K}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{K}\}$
   Prendiamo come esempio $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$

   $$\begin{aligned} &(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n) \\ &\alpha(x_1, ..., x_n) = (\alpha x_1, ..., \alpha x_n) \end{aligned}$$

   Esempio pratico

   $$\begin{aligned} &4(2,1,6) + 5(-1,2,\frac{1}{4}) + \frac{3}{2}(0,1,3) = \\ =&(8,4,24) + (-5,10,\frac{5}{4}) + (0,-\frac{3}{2},-\frac{9}{2}) = (3,\frac{25}{2},\frac{83}{4}) \end{aligned}$$

2. Definzione: Una matrice a m righe e n colonne a **coefficienti nel campo** $\mathbb{K}$ è una tabella di elementi di $\mathbb{K}$ del tipo

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & a_{ij} & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Chiamiamo $M_{mn}(\mathbb{K})$ tale insieme.
Diciamo che una matrice è **quadrata** se $m = n$

Notazione:

Se $A \in M_{mn}(\mathbb{K})$ denoto con

- $(A)_{ij}$ l'elemento di posto (i, j)
- A^i l'i-esima colonna
- A_j la j-esima riga

Esempio

$$\begin{gathered} A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 5 & 6 \end{pmatrix} \\ (A)_{11} = 1 \quad (A)_{12} = 2 \quad (A)_{13} = 3 \\ (A)_{21} = 4 \quad (A)_{22} = 5 \quad (A)_{23} = 6 \\ A^1 = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \quad A^2 = \begin{pmatrix} 2 \\ 5 \end{pmatrix} \quad A^3 = \begin{pmatrix} 3 \\ 6 \end{pmatrix} \\ A_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \quad A_1 = \begin{pmatrix} 4 & 5 & 6 \end{pmatrix} \end{gathered}$$

$M_{mn}(\mathbb{K})$ è uno **spazio vettoriale** rispetto a

$$\begin{aligned} (A+B)_{ij} = (A)_{ij} + (B)_{ij} \qquad & 1 \leq i \leq m \\ & 1 \leq j \leq n \\ \alpha \in \mathbb{K} \quad (\alpha A)_{ij} = \alpha (A)_{ij} \qquad & 1 \leq i \leq m \\ & 1 \leq j \leq n \end{aligned}$$

N.B.:

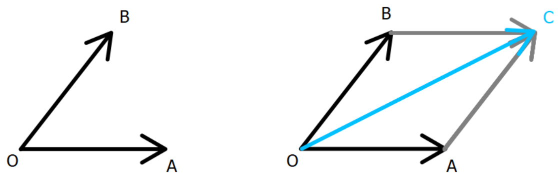
- se $m = n = 1,\ M_{11}(\mathbb{K}) = \mathbb{K}$, dunque ogni campo è uno **spazio vettoriale su se stesso**;
- se $m = 1,\ M_{1n}(\mathbb{K}) = \mathbb{K}^n$, chiamati **vettori riga**;
- se $n = 1,\ M_{m1}(\mathbb{K}) \leftrightarrow \mathbb{K}^m$, chiamati **vettori colonna**.

3. **Vettori geometrici**

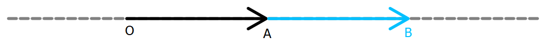
   Consideriamo lo spazio **bidimensionale della geometria euclidea** e fissiamo un punto o. Chiamiamo **vettore** un segmento orientato $\overrightarrow{AB}$. Definiamo una struttura di **spazio vettoriale su** $\mathbb{R}$ sull'insieme ν_0 dei vettori applicati in o.

$$\nu_0 = \{\overrightarrow{OA} : a \in \mathbb{E}^3\}$$

- $\overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{OC}$

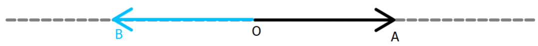


- $0 \cdot \overrightarrow{OA} = \overrightarrow{OO}$
  $\alpha \cdot \overrightarrow{OO} = \overrightarrow{OO}$
  - Se $\alpha > 0$



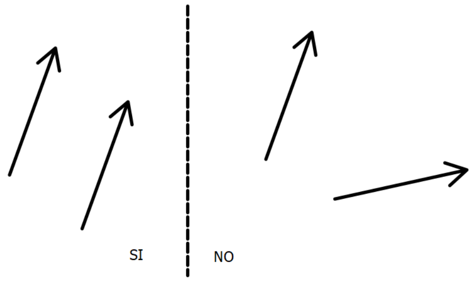
$$\overrightarrow{OB} = \alpha \cdot \overrightarrow{OA}$$

  - Se $\alpha < 0$



$$\overrightarrow{OB} = \alpha \cdot \overrightarrow{OA}$$

Si definiscono poi i **vettori liberi** come lo spazio di vettori applicati modulo la **relazione di equivalenza** che identifica due vettori applicati se esiste una **traslazione** che manda uno all'altro



le operazioni di ν_0 passano al quoziente.

Prodotto righe per colonne tra matrici

Per comodità scrivo M_{mn} invece di $M_{mn}(\mathbb{K})$.

$$M_{ms} \times M_{sn} \to M_{mn}$$
$$(AB)_{ij} = \sum_{k=1}^{s} (A)_{ik} \cdot (B)_{kj}, \quad 1 \leq i \leq m, \; 1 \leq j \leq n$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 & 4 & -1 \\ 2 & 3 & 0 & 4 \\ 3 & 6 & -1 & -1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1\cdot 0 + 2\cdot 2 + 3\cdot 3 & 1\cdot 1 + 2\cdot 3 + 3\cdot 6 & 1\cdot 4 + 2\cdot 0 + 3\cdot(-1) & 1\cdot(-1) + 2\cdot 4 + 3\cdot(-1) \\ 4\cdot 0 + 5\cdot 2 + 6\cdot 3 & 4\cdot 1 + 5\cdot 3 + 6\cdot 6 & 4\cdot 4 + 5\cdot 0 + 6\cdot(-1) & 4\cdot(-1) + 5\cdot 4 + 6\cdot(-1) \end{pmatrix} =$$

$$= \begin{pmatrix} 13 & 25 & 1 & 4 \\ 28 & 55 & 10 & 10 \end{pmatrix}$$

Proposizone

Se $A \in M_{ms},\ B \in M_{st},\ C \in M_{tn}$

$$(AB)C = A(BC)$$

Osservazione

Nel caso delle matrici quadrate M_n, il prodotto righe per colonne è un'operazione binaria associativa per la proprietà precedente che, per elemento neutro ha la **matrice identità**

$$I_n = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & ... & 1 & 0 \\ 0 & ... & 0 & 1 \end{pmatrix}$$

$(I_n)_{ij} = \delta_{ij}$ dove δ_{ij} è detta la **delta di Krnoecker** ed è definita come segue

$$\delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

ovvero vale 1 solamente nella **diagonale** e tutto il resto è 0.

Proposizione

$M_n(\mathbb{K})$ è un **anello con unità**.
N.B.: se $n \geq 2$, $M_n(\mathbb{K})$ **non è commutativo**

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 8 \\ -3 & 18 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 8 & 10 \end{pmatrix}$$

Esempi di gruppi

1. $(\mathbb{Z}, +),\ (\mathbb{Z}_n, +)$
2. $(\nu, +),\ \nu$ spazio vettoriale $(\nu = \mathbb{R},\ \mathbb{Q})$
3. S_n
4. $\mathbb{U}_n$ elementi invertibili in $\mathbb{Z}_n$
5. $(\mathbb{K} \setminus \{0\}, \cdot)$

Domanda

Abbiamo visto che M_n sono **un anello**; possiamo chiederci se $M_n \setminus \{0\}$ è un **gruppo** rispetto il **prodotto righe per colonne**. Questo è vero se per ogni $A \in M_n,\ A \neq 0\ \exists B \in M_n$ tale che

$$AB = BA = I_n \quad (*)$$

Questo in generale è **falso**. Dimostreremo che esiste una funzione detta **determinante**

$$\det : M_n(\mathbb{K}) \to \mathbb{K}$$

tale che

$$A \text{ è invertibile } \iff \det A \neq 0$$

cioè vale $(*)$. Quindi $\{A \in M_n(\mathbb{K}) : \det A \neq 0\}$ è un gruppo **infinito** (se $\mathbb{K}$ è infinito) **non abeliano** se $n \geq 2$.

Esempio:

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

Definizione - Sottogruppo

Sia G un **gruppo**. Diciamo che $\emptyset \neq H \subseteq G$ è un **sottogruppo** di G (notazione: $H \leq G$) se H è un **gruppo rispetto all'operazione indotta da G.**

$$\begin{tikzcd} G \times G \arrow[r] & G \\ H \times H \arrow[u, phantom, "\cup" rotate=90] \arrow[ur] \arrow[r] & H \arrow[u, phantom, "\cup" rotate=90] \end{tikzcd}$$

Osservazione: $H \leq G$ se e solo se

1. $\forall h_1, h_2 \in H \qquad h_1 \cdot h_2 \in H$
2. $e \in H$
3. $\forall h \in H,\ h^{-1} \in H$

Proposizione

$$H \leq G \iff ab^{-1} \in H, \quad \forall a, b \in H \ (*)$$

con questa scrittura sono state compattate le tre proprietà sopra.

Nota: in notazione additiva:

$$ab^{-1} \in H \text{ diventa } a - b \in H$$

Dimostrazione: Supponiamo che valgano *1. 2.* e *3.* e vediamo che vale $(*)$.

Dati $a, b \in H$, per la proprietà *3.* si ha $b^{-1} \in H$ e per la *1.* $ab^{-1} \in H$, quindi vale $(*)$.

Supponiamo che valga $(*)$, dobbiamo dimostrare *1. 2.* e *3.*

Prendiamo in $(*)$ $a = b$

$$ab^{-1} = aa^{-1} = e \in H$$

quindi vale *2.* Prendiamo in $(*)$ $a = e,\ b = h$. Abbiamo

$$e \cdot h^{-1} = h^{-1} \in H$$

quindi vale *3.* Infine prendiamo in $(*)$ $a = h_1,\ b = h_2^{-1}$

$$ab^{-1} = h_1(h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$$

quindi vale *1.*

Esempio: **il centro di un gruppo**. Sia G un gruppo. Definiamo

$$Z(G) = \{x \in G : xy = yx\ \forall y \in G\}$$

osserviamo che G è **abeliano** se e solo se $Z(G) = G$ (tutti gli elmenti in G commutano). In generale si ha $Z(G) \leq G$.

Verifichiamolo usando la proposizione precedente: $x, y \in Z(G) \Rightarrow xy^{-1} \in Z(G)$

- **Ipotesi**:

$$\begin{aligned} xg = gx \quad \forall g \in G\ (2) \\ yg = gy \quad \forall g \in G \end{aligned}$$

- **Tesi**: $xy^{-1}g = gxy^{-1} \quad \forall g \in G$

  $yg = gy$ può essere riscritta come

$$\begin{aligned} y^{-1}ygy^{-1} &= y^{-1}gyy^{-1} \qquad \text{moltiplico } y^{-1} \text{ a sx e dx} \\ gy^{-1} &= y^{-1}g\ (1) \end{aligned}$$

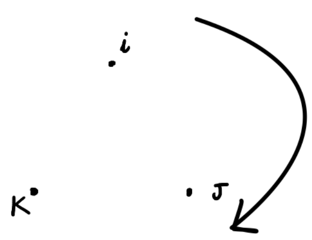
  Da cui si ricava

$$xy^{-1}g = x(y^{-1}g) \overset{(1)}{=} x(gy^{-1}) = (xg)y^{-1} \overset{(2)}{=} (gx)y^{-1} = gxy^{-1}$$

Esempio: Q **:** unità dei **quaternioni**

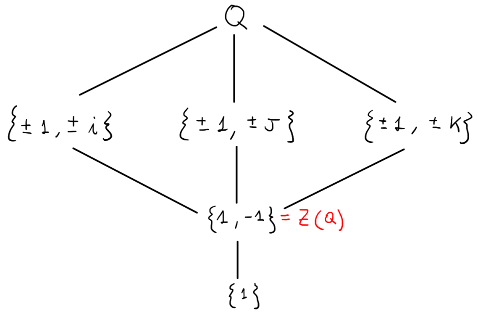
$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

Le regole moltiplicative seguono dal seguente disegno:



- $i^2 = j^2 = k^2 = -1$
- $ij = k \quad jk = i \quad ki = j$
- $ji = -k \quad kj = -i \quad ik = -j$

I **sottogruppi generati** sono i seguenti:



Sottogruppi di Z

<u>Proposizione</u>: i sottogruppi di $\mathbb{Z}$ sono tutti e soli del tipo $n\mathbb{Z}, \ n \in \mathbb{N}$.

<u>Dimostrazione</u>: vediamo prima di tutto che $n\mathbb{Z}$ è un sottogruppo. Per la proposizione dobbiamo vedere che se $x, y \in n\mathbb{Z}$, allora $x - y \in n\mathbb{Z}$ (ricordiamo che $\mathbb{Z}$ non + un gruppo rispetto alla moltiplicazione, quindi usiamo la notazione additiva).

Ma $x, y \in n\mathbb{Z}$ significa $x = na, \ y = nb$, per cui

$$x - y = na - nb = n(a - b) \in n\mathbb{Z}$$

Viceversa, sia $H \leq \mathbb{Z}$; se $H = \{0\}$ allora $H = n\mathbb{Z}$ con $n = 0$. Quindi possiamo supporre che esista $h \in H, n \neq 0$; poiché $H \leq \mathbb{Z}$, se $h \in H$, anche $-h \in H$, quindi posso supporre $h > 0$. Sia

$$\emptyset \neq H' = \{h \in H : h > 0\}$$

Quindi esiste $\overline{h} = \min H'$.

Dico che $H = \overline{h}\mathbb{Z}$. È chiaro che $\overline{h}\mathbb{Z} \subseteq H$, perchè $\overline{h} \in H$ e quindi tutti i multipli di $\overline{h}$ appartengono ad H ($H \leq \mathbb{Z}$).

Viceversa, prendo $x \in H$ e scrivo

$$x = q\overline{h} + r \qquad 0 \leq r < h$$

quindi $r = x - q\overline{h}$ e sappiamo che $x \in H$ per ipotesi. Dunque $r \in H$, ma $\overline{h}$ è il **minimo intero positivo** che appartiene ad H, quindi $r = 0$ e quindi

$$x = q\overline{h} \in \overline{h}\mathbb{Z}$$

come volevamo.

Omomorfismo

Siano $G_1, \ G_2$ gruppi. Un **omomorfismo** tra G_1 e G_2 è un'applicazione

$$f : G_1 \to G_2$$

tale che $f(gg') = f(g)f(g'), \ \forall g, g' \in G_1$.

Un **isomorfismo**

$$f : G_1 \to G_2$$

è un **omomorfismo biunivoco**.

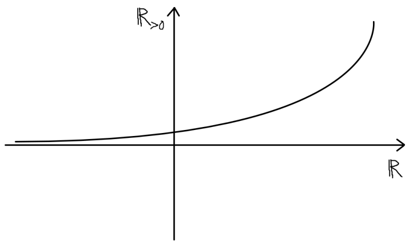
Esempio:

$$f : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$$
$$x \mapsto e^x$$

è un **isomorfismo** in quanto

$$f(x+y) = f(x)f(y)$$
$$e^{x+y} = e^x e^y$$

La **biunivocità** segue dal grafico dell'esponenziale



Lezione 13 - 28/10/2022

Notazione - definizione

Sia G un **gruppo** e $g \in G$. Definiamo le **potenze** come segue

$$g^i = \begin{cases} g^{i-1} \cdot g & \text{se } i > 0 \\ e & \text{se } i = 0 \\ (g^{-1})^{-i-1} \cdot g^{-1} & \text{se } i < 0 \end{cases}$$

Nota: è una definizione induttiva

Osservazione: in notazione additiva si ha

$$\begin{gathered} g^i \rightarrow ig \\ g^{-i} \rightarrow -ig \end{gathered}$$

> ⚠️ Fare la **potenza** di un elemento x di un gruppo G equivale ad **iterare** a partire da x o da x^{-1} l'operazione del gruppo.

Proposizione

Se H, K sono **sottogruppi** di un gruppo G, anche $H \cap K$ lo è.
Dimostrazione: Per ipotesi

$$\begin{aligned} h_1 h_2^{-1} \in H \quad \forall h_1, h_2 \in H \ (1) \\ k_1 k_2^{-1} \in K \quad \forall k_1, k_2 \in K \ (2) \end{aligned}$$

Siano ora $x,\ y$ elementi qualsiasi di $H \cap K$. Devo dimostrare che

$$xy^{-1} \in H \cap K$$

ma se $x, y \in H \cap K$, in particolare $x, y \in H$ quindi per (1) $xy^{-1} \in H$ e $x, y \in K$, quindi per (2) $xy^{-1} \in K$. Dunque $xy^{-1} \in H \cap K$.

Osservazione: L'enunciato vale per una qualsiasi **famiglia di sottogruppi** di G

$$\alpha \in A \quad H_\alpha \leq G \Longleftrightarrow \bigcap_{\alpha \in A} H_\alpha \leq G$$

Definizione - Sottogruppo generato

Sia G un **gruppo** e $X \leq G$. Si definisce **sottogruppo generato da X** l'insieme

$$< X >= \bigcap_{X \subseteq H \leq G} H$$

Caso speciale (importante): $X = \{g\}$ allora

$$< g >= \{g^i : i \in \mathbb{Z}\}$$

e prende il nome di **sottogruppo ciclico generato da g.**

Proposizione

Sia $X = \{x_1, x_2, ...\} \leq G$. Allora

$$< x >= \{t_1 \cdot ... \cdot t_r : r \in \mathbb{N},\ t_i \in X \text{ oppure } t_i^{-1} \in X\}$$

Idea: per generare un gruppo a partire dagli elementi di X devo prendere **tutti i possibili prodotti di elementi di X e dei loro inversi**.

Esempio: in $\mathbb{Z}$

$$< 2, 3 >= \{2s + 3t : s, t \in \mathbb{Z}\} = \mathbb{Z}$$

Definizione - Gruppo ciclico

Un **gruppo** G si dice **ciclico** se $\exists g \in G : G =< g >$.

Esempi:

1. $(\mathbb{Z}, +)$ è **ciclico**, generato da 1

$$n = n \cdot 1$$

Nota: anche -1 genera $\mathbb{Z}$ e **nessun altro intero** lo genera.

2. $(\mathbb{Z}_n, +)$ è ciclico, generato da $\bar{1}$

$$\bar{n} = n \cdot \bar{1}$$

Dimostreremo che $\mathbb{Z}_n$ ha $\phi(n)$ generatori.

Esempio:

- $\mathbb{Z}_6$ ha $\phi(6) = \phi(3)\phi(2) = 2$ generatori
- $\mathbb{Z}_8$ ha $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ generatori. Verifica:

$$\begin{aligned}
&< \bar{0} > = \{\bar{0}\} \\
&< \bar{1} > = \mathbb{Z}_8 \\
&< \bar{2} > = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\} \\
&< \bar{3} > = \{\underbrace{\bar{3}, \bar{6}}_{+3}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{0}\} = \mathbb{Z}_8 \\
&< \bar{4} > = \{\bar{4}, \bar{0}\} \\
&< \bar{5} > = \{\underbrace{\bar{5}, \bar{2}}_{+5}, \bar{7}, \bar{4}, \bar{1}, \bar{6}, \bar{4}, \bar{0}\} = \mathbb{Z}_8 \\
&< \bar{6} > = \{\bar{6}, \bar{4}, \bar{2}, \bar{0}\} \\
&< \bar{7} > = \{\bar{7}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0}\} = \mathbb{Z}_8
\end{aligned}$$

3. $(\mathbb{R} \setminus \{0\}, \cdot) \geq \{\pm 1\} \cong \mathbb{Z}_2$ ($\cong$ è il simbolo che indica un **isomorfismo**). Sia

$$\begin{aligned}
\phi : \{\pm 1\} &\to \mathbb{Z}_2 \\
1 &\mapsto \bar{0} \\
-1 &\mapsto \bar{1}
\end{aligned}$$

Si ha che

$$\phi(1 \cdot 1) = \phi(1) + \phi(1) = \bar{0} + \bar{0}$$
$$\phi(1 \cdot (-1)) = \phi(1) + \phi(-1) = \bar{0} + \bar{1} = \bar{1}$$
$$\phi((-1) \cdot (-1)) = \phi(-1) + \phi(-1) = \bar{1} + \bar{1} = \bar{0}$$

Definzione - Ordine

L'**ordine** di $g \in G$, denotato con $o(g)$, è il **minimo intero positivo**, se esiste, tale che

$$g^n = e$$

se tale n **non esiste**, si pone $o(g) = +\infty$.

Osservazione: in altri termini

$$o(g) = | < g > |$$

in particolare G è **ciclico se e solo se esiste** $g \in G$, con $o(g) = |G|$

Osservazione: se G è **ciclico**, allora è **abeliano**. Infatti, se $G =< g >,\ x, y \in G$

$$x = g^i,\ y = g^j$$
$$xy = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = yx$$

Il viceversa **non è vero**.

Esempio: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$

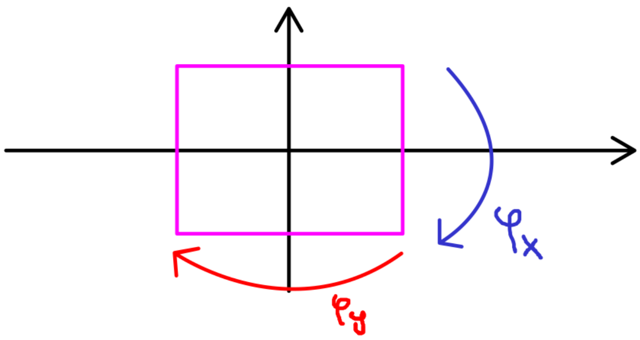
$$< (\bar{0}, \bar{0}) > = \{(\bar{0}, \bar{0})\}$$
$$< (\bar{1}, \bar{0}) > = \{(\bar{1}, \bar{0}), (\bar{0}, \bar{0})\}$$
$$< (\bar{0}, \bar{1}) > = \{(\bar{0}, \bar{1}), (\bar{0}, \bar{0})\}$$
$$< (\bar{1}, \bar{1}) > = \{(\bar{1}, \bar{1}), (\bar{0}, \bar{0})\}$$

Quindi tutti gli elmento diversi da $e = \{(\bar{0}, \bar{0})\}$ hanno ordine 2, quindi nessuno di essi ha ordine 4 e quindi il **gruppo non è ciclico**.

Il gruppo è chiaramente **abeliano**, ma **non è ciclico**.

Nota

Il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ è **isomorfo** al cosiddetto **gruppo di Klein**, delle **simmetrie di un rettangolo** con non è un quadrato:



$$V = \{Id, \phi_x, \phi_y, \phi_o\}$$
$$\phi_x(x, y) = (x, -y)$$
$$\phi_y(x, y) = (-x, y)$$
$$\phi_o(x, y) = (-x, -y)$$

Osservazione: abbiamo due gruppi di ordine 4 **non isomorfi** $\mathbb{Z}_4$ e V: il primo è **ciclico** mentre il secondo **non è ciclico**.

Proposizione

Sia G un **gruppo** e $g \in G$. Se $o(g) = +\infty$, allora $g^h \neq g^k$ per $h \neq k$. Se invece $o(g) = n$ allora

$$< g >= \{e, g, ..., g^{n-1}\}$$

e $g^h = g^k$ sse $h \equiv k \mod n$.

Dimostrazione: Supponiamo $o(g) = +\infty$ e $g^h = g^k$. Allora

$$g^{h-k} = e \Rightarrow h - k = 0 \Rightarrow h = k$$

Se $o(g) = n$, per definizione $e, g, ..., g^{n-1}$ sono **elementi distinti del sottogruppo** $< g >$ (se fosse $g^i = g^j, \ 1 \leq i \leq j < n$ avremmo $g^{i-j} = e$ con $i - j < n$ contro la definzione di $o(g)$).

Dunque basta vedere che ogni potenza di g è nella lista $\{e, g, ..., g^{n-1}\}$.

Consideriamo $g^s, \ s \in \mathbb{Z}$; $s = qn + r \quad 0 \leq r < n$

$$g^s = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e^q g^r = eg^r = g^r \quad 0 \leq r \leq n - 1$$

Supponiamo ora $g^h = g^k$

$$g^{h-k} = e \qquad h-k = q'n + r' \quad 0 \le r' \le n-1$$
$$g^{h-k} = g^{q'n+r'} = g^{r'} \Rightarrow r' = 0$$

ovvero $h-k = q'n$ ovvero $h \equiv k \mod n$.

Viceversa, $h \equiv k \mod n, \ h = k + tn$

$$g^h = g^{k+tn} = g^k g^{tn} = g^k (g^n)^t = g^k e^t = g^k e = g^k$$

Lezione 14 - 03/11/2022

Reminescenze gruppo ciclico

Ricordiamo che un gruppo G si dice ciclico se $\exists g \in G : G =< g >$.

<u>Esempi</u>:

1. $\mathbb{Z} =< 1 >$
2. $\mathbb{Z}_n =< \bar{1} >$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico

<u>Osservazione</u>: G ciclico $\Rightarrow G$ abeliano, ma non è vero il viceversa (come nell'esempio 3.).

Proposizione 1

Ogni sottogruppo di un gruppo ciclico G è **ciclico**.

<u>Dimostrazione</u>: sia $G =< g >$ e $H \leq G$.

Se $H = \{e\}$, allora $H =< e >$ quindi è **ciclico**.

Supponiamo $H \neq \{e\}$, quindi esiste $g^i \in H, i \neq 0$. Siccome $H \leq G$, se $g^i \in H$ anche $g^{-i} \in H$. Pertanto $\{i \in \mathbb{N} : g^i \in H\} \neq \emptyset$ e quindi **ammette minimo**, chiamiamolo m.

Dico che $H =< g^m >$. Poichè $g^m \in H$, $g^{km} \in H \; \forall k \in \mathbb{Z}$ (perché $H \leq G$), quindi $< g^m > \subseteq H$. Devo dimostrare l'inclusione contraria.

Sia $g^t \in H$

$$\begin{gathered} t = qm + r, \quad 0 \leq r < m \\ g^t = g^{qm+r} = g^{qm} g^r \\ g^r = g^t g^{-qm} \in H \end{gathered}$$

Per la **minimalità di** m segue che $r = 0$. Dunque $t = qm$ e quindi $g^t \in < g^m >$, che è quanto volevamo.

Proposizione 2

Sia $G =< g >$ un **gruppo ciclico finto** di ordine n. Allora

a. $H \leq G, \; |H| \mid n$ (la cardinalità di H divide n)
b. Se $k \mid |G|$, esiste **un unico** $H \leq G, \; |H| = k$

Dimostrazione a.: Sia $H \leq G$; per la $\text{prop } 1.$ $H =< g^m >$;

$$(g^m)^n = (g^n)^m = e^m = e$$

quindi $o(g^m) \mid n$, dove $g^m = |H|$ e $n = |G|$ (in generle se $g^k = e \Rightarrow o(g) \mid k$).

Dimostrazione b.: Sia $k \mid n$; allora $| < g^{\frac{n}{k}} > | = k$.

Facciamo vedere che $< g^{\frac{n}{k}} >$ è l'**unico** sottogruppo di ordine k. Sia H un altro tale sottogruppo; $H =< g^h >$ dove h è il **minimo intero positivo** tale che $g^h \in H$

$$|H| = k = | < g^h > | = \frac{n}{h}$$

dunque $h = \frac{n}{k}$ e $H =< g^{\frac{n}{k}} >$.

Proposizione: Se $g \in G$ ha ordine finito n, allora

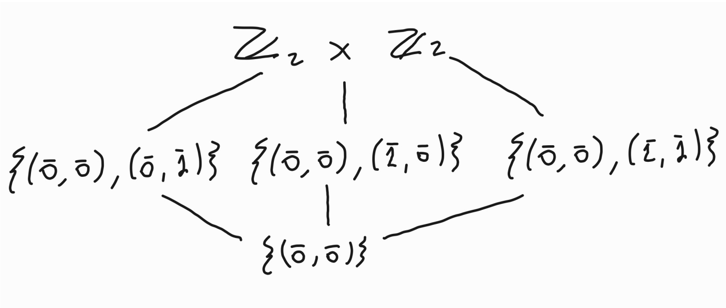
$$o(g^k) = \frac{n}{(n,k)}$$

Corollario delle prop 1. e 2.: Il **reticolo dei sottogruppi** di un gruppo cicliclo di ordine n è **isomorfo al reticolo dei divisori di** n.

Esempio: POSET dei sottogruppi di un gruppo:

$$H_1, H_2 \leq G \qquad H_1 \preccurlyeq H_2 \Leftrightarrow H_1 \subseteq H_2$$

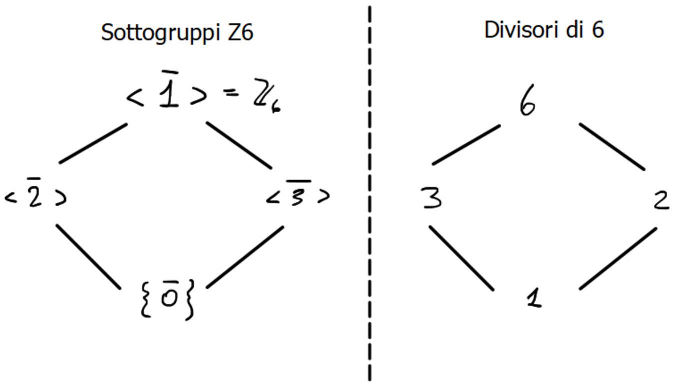
- $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{1})\}$



$\mathbb{Z}_6 =< \bar{1} >$

Abbiamo visto che il sottogruppo di ordine k è generato da $g^{\frac{n}{k}}$

$$\begin{array}{llll} n & k & & \\ 6 & 6 & \bar{1} & \\ & 3 & \bar{2} & < \bar{2} >= \{\bar{2},\bar{4},\bar{0}\} \\ & 2 & \bar{3} & < \bar{3} >= \{\bar{3},\bar{0}\} \\ & 1 & \bar{0} & \end{array}$$



Proposizione 3

Sia $G =< g >$ un **gruppo ciclico** di ordine n. Allora $< g^i >$ genera G se e solo se $(i,n) = 1$.

<u>Dimostrazione</u>: g^i genera G se e solo se $o(g^i) = n$

$$n = o(g^i) = \frac{n}{(n,i)} \iff (n,i) = 1$$

Gruppo simmetrico

$$S_n = \{f : \{1,...,n\} \to \{1,...,n\} | f \text{ è biunivoca}\}$$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Per scrivere le permutazioni in modo più conveniente, introduciamo, fissata $\sigma \in S_n$, una **relazione di equivalenza** su $\{1, ..., n\}$

$$i \equiv_\sigma j \iff \exists k \in \mathbb{Z} : i = \sigma^k(j)$$

<u>Esempio</u>:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 3 & 2 & 5 & 4 & 7 & 9 & 8 & 6 & 1 \end{pmatrix}$$

$$\begin{aligned} &1 \equiv_\sigma 10 \\ &2 \equiv_\sigma 3 \\ &4 \equiv_\sigma 5 \\ &6 \equiv_\sigma 7 \equiv_\sigma 9 \\ &8 \equiv_\sigma 8 \end{aligned}$$

quindi si ha che

$$\sigma = (1, 10)(2, 3)(4, 5)(6, 7, 9)$$

Tale rappresentazione viene chiamata **rappresentazione in cicli disgiunti.**

> ⚠️ Gli elementi in σ che restano fissati, come in questo caso l'8, non vengono riportati nella rappresentazione in cicli disgiunti.

Verifichiamo ora che $\equiv_\sigma$ è di equivlenza:

- **Riflessiva**: $i \equiv_\sigma i$ ovvio perché $i = \sigma^0(i)$
- **Simmetrica**: $i \equiv_\sigma j \Rightarrow j \equiv_\sigma i$. Vera in quanto $\exists k : i \in \sigma^k(j)$ e $j = \sigma^{-k}(i)$.
- **Transitiva**: $i \equiv_\sigma j,\ j \equiv_\sigma k \Rightarrow i \equiv_\sigma k$.

$$\begin{gathered} \exists t : i = \sigma^t(j) \\ \exists s : j = \sigma^s(k) \\ i = \sigma^t(j) = \sigma^t(\sigma^s(k)) = \sigma^{t+s}(k) \end{gathered}$$

  quindi $i \equiv_\sigma k$.

Definizione

Data $\sigma \in S_n$, un **ciclo** di σ è l'insieme ordinato

$$(x, \sigma(x), \sigma^2(x), ..., \sigma^{m-1}(x))$$

due cicli si dicono **disgiunti** se lo sono come insiemi.

Osservazione: possiamo interpretare un ciclo come la permutazione

$$x \mapsto \sigma(x), \sigma(x) \mapsto \sigma^2(x), ..., \sigma^{m-1}(x) \mapsto x$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 2 & 7 & 1 & 4 \end{pmatrix} = (1,8,3,6,7)(2,5)$$

Esempio: trasformazione di cicli non disgiunti in cicli disgiunti

$$(1,2,3,4)(2,6,4,8)(8,7,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 3 & 8 & 5 & 1 & 4 & 7 \end{pmatrix} = (1,2,6)(4,8,7)$$

Procediemento:

- Inizio dall'1 e lo faccio scorrere attraverso i vari cicli (non disgiunti) da **destra verso sinistra** e vedo dove va a finire:
  1. Nel ciclo $(8,7,3)$ l'1 non viene mappato da nessuna parte;
  2. Nel ciclo $(2,6,4,8)$ l'1 non viene mappato da nessuna parte;
  3. Nel ciclo $(1,2,3,4)$ l'1 viene mappato in 2, i cicli sono finiti e quindi nella permutazione avremo $\sigma(1) = 2$.
- Passo al 2 e faccio lo stesso procedimento:
  1. Nel ciclo $(8,7,3)$ il 2 non viene mappato da nessuna parte;
  2. Nel ciclo $(2,6,4,8)$ il 2 viene mappato in 6, quindi ora nel prossimo ciclo dovrò controllare il 6 dove verrà mappato;
  3. Nel ciclo $(1,2,3,4)$ il 6 non viene mappato da nessuna parte, i cicli sono finiti e quindi avremo $\sigma(2) = 6$.
- Passo al 3:
  1. Nel ciclo $(8,7,3)$ il 3 viene mappato in 8;
  2. Nel cilclo $(2,6,4,8)$ l'8 viene mappato in 2;

3. Nel ciclo $(1, 2, 3, 4)$ il 2 viene mappato in 3, quindi $\sigma(3) = 3$.

- …

Infine vengono scritti i cicli disgiunti partendo dalla permutazione ottenuta.

Proposizione - Permutazione prodotto di cicli

Ogni permutazione è **prodotto dei suoi cicli**.

Dimostrazione: sia $\sigma \in S_n$ e siano $\gamma_1, ..., \gamma_k$ i suoi cicli. Poiché $\equiv_\sigma$ è una **relazione di equivalenza**, pensando i cilci come **insiemi** si ha

$$\bigcup_{i=1}^{k} \gamma i = \{1, ..., n\} \quad \gamma_i \cap \gamma_j = \emptyset, \ i \neq j$$

Dobbiamo far vedere che se penso $\gamma_1, ..., \gamma_k$ come **permutazioni** allora $\sigma = \gamma_1, ..., \gamma_k$, ovvero

$$\sigma(x) = (\gamma_1, ..., \gamma_k)(x) \; \forall x \in \{1, ..., n\}$$

Ora, ogni $x \in \{1, ..., n\}$ compare in **uno solo** dei cicli $\gamma_1, ..., \gamma_k$. Sia questo ciclo $\gamma_i = (x, \sigma(x), ..., \sigma^{m-1}(x))$. Per ogni $j \neq i$ e per ogni $y = \sigma^h(x)$ (ovvero per ogni y che compare nella scrittura di γ_i) risulta

$$\gamma_i(y) = y$$

dunque, $\forall x \in \{1, ..., n\}$

$$(\gamma_1, ..., \gamma_k)(x) = (\gamma_1, ..., \gamma_i)(x) = \gamma_1 ..., \gamma_{i-1}(\sigma(x)) = \sigma(x)$$

quindi $\sigma = \gamma_1, \gamma_2, ..., \gamma_k$.

Proposizione - Ordine di una permutazione

Se $\sigma = \gamma_1 ... \gamma_k$ è la **decomposizione in cicli disgiunti** di σ e γ_i ha lunghezza m_i, allora

$$o(\sigma) = \mathrm{m.c.m}\{m_1, ..., m_k\}$$

Dimostrazione: Ovvio dalla **definizione di ordine** e dal fatto che i cicli disgiunti **commutano**. Sia m_i l'ordine dell'i-esimo ciclo e $S = \mathrm{m.c.m}(m_1, ..., m_k)$ si ha che

$$\sigma^S = (\gamma_1, ..., \gamma_k)^S = \gamma_1^S ... \gamma_k^S$$

Esempi:

1. Calcolare l'ordine di

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$$

   Riportiamo σ in notazione in cicli disgiunti:

$$\sigma = (1, 2, 3)(4, 5, 6, 8)$$

   quindi $o(\sigma) = \mathrm{m.c.m}(3, 4) = 12$.

2. Calcolare l'ordine di

$$\sigma = (1, 2, 3)(2, 3, 4)(3, 4, 5)$$

   Attenzione: non è 3 in quanto i cicli **non sono disgiunti**! Riportiamo σ in notazione in cilci disgiunti:

$$\sigma = (1, 2)(4, 5)$$

   quindi $o(\sigma) = \mathrm{m.c.m}(2, 2) = 2$.

Notazione

I cicli di lunghezza m vengono chiamati m-cicli. I cicli di lunghezza 2 vengono chiamati **trasposizioni**.

Porposizione- Ciclo prodotto di trasposizioni

Ogni **ciclo** è **prodotto di trasposizioni**. In particolare, S_n è generato dalle trasposizioni.

Dimostrazione: ogni ciclo si può scrivere come prodotto di trasposizioni, ad esempio

$$(1, 2, ..., n) = (1, n)(1, n-1)(1, n-2)...(1, 3)(1, 2)$$

Ora **ogni permutazione è prodotto di cicli** e **ogni ciclo è prodotto di trasposizioni**, quindi **ogni permutazione è prodotto di trasposizioni**.

Osservazione: La scrittura come prodotto di trasposizioni non è unica

$$(1, 3) = (1, 2)(2, 3)(1, 2) = (2, 3)(1, 2)(2, 3)$$

Teorema

Se $\sigma = \tau_1...\tau_k = \tau'_1...\tau'_h$ con τ_i, τ'_j trasposizioni, allora $h \equiv k \mod z$.

Definizione - Parità delle permutazioni

Diciamo che σ è **pari** se si scrive come **prodotto di un numero pari di trasposizioni**, **dispari** altrimenti.

Esercizio: determinare ordine e parità della seguente permutazione

$$\sigma = (1,4,7,8)(2,9,7,6)(4,3,1,7)(2,9,5)$$

riportiamola in notazione in cicli disgiunti

$$\sigma = (1,6,2,8)(3,4)(5,9) \quad (*)$$

da cui deduciamo che $o(\sigma) = \text{m.c.m}(4,2,2) = 4$. Ora riportiamo i cicli disgiunti in prodotti di trasposizioni:

$$\sigma = (1,8)(1,2)(1,6)(3,4)(5,9)$$

da cui deduciamo che è **dispari**.

Definizione - Partizione di un numero naturale

Una **partizione** di $n \in \mathbb{N}$ è una sequenza di interi $\lambda_1 \geq ... \geq \lambda_k \geq 1$ tali che

$$\sum_{i=1}^{k} \lambda_i = n$$

Chiamiamo con $p(n)$ il **numero di partizioni** di n. Si ha che

$$\begin{array}{llllllll}
p(1) = 1 \\
p(2) = 2 & 2 & 11 \\
p(3) = 3 & 3 & 21 & 111 \\
p(4) = 5 & 4 & 31 & 22 & 211 & 1111 \\
p(5) = 7 & 5 & 41 & 32 & 311 & 221 & 2111 & 11111
\end{array}$$

Definizione - Struttura ciclica di una permutazione

Osserviamo che una permutazione di S_n individua, tramite la **decomposizione in cicli disgiunti**, una partizione di n che è detta **struttura ciclica** della permutazione.

La **struttura ciclica** della σ precedente $(*)$ è: 4221.

Esempio: $p(5) = 7$

		ordine	parità
5	$(1,2,3,4,5)$	5	p
41	$(1,2,3,4)$	4	d
32	$(1,2,3)(4,5)$	6	d
311	$(1,2,3)$	3	p
221	$(1,2)(3,4)$	2	p
2111	$(1,2)$	2	d
11111	id	1	p

Relazione coniugio

Ricordiamo che in un gruppo qualsiasi due elementi g_1, g_2 si dicono **coniugati** se esiste $g_3 \in G$:

$$g_1 = g_3 g_2 g_3^{-1}$$

Teorema

$\sigma, \tau \in S_n$ sono **coniugate** se e solo se hanno la **stessa struttura ciclica**.

Idea della dimostrazione: $\tau\sigma\tau^{-1}$ si ottiene dalla decomposizione in cicli disgiunti di σ sostituendo ad a la cifra $\tau(a)$.

$$\sigma = (a, b, c, d)(e, f)(g, h)$$
$$\tau\sigma\tau^{-1} = (\tau(a), \tau(b), \tau(c), \tau(d))(\tau(e), \tau(f))(\tau(g), \tau(h))$$

Esempio:

$$\sigma = (1,2,3,4)(5,6)(7,8)$$
$$\sigma' = (2,4,6,8)(7,1)(3,5)$$

⚠️ Notare che σ e σ' hanno la **stessa struttura ciclica**: 422

una permutazione τ che **conigua** σ in σ' è

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 1 & 3 & 5 \end{pmatrix}$$

in quanto $\tau\sigma\tau^{-1} = \sigma'$:

$$\begin{aligned} \tau\sigma\tau^{1} &= (1,7)(2,4,6,8)(3,5) = \\ &= (2,4,6,8)(7,1)(3,5) = \sigma' \end{aligned}$$

⚠️ Ricordiamo che per risolvere questo tipo di esercizio si procede applicando le permutazioni da **destra verso sinistra**, quindi prima applico τ^{-1} e vedo dove viene mappato ogni elemento che man mano viene scelto, poi applico σ ed infine τ.
Ricordiamo inoltre che τ^{-1} vuol dire **leggere la permutazione al contrario**, quindi ogni elemento all'interno di un ciclo viene mappato in quello che si trova alla sua sinistra e non destra.

Lezione 15 - 04/11/2022

Osservazione - Il sottogruppo alterno

La mappa $\epsilon : S_n \to \{\pm 1\}$ definita come

$$\epsilon(\sigma) = \begin{cases} 1 & \sigma \text{ è pari} \\ -1 & \sigma \text{ è dispari} \end{cases}$$

è un **omomorfismo** di gruppi; questo è equivalente a dire che il **prodotto** di due permutaizioni pari **è pari** così come il prodotto di una permutazione pari ed una dispari e il prodotto di una permutazione dispari ed una pari **è dispari**. A sua volta questo segue dalle definizioni.

Esempio:

$$\sigma = \tau_1 ... \tau_6 \qquad \sigma' = \tau_1' ... \tau_8' \qquad \tau_i, \tau_j' \text{ trasposizioni}$$
$$\sigma\tau = \underbrace{\tau_1 ... \tau_6 \tau_1' ... \tau_8'}_{14 \text{ trasposizioni}}$$

In particolare

$$A_n = \{\sigma \in S_n : \sigma \text{ è pari}\}$$

è un sottogruppo di S_n e prende il nome di **sottogruppo alterno**.

Lemma - Cardinalità del sottogruppo alterno

$|A_n| = \dfrac{n!}{2}$ (ovvero sono metà pari e metà dispari)

Dimostrazione: basta costruire una **corrispondenza biunivoca**

$$\Phi : A_n \to \{\sigma \in S_n | \sigma \text{ è dispari}\}$$

Questo conclude perché se $a = |A_n|$

$$n! = a + |\{\sigma \in S_n : \sigma \text{ è dispari}\}| = 2a \implies a = \frac{n!}{2}$$

Sia τ una permutazione **dispari fissata**

$$\Phi(\sigma) = \sigma\tau$$

$\Phi(\sigma)$ è dispri, perchè σ è pari, quindi Φ è effettivamente un'applicazione

$$A_n \to \{\sigma \in S_n : \sigma \text{ è dispari}\}$$

- Φ è **iniettiva**:

$$\begin{gathered}\Phi(\sigma) = \Phi(\sigma') \\ \sigma\tau = \sigma'\tau \\ \sigma\tau\tau^{-1} = \sigma'\tau\tau^{-1} \\ \sigma = \sigma'\end{gathered}$$

- Φ è **suriettiva**: $\alpha \in S_n$ dispari, $\alpha\tau^{-1} \in A_n$ e

$$\Phi(\alpha\tau^{-1}) = \alpha\tau^{-1}\tau = \alpha$$

Esercizio sulla relazione coniugio

Siano $\sigma = (1, 5)(2, 3, 4)$ e $\tau = (1, 4, 3)(2, 6, 7, 5)$

$$\tau\sigma\tau^{-1} = (\tau(1), \tau(1))(\tau(2), \tau(3), \tau(4)) = (4, 2)(6, 1, 3)$$

derivata nel seguente modo

$$\begin{aligned}\tau\sigma\tau^{-1}: &1 \to 3 \to 4 \to 3\\ &2 \to 5 \to 1 \to 4\\ &3 \to 4 \to 2 \to 6\\ &4 \to 1 \to 5 \to 2\\ &5 \to 7 \to 7 \to 5\\ &6 \to 2 \to 3 \to 1\\ &7 \to 6 \to 6 \to 7\end{aligned}$$

Calcolare τ tale che $\tau\sigma\tau^{-1} = \mu$ dove

$$\sigma = (1,2,3)(4,7,8)$$
$$\tau = (3,4,9)(5,2,1)$$

$$\begin{aligned}\tau\sigma\tau^{-1} &= (\tau(1),\tau(2),\tau(3))(\tau(4),\tau(7),\tau(8)) =\\ &= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 4 & 9 & 5 & 6 & 7 & 2 & 1 & 8\end{pmatrix}\end{aligned}$$

ℹ️ In quanto in σ non sono presenti $5, 6$ e 9, in $\tau\sigma\tau^{-1}$ possono essere messi uno dei valori rimanenti a caso.

Lemma - Gli r-cicli di Sn

In S_n gli r-cicli sono

$$\frac{1}{r} \cdot \frac{n!}{(n-r)!}$$

Dimostrazione: Il **primo numero** del ciclo lo posso scegliere in n modi, **il secondo** in $n-1$, il terzo in $n-2$ .... l'r**-esimo** in $n-r+1$ modi. In totale

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

Però ognuno dei cicli ottenuti in questo modo viene **contato** r **volte** (ci sono ripetizioni):

$$(1,2,...,r) = (2,3,...,r,1) = (3,4,...,r,1,2)....$$

Ad esempio in S_n ci sono $\binom{n}{2}$ trasposizioni.

Classi laterali e teorema di Lagrange

Sia G un gruppo e $H \leq G$; definiamo **due relazioni di equivalenza** ρ_d, ρ_s su G:

$$a\rho_d b \iff ab^{-1} \in H$$
$$a\rho_s b \iff b^{-1}a \in H$$

1. ρ_d, ρ_s sono relazioni di equivalenza
   - **Riflessiva**: $a\rho_d a \qquad aa^{-1} \in H \qquad e \in H$
   - **Simmetrica**: $a\rho_d b \Rightarrow b\rho_d a$

   $$ab^{-1} \in H \qquad (ab^{-1})^{-1} \in H$$
   $$(ab^{-1})^{-1} = ba^{-1} \Leftrightarrow b\rho_d a$$

   - **Transitiva**: $a\rho_d b,\ b\rho_d c \Rightarrow a\rho_d c$. Si ha che $ab^{-1} \in H$ e $bc^{-1} \in H$ e si ha che $H \leq G$.

   $$(ab^{-1})(bc^{-1}) \in H$$
   $$(ab^{-1})(bc^{-1}) = abb^{-1}c^{-1} = ac^{-1} \Leftrightarrow a\rho_d c$$

2. $\rho_d = \rho_s$ se G è **abeliano**.
3. <u>Esempio</u>: $G = \mathbb{Z}$ e $H = n\mathbb{Z}$. Sia $\rho = \rho_d = \rho_s$

   $$a\rho b \Leftrightarrow ab^{-1} \in H \rightarrow a - b \in n\mathbb{Z}$$

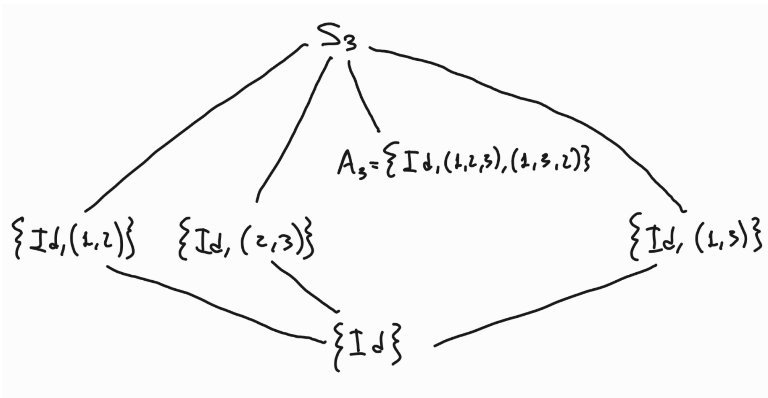
   che implica che ρ è precisamente la **congruenza mod n**.
4. Struttura delle **classi di equivalenza**
   - Classe **laterale destra** di $a \bmod H$

   $$\begin{aligned}\{b \in G : b\rho_d a\} &= \{b \in G : ba^{-1} \in H\} \\ &= \{b \in G : ba^{-1} = h \text{ per qualche } h \in H\} \\ &= \{b \in G : b = ha \text{ per qualche } h \in H\} \\ &= Ha \leftarrow \text{classe laterale destra di } a \bmod H\end{aligned}$$

   - Classe **laterale sinistra** di $a \bmod H$

$$\begin{aligned}
\{b \in G : b\rho_s a\} &= \{b \in G : a^{-1}b \in H\} \\
&= \{b \in G : a^{-1}b = h \text{ per qualche } h \in H\} \\
&= \{b \in G : b = ah \text{ per qualche } h \in H\} \\
&= aH \leftarrow \text{classe laterale sinistra di } a \bmod H
\end{aligned}$$

Esempio: $S_3 = \{Id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$



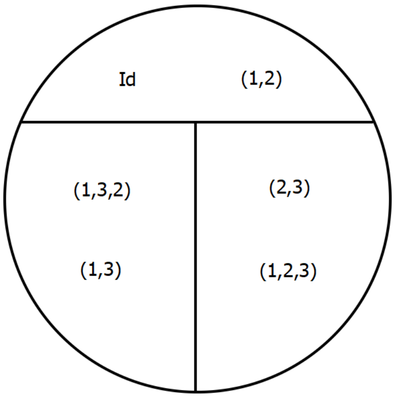
Poniamo $H = \{Id, (1,2)\}$ e troviamo le **classi laterali destre** e **sinistre** di $S_3 \bmod H$:

$$\begin{aligned}
HId &= H \\
H(1,2) &= \{Id \cdot (1,2), (1,2)(1,2)\} = \{(1,2), Id\} = H \\
H(2,3) &= \{Id \cdot (2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\} \\
H(1,3) &= \{Id \cdot (1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\} \\
H(1,2,3) &= \{Id \cdot (1,2,3), (1,2)(1,2,3)\} = \{(1,2,3), (2,3)\} \\
H(1,3,2) &= \{Id \cdot (1,3,2), (1,2)(1,3,2)\} = \{(1,3,2), (1,3)\}
\end{aligned}$$

Quindi si ha che

- $H = H(1,2)$
- $H(2,3) = H(1,2,3)$
- $H(1,3) = H(1,3,2)$

Che formano la seguente **partizione** di S_3:



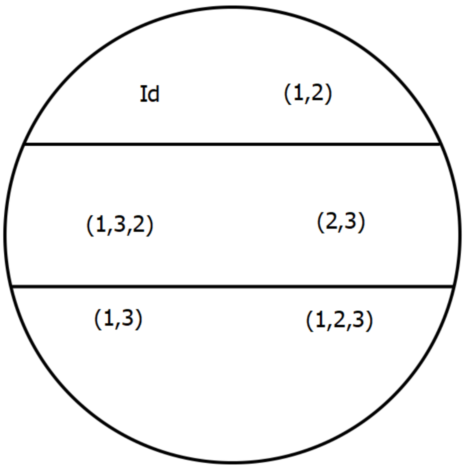
Passiamo ora alle **classi laterali sinistre**:

$$\begin{aligned} IdH &= H \\ (1,2)H &= \{(1,2)\cdot Id, (1,2)(1,2)\} = H \\ (2,3)H &= \{(2,3)\cdot Id, (2,3)(1,2)\} = \{(2,3),(1,3,2)\} \\ (1,3)H &= \{(1,3)\cdot Id, (1,3)(1,2)\} = \{(1,3),(1,2,3)\} \\ (1,2,3)H &= \{(1,2,3)\cdot Id, (1,2,3)(1,2)\} = \{(1,2,3),(1,3)\} \\ (1,3,2)H &= \{(1,3,2)\cdot Id, (1,3,2)(1,2)\} = \{(1,3,2),(2,3)\} \end{aligned}$$

Quindi si ha che

- $(1,2)H = H$
- $(2,3)H = (1,3,2)H$
- $(1,3)H = (1,2,3)H$

Che formano la seguente **partizione** di S_3:



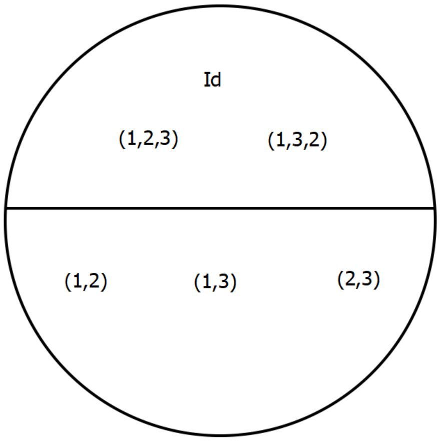
Sia ora $H = \{Id, (1,2,3), (1,3,2)\}$. Poichè H è un sottogruppo

$$H = H(1,2,3) = H(1,3,2) = (1,2,3)H = (1,3,2)H$$

Calcoliamo ora le **classi laterali destre**:

$$\begin{aligned} H(1,2) &= \{(1,2), (1,2,3)(1,2), (1,3,2)(1,2)\} \\ &= \{(1,2), (1,3), (2,3)\} = (1,2)H \\ H(2,3) &= \{(2,3), (1,2,3)(2,3), (1,3,2)(2,3)\} \\ &= \{(2,3), (1,2), (1,3)\} = (2,3)H \\ H(1,3) &= \{(1,3), (1,2,3)(1,3), (1,3,2)(1,3)\} \\ &= \{(1,3), (2,3), (1,2)\} = (1,2)H \end{aligned}$$

Che forma la seguente **partizione**



Teorema - Cardinalità classi laterali destre e sinistre

Tutte le **classi laterali destre e sinistre** hanno **la stessa cardinalità**, che è quella di H.

<u>Dimostrazione</u>: dati $a, b \in G$ costruiamo una **corrispondenza**

$$\alpha : Ha \to Hb$$
$$\alpha(ha) = hb$$

α è **biunivoca**

- **Iniettività**:

$$\alpha(ha) = \alpha(h'a)$$
$$hb = h'b$$
$$hbb^{-1} = h'bb^{-1}$$
$$h = h'$$

- **Suriettività**: dato che $hb \in Hb$, risulta per definizione

$$hb = \alpha(ha)$$

Ora se prendo $b = e$ ottengo una corrispondenza biunivoca

$$\alpha : Ha \to He = H$$

Posso procedere allo stesso modo con i **laterali sinistri**:

$$\beta : aH \to bH$$
$$\beta(ah) = bh$$

è una biezione, che da luogo ad una biezione $aH \leftrightarrow H$ quando prendo $b = e$. Quindi

$$\begin{array}{ccccc} aH & \leftrightarrow & H & \leftrightarrow & Ha \\ \beta \updownarrow & & & & \updownarrow \alpha \\ bH & & & & Hb \end{array}$$

Teorema - Teorema di Lagrange

Se G è un **gruppo finito** e $H \leq G$, detto $[G : H]$ il **numero di laterali** di H in G, risulta

$$|G| = [G : H]|H|$$

ℹ️ $[G : H]$ si legge **indice di H in G**.

Corollario

Se $H \leq G$, G **finito** allora $|H| \mid |G|$

Dimostrazione: Abbiamo visto che tutte le classi laterali hanno la **stessa cardinalità** $|H|$. Poiché le classi laterali **formano una partizione** di G, l'ordine di G è quello di H moltiplicato per il numero di classi laterali denotato con $[G : H]$.

Lezione 17 - 10/11/2022

Numeri complessi

Introduciamo ora i **numeri complessi**. Nell'insieme $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ delle coppie ordinate di numeri reali, definiamo le seguenti operazioni:

- $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ ed equivale proprio alla somma in $\mathbb{R}^2$

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

- $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

<u>Esempio</u>:

$$(a, 0)(c, 0) = (ac, 0) \leftarrow \text{"copula"}$$
$$(0, 1)(0, 1) = (-1, 0)$$

Proposizione - C è un campo

$\mathbb{C}$ è un campo.

<u>Dimostrazione</u>: è chiaro che $(\mathbb{C}, +)$ è un **gruppo abeliano** il cui elemento neutro è $(0, 0)$. Dobbiamo vedere poi che $(\mathbb{C} \setminus \{0\}, \cdot)$ è un **gruppo abeliano**. Dico che:

1. $(1,0)$ è l'elemento neutro
2. se $(a,b) \neq (0,0)$ allora $(a,b)^{-1}$ è

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$$

Verifiche:

- $(1,0)$ elemento neutro

$$(a,b)(1,0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a,b)$$

- Inverso di (a,b)

$$\begin{aligned}
(a,b)(a,b)^{-1} &= (a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \\
&= \left(a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{-b}{a^2+b^2}, a \cdot \frac{-b}{a^2+b^2} + b \cdot \frac{a}{a^2+b^2}\right) = \\
&= \left(\frac{a^2+b^2}{a^2+b^2}, 0\right) = (1,0)
\end{aligned}$$

Forma algebrica

$$(a,b) = (a,0) + (0,b) = \underbrace{(a,0)}_{a} + \underbrace{(0,a)}_{i}\underbrace{(b,0)}_{b}$$

Abbiamo la seguente corrispondenza:

$$(a,b) \leftrightarrow a + ib$$

che prende il nome di **forma algebrica del numero complesso**. Inoltre, i viene chiamata **unità immaginaria**.

Si vede subito che le operazioni introdotte prima corrispondono, quando si usa la **forma algebrica**, a operare con le **usuali regole di calcolo** in $\mathbb{R}$ insieme a:

$$ib = bi \tag{1}$$
$$i^2 = -1 \tag{2}$$

<u>Esempio</u>:

$$(5+4i)(7-3i) = 35 + 28i - 15i - 4 \cdot 3i^2 = 47 + 13i$$

<u>Nota</u>:

$$\frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \underbrace{\frac{a-ib}{a^2+a^2}}_{(*)} = \frac{a}{a^2+b^2} + i \cdot \frac{-b}{a^2+b^2}$$

La scrittura $(*)$ non ha senso **come numero complesso**, mentre quella alla sua destra dopo l'uguale ha senso.

Definizoni - Coniugato e modulo

Sia $z = a + ib$. Il **coniugato** di z è

$$\bar{z} = a - ib$$

mentre il suo **modulo** è

$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2} \in \mathbb{R}$$

infatti

$$\sqrt{z\bar{z}} = \sqrt{(a+ib)(a-ib)} = \sqrt{a^2-(ib)^2} = \sqrt{a^2+b^2} \in \mathbb{R}$$

<u>Nota</u>: $z^{-1} = \dfrac{\bar{z}}{|z|^2}$

Proprietà

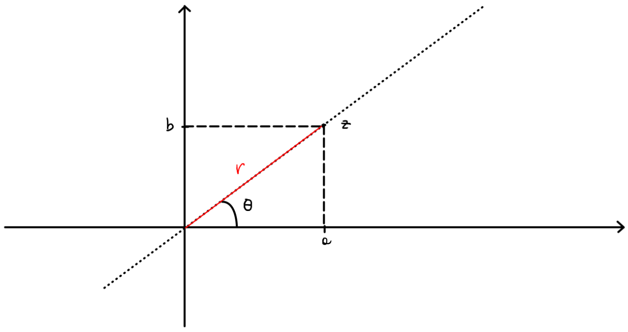
- $\overline{\overline{z}} = z$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$
- $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$
- $z\overline{z} = a^2 + b^2 \geq 0;\ z\overline{z} = 0 \Leftrightarrow z = 0$

  Il numero reale $z\overline{z}$ prende il nome di **norma del numero complesso** z
- $|z_1 z_2| = |z_1||z_2|$
- $|z_1 + z_2| \leq |z_1| + |z_2|$ (ovvero vale la **disugualianza triangolare**)

Forma trigonometrica

Si ha la corrispondenza

$$\begin{array}{ccc} \mathbb{C} & \longleftrightarrow & \mathbb{R}^2 \\ z = a + ib & & (a,b) \end{array}$$



dove:

$$a = r \cos \theta$$
$$b = r \sin \theta$$
$$z = r \cdot (\cos \theta + i \sin \theta)$$
$$r = |z| = \sqrt{a^2 + b^2}$$

ℹ️ L'angolo θ prende il nome di **argomento del numero complesso** z.

N.B.: Se $z' = r'(\cos \theta' + i \sin \theta')$

$$zz' = rr'(\cos(\theta + \theta') + i \sin(\theta + \theta'))$$

che ci dice che il **prodotto** di due numeri complessi scritti sotto forma trigonometrica è il numero complesso che ha come argomento la **somma degli argomenti** e come modulo il **prodotto dei moduli** (ricordiamo che r è il modulo).

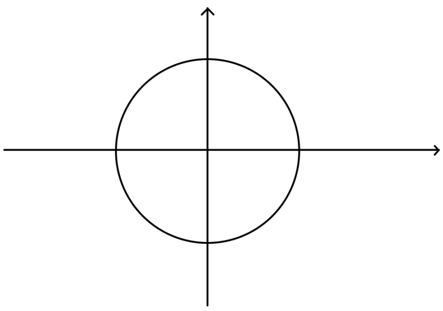
In particolare, la forma trigonometrica di un numero complesso si presta molto bene al **calcolo delle potenze**, perché per ogni intero $n \geq 0$ si ha la seguente formula di **de Moivre**:

$$z^n = r^n(\cos n\theta + i \sin n\theta)$$

Osservazioni varie:

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

rappresenta la circonferenza unitaria:



$$z \in S^1$$
$$z = \cos\theta + i \sin\theta$$

S^1 è un **gruppo** rispetto alla **moltiplicazione**.

Radici n-esime di un numero complesso

Dato $\alpha \in \mathbb{C}$, vogliamo trovare le soluzioni complesse di

$$z^n = \alpha$$

Vedremo che avremo sempre, se $\alpha \neq 0$, n radici n-esime distinte.

Osserviamo che quest'affermazione è falsa in $\mathbb{R}$:

- $\alpha = -1$ con n pari non ha nessuna soluzione
- $\alpha = 1$, $n = 3$ ha una sola soluzione

$$x^3 = 1 \quad x^3 - 1 = 0 \quad (x-1)\underbrace{(x^2+x+1)}_{>0} = 0 \Leftrightarrow x = 1$$

Proposizione

Se $\alpha = r(\cos\theta + i\sin\theta),\ \alpha \neq 0,\ n > 0$ le **radici n-esime** di α sono:

$$z_k = \sqrt[n]{r} \cdot \left(\cos\frac{\theta + 2k\pi}{n} + i \sin\frac{\theta + 2k\pi}{n}\right)$$

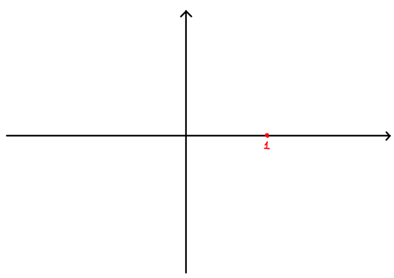
con $k \in \{0, ..., n-1\}$

Vedremo negli esercizi che

$$C_n = \{z \in \mathbb{C} : \overbrace{z^n = 1}^{\text{radici n-esime dell'unità}} \}$$

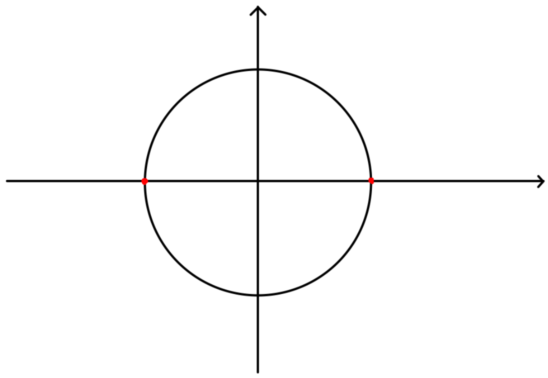
è un **sottogruppo** di $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ **isomorfo** a $\mathbb{Z}_n$.

Se $\alpha = 1$, allora $r = 1$ e $\theta = 0$

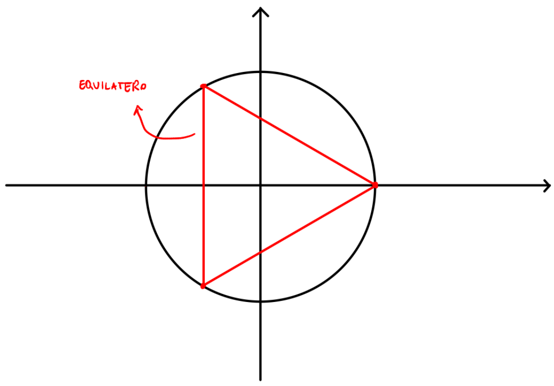


$$z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

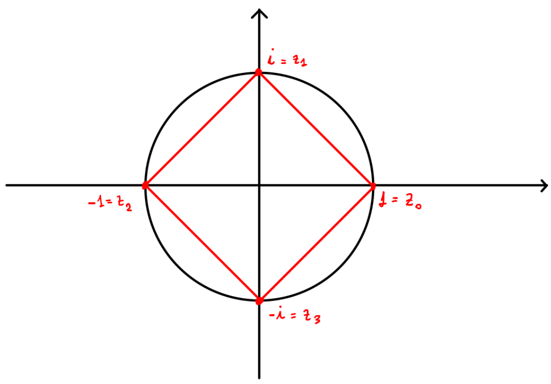
- $n = 2$



- $n = 3$



- $n = 4$



Corollari

Ricoridiamo il **teorema di Lagrange:**

Se G è un **gruppo finito** e $H \leq G$, allora $|H| \mid |G|$. Precisamente

$$|G| = [G : H]|H|$$

Corollario 1

Se $G = p$, p **primo**, allora G è **ciclico**.

Sia $g \in G,\ g \neq e$. Allora $| < g > |$ divide $|G| = p$. Poiché p è **primo**

$$| < g > | = o(g) = p$$

quindi G è ciclico.

Corollario 2

Se G è un **gruppo finito**

$$o(g) \mid |G| \ \forall g \in G$$

Infatti, $o(g) = | < g > |$, che divide $|G|$

Corollario 3

Se $|G| = n$, allora $g^n = e \ \forall g \in G$. Infatti, dato $g \in G$ $|G| = k \cdot o(g)$ quindi

$$g^{|G|} = g^{k \cdot o(g)} = \left(g^{o(g)}\right)^k = e^k = e$$

Esempio: $G = \mathbb{U}_{16}$, $|G| = \phi(2^4) = 8$

$$3^{|G|} = 3^8 = 6561 \equiv 1 \mod 16$$

Osservazione: nuova dimostrazione del **teorema di Eulero-Fermat**:

$$(a, n) = 1 \quad a^{\phi(n)} \equiv 1 \mod n$$

Infatti $U(n)$ ha carindalità $\phi(n)$ e quindi la relazioni precedente è il **corollario 3** in questo caso.

Isomorfismo

$\Phi : G \to G$' è un **omomorfismo** se

$$\Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2) \qquad \forall g_1, g_2 \in G$$

Φ è un **isomorfismo** se è **biunivoca.**

Proprietà che si conservano per isomorfismo

- Abelianità

- Cardinalità
- Ordine dei sottogruppi e degli elementi

Esempi: $(\mathbb{Z}, +)$ e $(\mathbb{Q} \setminus 0, \cdot)$ **non sono isomorfi**.

In $(\mathbb{Z}, +)$ tutti gli elementi **non nulli** hanno **ordine infinito**, mentre in $(\mathbb{Q} \setminus \{0\}, \cdot)$ gli elementi 1 e -1 hanno **ordine** 2.

Più formalmente, se esistesse

$$f : \mathbb{Q} \setminus \{0\} \to \mathbb{Z} \text{ isomorfismo}$$

$f(-1)$ dovrebbe avere ordine 2, ma **nessun elemento non nullo** di $\mathbb{Z}$ ha **ordine finito**.

Classificazione dei gruppi di ordine ≤ 7 a meno di isomorfismo

1. $\{e\}$
2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_4,\ V = \mathbb{Z}_2 \times \mathbb{Z}_2\ (*)$
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_6,\ S_3$ (la vedremo in futuro)
7. $\mathbb{Z}_7$

Classificazione dei gruppi di ordine 4 (*)

Se **esiste un elemento di ordine** 4, allora il gruppo è **ciclico**. Altrimenti tutti gli elementi non identici hanno ordine 2.

$$G = \{Id, a, b, c\} \quad a^2 = b^2 = c^2 = e$$
$$ab = \begin{array}{cccccc} e & \rightsquigarrow & ab = e & \Rightarrow & a = b^{-1} = b & \text{No} \\ a & \rightsquigarrow & ab = a & \Rightarrow & b = e & \text{No} \\ b & \rightsquigarrow & ab = b & \Rightarrow & a = e & \text{No} \\ c & \rightsquigarrow & ab = c & & & \text{Sì} \end{array}$$

Con $ab = c$ si ha

$$\begin{aligned} ab = c = ba \\ bc = a = cb \\ ac = b = ca \end{aligned}$$

Ker e Im

Sia $\Phi : G \to G'$ un **omomorfismo**. Definiamo

$$\begin{aligned} \mathrm{Ker}\Phi &= \{g \in G : \Phi(g) = e'\} \\ \mathrm{Im}\Phi &= \{g \in G' : \exists g \in G : \Phi(g) = g'\} \end{aligned}$$

Proprietà

1. $\Phi(e) = e'$

$$e'\Phi(g) = \Phi(g) = \Phi(eg) = \Phi(e)\Phi(g) = e'\Phi(g)\Phi(g)^{-1} = \Phi(e)\Phi(g)\Phi(g)^{-1} = e' = \Phi(e)$$

2. $\Phi(g^{-1}) = \Phi(g)^{-1}$

$$\Phi(g)\Phi(g^{-1}) = \Phi(gg^{-1}) = \Phi(e) = e' \rightsquigarrow \Phi(g^{-1}) = \Phi(g)^{-1}$$

Esercizio: $\mathrm{Ker}\Phi \leq G,\ \mathrm{Im}\Phi \leq G'$

- $\mathrm{Ker}\Phi \leq G$: devo mostrare che

$$a, b \in \mathrm{Ker}\Phi \Rightarrow ab^{-1} \in \mathrm{Ker}\phi$$

  - **Ipotesi**: $\Phi(a) = \Phi(b) = e'$
  - **Tesi**: $\Phi(ab^{-1}) = e'$

$$\Phi(ab^{-1}) = \Phi(a)\Phi(b^{-1}) = \Phi(a)\Phi(b)^{-1} = e'e'^{-1} = e'$$

- $\mathrm{Im}\Phi \leq G'$: devo mostrare che

$$a', b' \in \mathrm{Im}\Phi \Rightarrow a'b'^{-1} \in \mathrm{Im}\Phi$$

  - **Ipotesi**: $a' = \Phi(a),\ b' = \Phi(b)$
  - **Tesi**: $\exists c \in G : \Phi(c) = a'b'^{-1}$

$$a'b'^{-1} = \Phi(a)\Phi(b)^{-1} = \Phi(a')\Phi(b'^{-1}) = \Phi(\underbrace{ab^{-1}}_{c})$$

Proposizione

Sia $\Phi : G \to G'$ un **isomorfismo**. Allora Φ è **iniettiva** se e solo se $\mathrm{Ker}\Phi = \{e\}$.

Dimostrazione: **Supponiamo Φ iniettiva** e consideriamo $g \in \mathrm{Ker}\Phi$.
Vogliamo dimostrare che $g = e$. Abbiamo

$$\Phi(g) = e' = \Phi(e)$$

Poichè Φ **è iniettiva**, $g = e$.

Viceversa, supponiamo che $\mathrm{Ker} = \{e\}$ e proviamo che Φ è inieittiva, ovvero

$$
\begin{aligned}
\Phi(g_1) = \Phi(g_2) &\Rightarrow g_1 = g_2 \\
\Phi(g_1)\Phi(g_2)^{-1} &= \Phi(g_2)\Phi(g_2)^{-1} \quad \text{molt. a dx per } \Phi(g_2)^{-1} \\
\Phi(g_1)\Phi(g_2^{-1}) &= e' \\
\Phi(g_1 g_2^{-1}) &= e' \\
g_1 g_2^{-1} \in \mathrm{Ker}\Phi &= \{e\} \\
g_1 g_2^{-1} &= e \\
g_1 g_2^{-1} g_2 &= e g_2 \quad \text{molt. a dx per } g_2 \\
g_1 &= g_2
\end{aligned}
$$

Definizione - Sottogruppo normale

$N \leq G$ si dice **normale** in G ($N \trianglelefteq G$) se

$$xN = Nx \quad \forall x \in G$$

ovvero se i **laterali destri e sinistri coincidono**, ovvero

$$
\begin{gathered}
\forall n_1 \in \mathbb{N}\ \exists n_2 \in \mathbb{N} : xn_1 = n_2 x \\
\forall n_2 \in \mathbb{N}\ \exists n_1 \in \mathbb{N} : xn_2 = n_1 x
\end{gathered}
$$

Esempi:

1. In un **gruppo abeliano**, ogni sottogruppo è normale
2. In S_3 abbiamo verificato direttamente che
   - $\{\mathrm{Id}, (1,2,3), (1,3,2)\} \trianglelefteq S_3$ in quanto:

$$
\begin{aligned}
H = H(1,2,3) = H(1,3,2) = (1,2,3)H &= (1,3,2)H \\
H(1,2) &= (1,2)H \\
H(2,3) &= (2,3)H \\
H(1,3) &= (1,3)H
\end{aligned}
$$

   - $\{\mathrm{Id}, (1,2)\} \not\trianglelefteq S_3$ in quanto ad esempio:

$$H(2,3) = \{(2,3)(1,2,3)\} \neq \{(2,3)(1,3,2)\} = (2,3)H$$

Ricordiamo che $x, y \in G$ si dicono **coniugati** se

$$\exists g \in G : y = gxg^{-1}$$

Notazione: Se $H \leq G$

$$H^x = xHx^{-1} = \{xhx^{-1} : h \in H\}$$

Proposizione

Sia $N \leq G$. Sono equivalenti

1. $N \trianglelefteq G$
2. $N^x = N \; \forall x \in G$
3. $xnx^{-1} \in N, \; \forall x \in G, \forall n \in N$
4. N è un **unione di classi di coniugio**.

Dimostrazione: bisogna vedere che $1. \Rightarrow 2. \Rightarrow 3. \Rightarrow 4. \Rightarrow 1.$

- $1. \Rightarrow 2.$

$$
\begin{aligned}
xN &= Nx \; \forall x \\
xNx^{-1} &= Nxx^{-1} = N \\
N^x &= N
\end{aligned}
$$

- $2. \Rightarrow 3.$

  Ovvio. Sappiamo che $xNx^{-1} = N$; in particolare, dato $n_1 \in N \; \exists n_2 \in N$ tale che

$$
xn_1x^{-1} = n_2 \in N
$$

- $3. \Rightarrow 4.$

  Basta vedere che per ogni elemento $n \in N$ la sua classe di coniugio è contenuta in N. Ma questa è proprio l'ipotesi.

- $4. \Rightarrow 1.$

  Dimostrata nella prossima lezione.

Lezione 18 - 11/11/2022

Ultima dimostrazione della lezione precedente

Ricordiamo: $N \leq G$ è **normale** se

$$xN = Nx \ \forall x \in G$$

Dimostrazione:

- $4. \Rightarrow 1.$

  Ricordiamo che la classe di coniugio di $z \in G$ è

  $$\mathrm{cl}(z) = \{xzx^{-1} : x \in G\}$$

  Per ipotesi sappiamo che

  $$N = \dot{\bigcup_{n \in I \subset N}} \mathrm{cl}(n)$$

  Devo dimostrare che $xN = Nx$, ovvero che:

  - dato $n_1 \in N,\ \exists n_2 : xn_1 = n_2x$ e
  - dato $n_1' \in N\ \exists n_2' \in N : n_1'x = xn_2'$

  Ora $n_1 \in \mathrm{cl(n)}$ per qualche $n \in I$, dunque

  $$yn_1y^{-1} = n \rightsquigarrow n_1 = y^{-1}ny$$
  $$xn_1x^{-1} = xy^{-1}nyx^{-1} = xy^{-1}n(xy^{-1})^{-1} \in \mathrm{cl}(n)$$

  e quindi $xn_1x^{-1} \in N$ ovvero $xn_1x^{-1} = n_2$ per qualche $n_2 \in N$, ovvero $xn_1 = n_2x$.
  Ripetendo allo stesso modo l'argomento per n_1' otteniamo che $n_1'x = xn_2'$

Perchè abbiamo introdotto i sottogruppi normali

Se $N \trianglelefteq G$, l'insieme delle classi laterali (destre o sinistre), denotato con G/N, si può dotare della **struttura di gruppo**.

Teorema - G/N è un gruppo

G/N (G modulo N) con l'**operazione binaria**

$$NxNy = Nxy$$

è un **gruppo**. Se G è finito

$$|G/N| = |G|/|N|$$

<u>Dimostrazione</u>: verifichiamo anzitutto che l'operazione è **ben posta**, ovvero

$$Nx = Nx',\ Ny = Ny' \Rightarrow Nxy = Nx'y'$$

questo **segue** dal fatto che $N \trianglelefteq G$. Infatti

$$Nxy = NxNy = Nx'Ny' = NNx'y' = Nx'y'$$

Mostriamo ora che ha le proprietà del gruppo:

- **Associatività**:

$$(NxNy)Nz = NxyNz = N(xy)z = Nx(yz) = NxNyz = Nx(NyNz)$$

- **Elemento neutro**:

$$NxNe = Nxe = Nx, \quad NeNx = Nex = Nx$$

- **Inverso**: $(Nx)^{-1} = Nx^{-1}$

$$\begin{gathered} NxNx^{-1} = Nxx^{-1} = Ne = N \\ Nx^{-1}Nx = Nx^{-1}x = Ne = N \end{gathered}$$

Proiezione al quoziente

Se $N \trianglelefteq G$ c'è un **omomorfismo suriettivo**

$$\begin{gathered} \pi : G \to G/N \\ \pi(x) = Nx \end{gathered}$$

È chiaro che π è **suriettiva**; è un omomorfismo

$$\pi(xy) = Nxy = NxNy = \pi(x)\pi(y)$$

Inoltre $\operatorname{Ker} \pi = N$. Infatti

$$\begin{aligned} \operatorname{Ker} \pi = \{g \in G : \pi(g) = Ne\} = \\ = \{g \in G : Ng = N\} = N \end{aligned}$$

Omomorfismo

Siano $(G_1, *_1),\ (G_2, *_2)$ gruppi, $f : G_1 \to G_2$ è un **omomorfismo** se

$$f(g *_1 g') = f(g) *_2 f(g')$$

<u>Esempio</u>: $f : \mathbb{Z}_4 \to \mathbb{Z}_8,\ f(\overline{x}) = 4\overline{x}$. Si ha

- $f(\overline{0}) = \overline{0}$
- $f(\overline{1}) = \overline{4}$
- $f(\overline{2}) = \overline{0}$
- $f(\overline{3}) = \overline{4}$

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}_4 \quad f(\overline{x} + \overline{y}) = f(\overline{x}) + f(\overline{y}) \quad \begin{aligned} &\text{e}\, \mathrm{Ker} f = \{\overline{0}, \overline{2}\} \\ &\mathrm{Im} f = \{\overline{0}, \overline{4}\} \end{aligned}$$

<u>Esempio</u>:

$$f : S_n \to \mathbb{Z}_2 \qquad f(w) = \begin{cases} \overline{0} & \text{se } w \text{ pari} \\ \overline{1} & \text{se } w \text{ dispari} \end{cases}$$

Per le **proprietà dei segni delle permutazioni** f è un omomorfismo

$$\mathrm{Ker} f = \{w \in S_n : f(w) = \overline{0}\} = \{w \in S_n : w \text{ è pari}\} = A_n$$

Lemma

Se $f : G \to G'$ è un **isomorfismo**,

$$\mathrm{Ker} f \trianglelefteq G$$

<u>Dimostrazione</u>: Il modo **più comodo per dimostrarlo è usando la condizione** $3.$ (negli esercizi va fatto proprio così) dell'ultima proposizione della lezione precedente.
Devo quindi far vedere che se $g \in \mathrm{Ker} f$ e $x \in G$, allora $xgx^{-1} \in \mathrm{Ker} f$;

- **Ipotesi**: $f(g) = e'$
- **Tesi**: $f(gxg^{-1}) = e'$

$$f(xgx^{-1}) = f(x)\overbrace{f(g)}^{=e}f(x^{-1}) = f(x)\overbrace{f(g)}^{=e}f(x)^{-1} = f(x)f(x)^{-1} = e'$$

Teorema - Teorema fondamentale di omomorfismo tra gruppi

Siano G, G' **gruppi** e $f : G \to G'$ un **omomorfismo**. Allora esiste un **unico isomorfismo**

$$\overline{f} : G/\mathrm{Ker}f \to \mathrm{Im}f$$

tale che $f = \overline{f} \circ \pi$, dove $\pi : G \to G/\mathrm{Ker}f$ è la **proiezione canonica**

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & \mathrm{Im}f \subset G' \\
& G/\mathrm{Ker}f \arrow[ur, dashed, "\overline{f}"'] &
\end{tikzcd}$$

Dimostrazione: poniamo $N = \mathrm{Ker}f$. Definiamo $\overline{f} : G/N \to \mathrm{Im}f$ come

$$\overline{f}(Nx) = f(x)$$

Devo vedere che:

1. $\overline{f}$ è **ben posta**
2. $\overline{f}$ è **iniettiva**
3. $\overline{f}$ è **suriettiva**
4. $\overline{f}$ è un **omomorfismo**

Verifiche:

1. significa che

$$\begin{aligned}
&Nx = Ny \Rightarrow \overline{f}(Nx) = \overline{f}(Ny) \\
&Nx = Ny \Rightarrow f(x) = f(y) \\
&xy^{-1} \in N \\
&xy^{-1} \in \mathrm{Ker}f \\
&f(xy^{-1}) = e' \qquad f(x)f(y^{-1}) = e' \\
&f(x)f(y)^{-1} = e' \quad f(x) = f(y)
\end{aligned}$$

2. $\overline{f}(Nx) = \overline{f}(Ny) \Rightarrow Nx = Ny$ cioè $f(x) = f(y) \Rightarrow Nx = Ny$

   Basta seguire al **contrario** le implicazioni di 1.

$$f(x) = f(y) \Rightarrow f(x)f(y^{-1}) = e' \Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \mathrm{Ker}f = N \Rightarrow Nx = Ny$$

3. Dato $y \in \mathrm{Im}f,\ \exists x \in G : y = f(x) = \overline{f}(Nx)$
4. $\overline{f}(NxNy) = \overline{f}(Nxy) = f(xy) = f(x)f(y) = \overline{f}(Nx)\overline{f}(Ny)$

Applicazione

Proposizione

Sia G un **gruppo ciclico**, se G è **infinito** allora $G \cong \mathbb{Z}$, se G è **finito** $G \cong \mathbb{Z}_n$ per qualche n.

Dimostrazione: Sia $G =< g >$. Consideriamo

$$f : \mathbb{Z} \to G,\ f(k) = g^k$$

f è chiaramente **suriettiva** ed è un **omomorfismo**:

$$f(k+h) = g^{k+h} = g^k g^h = f(k)f(h)$$

Se G è **infinito** sappiamo che $g^h \neq g^k$ per $h \neq k$, dunque f è **iniettiva**, quindi un **isomorfismo** $\mathbb{Z} \cong G$.

Se $G =< g >$ è **ciclico** di ordine n, allora $\mathrm{Ker} f = n\mathbb{Z}$ e per il **teorema di omomorfismo**

$$G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

Lezione 20 - 17/11/2022

Correzione sesto foglio esercizi

Spazio vettoriale

Ricordiamo la definizione di **spazio vettoriale su campo** $\mathbb{K}$. È un **insieme non vuoto** V dotato di operazioni:

$$\begin{aligned} V \times V &\to V, \qquad & \mathbb{K} \times V &\to V \\ (a, b) &\mapsto a + b, \qquad & (\alpha, v) &\mapsto \alpha v \end{aligned}$$

tali che $(V, +)$ è un **gruppo abeliano** e

$$\begin{array}{cl} \alpha(v+w) = \alpha v + \alpha w & \forall \alpha \in \mathbb{K}, \forall v, w \in V \\ (\alpha+\beta)v = \alpha v + \beta v & \forall \alpha, \beta \in \mathbb{K}, \forall v \in V \\ (\alpha\beta)v = \alpha(\beta v) & \forall \alpha, \beta \in \mathbb{K}, \forall v \in V \\ 1v = v & \forall v \in V \end{array}$$

<u>Esempi</u>:

1. $\mathbb{K}^n$, vettori riga
2. $M_{mn}(\mathbb{K})$, matrici $m \times n$ a coefficienti in $\mathbb{K}$
3. $\mathbb{K}[t]$, polinomi a coefficienti in $\mathbb{K}$ nella variabile t
4. V spazio vettoriale, I insieme

$$V^I = \{f : I \to V\}$$

V^I è uno spazio vettoriale.

$$f, g \in V^I \qquad (f+g)(x) = \underbrace{f(x)}_{\in V} + \underbrace{g(x)}_{\in V} \quad x \in I$$

$$\alpha \in \mathbb{K}, f \in V^I \qquad (\alpha f)(x) = \alpha f(x)$$

N.B.:

$$I = \{1, ..., n\}, \; V = \mathbb{K}$$
$$V^I = \mathbb{K}^{\{1,...,n\}} \equiv \mathbb{K}^n$$
$$f \rightsquigarrow f(1), ..., f(n) \rightsquigarrow \begin{pmatrix} f(1) \\ \vdots \\ f(n) \end{pmatrix} \in \mathbb{K}^n$$

Definizione - Sottospazio

Un **sottoinsieme non vuoto** $W \subset V$ è un **sottospazio vettoriale** di V se è uno **spazio vettoriale rispetto alle operazioni indotte da** V.

$$\begin{array}{ccc} V \times V & \longrightarrow & V \\ \cup| & & \cup \\ W \times W & \dashrightarrow & W \end{array} \qquad \begin{array}{ccc} \mathbb{K} \times V & \longrightarrow & V \\ \cup| & & \cup \\ \mathbb{K} \times W & \dashrightarrow & W \end{array}$$

Osservazione: In altri termini $W \subset V, \emptyset \neq W$ è un sottospazio se

$$w_1 + w_2 \in W \quad \forall w_1, w_2 \in W$$
$$\alpha w \in W \quad \forall \alpha \in \mathbb{K}, \forall w \in W$$

Criterio: $\emptyset \neq W \subset V$ è un **sottospazio** se e solo se

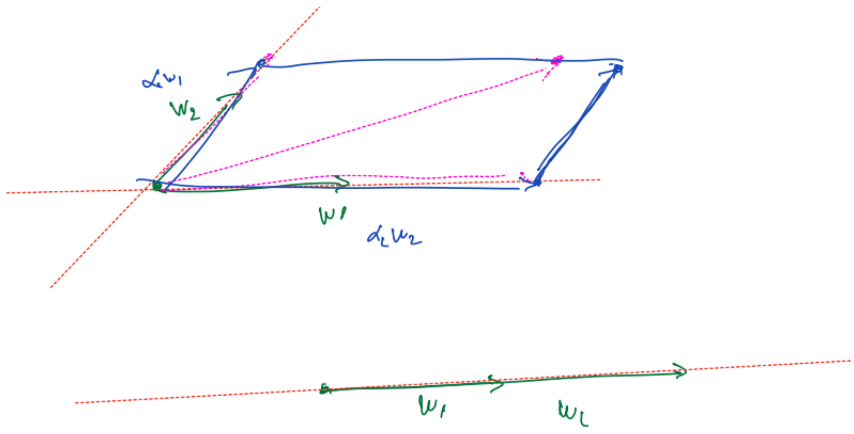
$$\alpha_1 w_1 + \alpha_2 w_2 \in W \quad \forall \alpha_1, \alpha_2 \in \mathbb{K}$$
$$\forall w_1, w_2 \in W$$

Definizone - Combinazione lineare

$\alpha_1 w_2 + \alpha_2 w_2$ si chiama **combinazione lineare** dei **vettori** w_1, w_2 con **scalari** α_1, α_2.

Esempio: Siamo interessati a considerare

$$\{\alpha_1 w_1 + \alpha_2 w_2 | \alpha_1, \alpha_2 \in \mathbb{K}\}$$



Qualsiasi multiplo prendo, posso ottenre tutti il piano

Definizione - Span

Sia V uno **spazio vettoriale**. La **combinazione lineare** dei vettori $v_1, ..., v_k$ con scalari $\alpha_1, ..., \alpha_k$ è il vettore

$$\alpha_1 v_1 + ... + \alpha_k v_k$$

Poniamo

$$\mathrm{Span}(v_1, ..., v_k) = \{\alpha_1 v_1 + ... + \alpha_k v_k | \alpha_1, \alpha_k \in \mathbb{K}\}$$

Proposizione

$\mathrm{Span}(v_1, ..., v_k)$ è un **sottospazio vettoriale** di V.

Dimostrazione: Dobbiamo dimostrare che se $x, y \in \mathrm{Span}(v_1, ..., v_k)$ e $\alpha, \beta \in \mathbb{K}$ allora $\alpha x + \beta y \in \mathrm{Span}(v_1, ..., v_k)$:

Poniamo:

- $x = \alpha_1 v_1 + ... + \alpha_k v_k$
- $y = \beta_1 v_1 + ... + \beta_k v_k$

Sostituendo x e y si ha che:

$$\begin{aligned} \alpha x + \beta y &= \alpha(\alpha_1 v_1 + ... + \alpha_k v_k) + \beta(\beta_1 v_1 + ... + \beta_k v_k) = \\ &= \alpha\alpha_1 v_1 + ... + \alpha\alpha_k v_k + \beta\beta_1 v_1 + ... + \beta\beta_k v_k = \\ &= (\alpha\alpha_1 + \beta\beta_1)v_1 + (\alpha\alpha_2 + \beta\beta_2)v_2 + ... + (\alpha\alpha_k + \beta\beta_k) \end{aligned}$$

che **per definizione** questo vettore appartiene a $\mathrm{Span}(v_1, ..., v_k)$.

Lezione 21 - 18/11/2022

Ripasso scorsa lezione

- $W \subset V, W \neq \emptyset$ è un **sottospazio vettoriale** di V se e solo se

$$\alpha_1 w_1 + \alpha_2 w_2 \in W \quad \begin{array}{l} \forall \alpha_1, \alpha_2 \in \mathbb{K} \\ \forall w_1, w_2 \in W \end{array}$$

- $v_1, ..., v_k \in V$, $\text{Span}(v_1, ..., v_k) = \{\alpha_1 v_1 + ... + \alpha_k v_k | \alpha_i \in \mathbb{K}\}$
- $\text{Span}(v_1, ..., v_k)$ è un **sottospazio** di V

Ripasso matrici

$A \in M_{mn}(\mathbb{K})$ è una matrice

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

La matrice inoltre può essere “affettata” per righe e colonne

$$A = (A^1 \dots A^n) = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$$

Ricordiamo anche la seguente notazione:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad \begin{aligned} A_1 &= (1\ 2\ 3) \\ A_2 &= (4\ 5\ 6) \end{aligned} \quad \begin{aligned} A^1 &= \begin{pmatrix} 1 \\ 4 \end{pmatrix} \\ A^2 &= \begin{pmatrix} 2 \\ 5 \end{pmatrix} \\ A^3 &= \begin{pmatrix} 3 \\ 6 \end{pmatrix} \end{aligned}$$

Prodotto righe per colonne

$$\begin{aligned} M_{mk}(\mathbb{K}) \times M_{kn}(\mathbb{K}) &\to M_{mn}(K) \\ (A, B) &\mapsto AB \end{aligned}$$

Dove si ha che

$$(AB)_{ij} = \sum_{h=1}^{k} (A)_{ih}(B)_{hj} \quad \begin{aligned} 1 \leq i \leq m \\ \\ 1 \leq j \leq n \end{aligned}$$

<u>Esempio</u>:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 14 & 32 \\ 32 & 77 \end{pmatrix}$$

e come si può vedere la prima matrice 2×3 moltiplicata per la seconda matrice 3×2 da vita alla matrice 2×2.

Sistemi lineari di m equazioni in n incognite

Un **sistema lineare di** m **equazioni in** n **incognite** è un sistema del tipo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \dots + a_{mn}x_n = b_n \end{cases}$$

Risolvere il sistema significa **trovare i vettori** $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ per cui **tutte le equazioni sono verificate**. Se il sistema ammette soluzioni allora si dice **compatibile**.

Esempio:

$$\begin{cases} x_1 = 1 \\ x_2 = 0 \end{cases}$$

non è compatibile.

In generale dovremo affrontare i seguenti problemi:

1. Decidere se un **sistema è compatibile**;
2. Se compatibile, **trovare tutte le soluzioni**;
3. Se compatibile, capire "da quanti parametri" **dipendono le soluzioni**.

Trasformazione di un sistema in matrici

Vediamo ora come trasformare un sistema nel suo equivalente sotto forma di matrici:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \dots + a_{mn}x_n = b_n \end{cases}$$

diventa

$$\begin{pmatrix} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \text{ in } \mathbb{K}^m$$

che a sua volta diventa

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & & & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

che si scrive: $AX = b$, dove:

- A è la **matrice dei coefficienti**;
- X è il **vettore delle incognite**;
- b è il **vettore dei termini noti**.

Inoltre viene chiamata $(A|b) \in M_{mn+1}(\mathbb{K})$ la **matrice completa del sistema**.

Esempio: si consideri il seguente sistema:

$$\begin{cases} 2x_1 + x_2 - 3x_3 + x_4 = 1 \\ x_3 + x_4 = 5 \\ x_1 - x_2 - x_3 - 2x_4 = 0 \end{cases}$$

si ha che

$$A = \begin{pmatrix} 2 & 1 & -3 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & -2 \end{pmatrix} \qquad b = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

mentre la matrice completa del sistema avrà la seguente forma:

$$(A|b) = \begin{pmatrix} 2 & 1 & 3 & 1 & 1 \\ 0 & 0 & 1 & 1 & 5 \\ 1 & -1 & -1 & -2 & 0 \end{pmatrix}$$

Quest'ultima forma ci da moltissime informazioni sul sitema quali: compatibilità, da quanti coefficienti dipende.

Osservazione importante

Il sistema $AX = b$ si può riscrivere nella forma $x_1 A^1 + x_2 A^2 + ... + x_n A^n = b(*)$

$$\begin{cases} 2x_1 - x_2 - x_3 \\ x_1 + x_3 = 5 \end{cases}$$
$$A = \begin{pmatrix} 2 & -1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 2x_1 - x_2 - x_3 \\ x_1 + x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$$

che si riscrive:

$$x_1 \begin{pmatrix} 2 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} -1 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$$

Proposizione

Il sistema $AX = b$ è compatibile se e solo se $b \in \mathrm{Span}(A^1, ..., A^n)$.

La relazione $(*)$ dimostra questa proposizione.

Nomenclatura - Sistema omogeneo

Un sistema lineare $AX = b$ con $b = 0_{\mathbb{K}^n}$ si dice **omogeneo**.

<u>Osservazione</u>: un sistema omogeneo è **sempre compatibile** perchè $X = 0_{\mathbb{K}^n}$ è soluzione: $A \cdot 0 = 0$.

Proposizione

L'insieme $\mathrm{Sol}(A|b) = \{X \in \mathbb{K}^n | AX = b\}$ è un **sottospazio vettoriale** di $\mathbb{K}^n$ se e solo se $b = 0$.

<u>Dimostrazione</u>: se $b \neq 0$, $0_{\mathbb{K}^n} \notin \mathrm{Sol}(A|b)$, quindi $\mathrm{Sol}(A|b)$ non può essere un sottospazio vettoriale di $\mathbb{K}^n$.
Viceversa, sia $b = 0$. Dimostriamo che $\mathrm{Sol}(A, 0)$ è un sottospazio.
Prendiamo $X_1, X_2 \in \mathrm{Sol}(A, 0),\ \alpha_1, \alpha_2 \in \mathbb{K}$ e dimostriamo che $\alpha_1 X_1 + \alpha_2 X_2 \in \mathrm{Sol}(A, 0)$.
Per **ipotesi**, $AX_1 = 0,\ AX_2 = 0$.

$$A(\alpha_1 X_1 + \alpha_2 X_2) = \alpha_1 \underbrace{AX_1}_{=0} + \alpha_2 \underbrace{AX_2}_{=0} = 0$$

Teorema

Supponiamo che $AX = b$ sia compatibile e sia $X_0 \in \mathrm{Sol}(A|b)$. Allora

$$\mathrm{Sol}(A|b) = X_0 + \mathrm{Sol}(A|0) \quad (\blacksquare)$$

<u>Dimostrazione</u>: dimostro la doppia inclusione in $(\blacksquare)$.

Prendiamo $X \in \mathrm{Sol}(A|b)$, che posso **riscrivere come**

$$X = X_0 + (X - X_0)$$

Basta vedere che $X - X_0 \in \mathrm{Sol}(A|0)$.

Per ipotesi $AX = b$ e $AX_0 = b$, quindi

$$A(X - X_0) = AX - AX_0 = b - b = 0$$

Quindi ho dimostrato l'inclusione $\subseteq$.
Per dimostrare $\supseteq$, scelgo $\overline{X} \in \mathrm{Sol}(A|0)$ e faccio vedre che $X_0 + \overline{X} \in \mathrm{Sol}(A|b)$

$$A(X_0 + \overline{X}) = AX_0 + A\overline{X} = b + 0 = b$$

Matrice a scala o a gradini

$$\begin{cases} x_1 + 2x_2 + 3x_3 = 1 \\ x_2 - x_3 = 4 \\ x_3 = 5 \end{cases}$$

Sottoforma di matrice diventa

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & -1 & 4 \\ 0 & 0 & 1 & 5 \end{pmatrix}$$

⚠️ Come si può vedere, gli 1 incontrari su ogni riga leggendole da sinistra verso destra formano dei “gradini”.

Le matrici di questa permettono di risolvere il sistema in modo semplice:

$$\begin{cases} x_1 = 1 - 2x_2 - 3x_x = 1 - 18 - 15 = -32 \\ x_2 = x_3 + 4 = 5 + 4 = 9 \\ x_3 = 5 \end{cases}$$

Basta sostituire dal basso verso l'alto per risolverlo.

Idea: cambiare il sistema senza cambiare le soluzioni ed arrivare ad una matrice a scala.

Operazioni che non cambiano le soluzioni

1. **Scambiare** due equazioni;
2. **Moltiplicare** un'equazione per $\alpha \in \mathbb{K} \setminus \{0\}$;
3. **Sommare** a un'equazione un multiplo di un'altra.

A livello di matrice completa dell sistema, 1. 2. e 3. diventano:

1. $A_i \leftrightarrow A_j$
2. $A_i \to \alpha A_i \quad \alpha \in \mathbb{K} \setminus \{0\}$
3. $A_i \to A_i + \beta A_j \quad \beta \in \mathbb{K}$

Definizione - Matrice a scala

Una **matrice a scala** è una matrice del tipo:

> ℹ️ Gli 1 vengono chiamati **gradini** o **pivot**.

Correzione dell'esercitazione del 15/11

Lezione 22 - 21/11/2022

Formula per contare il numero di cicli

In generale $\lambda = (1^{a_1}\ 2^{a_2}\ 3^{a_3}\ ...)$ si ha

$$|C_\lambda| = \frac{n!}{\prod j^{a_j}(a_j!)}$$

Esempio: si vogliono contare il numero di permutazioni formate dalla partizione $2^1 3^3 4^2$, avremo

$$44332$$
$$1\ 2\ 3\ 4 \mid 5\ 6\ 7\ 8 \mid 9\ 10\ 11 \mid 12\ 13\ 14 \mid 15\ 16\ 17 \mid 18\ 19$$

abbiamo diviso la partizione in gruppi di numeri distinti che andiamo a contare:

- Abbiamo che $n = 4^2 3^3 2^1 = 19$
- Quindi

$$|C_\lambda| = \frac{19!}{4^2 \cdot 3^3 \cdot 2^1 \cdot 3! \cdot 2!}$$

> ⚠️ Il $2!$ e il $3!$ al denominatore escono dal fatto che in questo caso i due gruppi da 4 elementi e i tre gruppi da 3 elementi **commutano**.

Risoluzione di sistemi lineari

Sistema di equazioni in n incognite $\rightsquigarrow AX = b$.

- $A \in M_{mn}(\mathbb{K})$
- $X \in \mathbb{R}^n = M_{n1}(\mathbb{K})$
- $b \in \mathbb{K}^m = M_{m1}(\mathbb{K})$

Abbiamo osservato che **tutte le informazioni** sono contenute nella **matrice completa** del sistema $(A|b) \in M_{mn+1}(\mathbb{K})$. Prendiamo il seguente sistema

$$\begin{cases} x_1 + x_2 - x_3 - 2x_4 = 4 \\ x_1 - x_3 = 0 \\ x_2 + x_4 = -2 \end{cases} \qquad \longleftrightarrow \qquad AX = b$$

Creiamo ora la **matrice** A e i **vettori** X e b:

- Matrice A dei **coefficienti**:

$$A = \begin{pmatrix} 1 & 1 & -1 & -2 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

- Vettore X delle **incognite**:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

- Vettore b **dei termini noti**:

$$b = \begin{pmatrix} 4 \\ 0 \\ -2 \end{pmatrix}$$

La **matrice completa del sitema** è:

$$(A|b) = \begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -2 \end{pmatrix}$$

Vogliamo ora **modificare** la matrice completa del sistema in modo tale da **non cambiare le soluzioni del sistema**. Ciò può essere ottenuto tramite le **operazioni elementari sulle righe**. Ricordiamo quali sono:

1. $A_i \leftrightarrow A_j$
2. $A_i \to \alpha A_i \quad \alpha \in \mathbb{K} \setminus \{0\}$
3. $A_i \to A_i + \beta A_j \quad \beta \in \mathbb{K}$

Definizione - Matrice a gradini o a scala

Una matrice A è in **forma a gradini** se è del tipo:

Più formalmente, A **è a gradini** se

1. $A_i = 0 \Rightarrow A_j = 0 \; \forall j \geq i$
2. $A_i \neq 0$, il primo elemento non nullo di A_i è 1
(se $j = \min\{k | a_{ik} \neq 0\}, a_{ij} = 1$)
3. Il pivot della riga i appare nella colonna j, il pivot della riga $j+1$, se esiste, appare nella colonna $h > j$.

> ⚠️ Se nella forma a gradini, c'è un 1 nell'ultima riga e colonna, allora il sistema non è compatibile.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \longrightarrow \begin{cases} x_1 = 1 \\ 0 = 1 \end{cases}$$

Algoritmo di Gauss per la digressione a gradini

1. Si individua il **primo elemento non nullo** scorrendo la matrice per colonne dall'**alto verso il basso** (a serpente). Se il primo elemento trovato appartiene alla riga i, scambio la riga i con la prima;
2. Rendiamo 1 tale elemento con operazioni di tipo 2;
3. Se il pivot appare nella colonna j, rendiamo 0 tutti gli elementi della colonna j, dalla riga 2 alla riga n con operazioni di tipo 3;
4. Iteriamo operando sulle righe di indice > 1 e sullo colonne di indice $> j$.

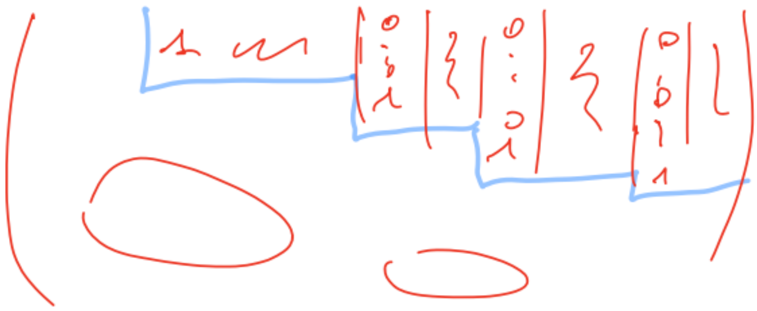
<u>Esempio</u>:

$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ \underline{1} & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -2 \end{pmatrix} \xrightarrow{A_2 \to A_2 - A_1}$$
$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 0 & -1 & 0 & 2 & -4 \\ 0 & 1 & 0 & 1 & -2 \end{pmatrix} \xrightarrow{A_2 \to -A_2}$$
$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & \underline{1} & 0 & 1 & -2 \end{pmatrix} \xrightarrow{A_3 \to A_3 - A_2}$$
$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 3 & -6 \end{pmatrix} \xrightarrow{A_3 \to \frac{A_3}{3}}$$
$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

Ora la matrice è in forma a gradini.

Definizione - Matrice a scala ridotta

Una matrice è a **scala ridotta** se è del tipo



ovvero nelle colonne dei pivot appaiono tutti 0 al di sopra del pivot.

Algoritmo per passare dalla forma a scala alla forma a scala ridotta

1. Partendo dal pivot che giace nella colonna più a destra, rendiamo 0 tutte le entrate di tale colonna sopra al pivot con operazioni di tipo 3;
2. Iteriamo procedendo da destra verso sinistra.

Esempio:

$$\begin{pmatrix} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix} \xrightarrow[A_1 \to A_1 + 2A_3]{A_2 \to A_2 + 2A_3}$$
$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix} \xrightarrow[A_1 \to A_1 - A_2]{}$$
$$\begin{pmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

Che risolve il seguente sistema:

$$\begin{cases} x_1 - x_3 = 0 \\ x_2 = 0 \\ x_4 = -2 \end{cases} \longrightarrow \begin{cases} x_1 = x_3 = t \\ x_2 = 0 \\ x_3 = t \\ x_4 = -2 \end{cases}$$

che in forma di matrice diventa:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + t \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

che risolve il sistema originale nel seguente modo:

$$\begin{cases} x_1 + x_2 - x_3 - 2x_4 = 4 & t - t - 2(-2) = 4 \\ x_1 - x_3 = 0 & t - t = 0 \\ x_2 + x_4 = -2 & 0 + (-2) = -2 \end{cases}$$

Esercizio completo: trasformare la seguente matrice in forma a gradini e risolvere il sistema

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 2 & 3 \end{pmatrix}$$

- Trasformazione in forma a gradini:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 2 & 3 \end{pmatrix} \overrightarrow{A_2 \leftrightarrow A_1}$$

$$\begin{pmatrix} 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 3 \end{pmatrix} \overrightarrow{A_3 \to A_3 - A_2}$$

$$\begin{pmatrix} 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 3 \end{pmatrix} \overrightarrow{A_3 \to \frac{A_3}{2}}$$

$$\begin{pmatrix} 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix}$$

- Trasfomrazione in forma a scala ridotta:

$$\begin{pmatrix} 0 & 0 & 1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix} \overrightarrow{A_1 \to A_1 + A_3}$$

$$\begin{pmatrix} 0 & 0 & 1 & 2 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix} \overrightarrow{A_1 \to A_1 - 2A_2}$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{3}{2} \end{pmatrix}$$

Se si pensa questa matrice come **matrice completa del sistema**, il sistema corrispondente è:

$$\begin{cases} x_3 = \frac{1}{2} \\ x_4 = 0 \\ x_5 = \frac{3}{2} \end{cases}$$

le soluzioni sono dunque:

$$\begin{cases} x_1 = t \\ x_2 = s \\ x_3 = \frac{1}{2} \\ x_4 = 0 \\ x_5 = \frac{3}{2} \end{cases}$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{3}{2} \end{pmatrix} + t \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + s \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Definzione - Rango

Il **rango** di una matrice è il **numero di pivot** di una sua forma a scala.

Notazione

$$\mathrm{rk}(A)$$

Teorema - Teorema di Rouchè-Capelli

Il sistema lineare $AX = b$, con $A \in M_{mn}(\mathbb{K})$ e $X \in \mathbb{K}^n, b \in \mathbb{K}^m$ è **compatibile** se e solo se

$$\mathrm{rk}(A) = \mathrm{rk}(A|b)$$

In tal caso esiste una **corrispondenza biunivoca** tra

$$\mathrm{Sol}(A|b) \to \mathbb{K}^{n-\mathrm{rk(A)}}$$

Tale corrispondenza si esplicita nel sistema **poratando al secondo memebro le incognite che non corrispondono a gradini e dando ad esse valori arbitrari e indipendenti**.

Lezione 23 - 24/11/2022

Riassunto Span

Ricrodiamo: V **spazio vettoriale**, $v_1, ...v_k \in V$

$$\text{Span}(v_1, ..., v_k) = \{\alpha_1 v_1 + ... + \alpha_k v_k | \alpha_i \in \mathbb{K}\}$$

Più in generale, se $S \subseteq V$, poniamo:

$$\text{Span} S = \text{insieme delle combinazioni lineari di tutti i sottoinsiemi finiti di } S$$

Definizione - Insieme di generatori

Diciamo che S è un **insieme di generatori** per V se $V = \text{Span} S$. Diciamo che V è **finitamente generato** se esiste un **insieme finito di generatori** per V.

In altri termini, V è finitmente generato se esistono vettori $v_1, ..., v_n \in V$ tali che ogni vettore di V si scrive come combinazione lineare di $v_1, ..., v_n$.

Esempi:

1. $V = \mathbb{K}^n$, poniamo

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \end{pmatrix} \leftarrow \text{posto } i$$

Faccio vedere che $V = \text{Span}(e_1, ..., e_n)$:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{pmatrix} + ... + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{pmatrix} =$$

$$= x_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + ... + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} =$$

$$= x_1 e_1 + x_2 e_2 + ... + x_n e_n$$

2. $V = M_{mn}(\mathbb{K})$, poniamo

$$e_{ij} = \begin{pmatrix} 0 & 0 & ... & 0 & 0 \\ 0 & \ddots & \vdots & & 0 \\ \vdots & & 1 & & \vdots \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & ... & 0 & 0 \end{pmatrix}$$

ovvero e_{ij} rappresenta un 1 all'**i-esima riga** e **j-esima colonna**.

$V = \text{Span}\{e_{ij} | 1 \leq i \leq n,\ 1 \leq j \leq n\}$

$A = (a_{ij})$

$$A = \sum_{\substack{i=1...m \\ j=1...n}} a_{ij} \cdot e_{ij}$$

<u>Esempio</u>:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = e_{11} + 2e_{12} + 3e_{13} + 4e_{21} + 5e_{22} + 6e_{23}$$

3. $V = \mathbb{K}[t]$, $V = \text{Span}\{t^i | 0 \leq i\}$

   Infatti, dato $p(t) \in V$,

$$p(t) = \sum_{i=0}^{N} a_i t^i$$

> ℹ️ Intepretriamo questa espressione come combinazione lineare di $1, t, t^2, ..., t^N$ con coefficienti $a_0, a_1, ..., a_n$.

   Esempio: $1 + 3t + 5t^7 - 9t^{12}$

   Osserviamo che V **non è finitamente generato**. Infatti, se $\deg\, p(t)$ denota il **grado** di $p(t)$, il grado

$$\deg(\alpha p(t) + \beta q(t)) \leq \max\{\deg\, p(t), \deg\, q(t)\}$$

   Pertanto non può esistere un insieme finito di generatori per V, perché se

$$S = \{p_1(t), ..., p_s(t)\}$$
$$h = \max_{1 \leq k \leq s} \deg\, p_k(t)$$

   si ha che $t^{h+1} \notin \text{Span}\ S$.

> ⚠️ Abbiamo dimostato che V non è finitamente generato perchè, se prendo due polinomi, qual è il grado della loro combinazione lineare? È minore o uguale del massimo dei gradi dei fattori, quindi se si ha una combinazione lineare finita di vettori, un polinomio più grande del massimo numero finito che si ha non si trova.

Nomenclatura

Se A è un **matrice**, la **trasposta** di A (notazione A^t o ${}^tA$) è la matrice ottenuta **scambiando righe e colonne**:

$$({}^tA)_{ij} = (A)_{ji}$$
$$A \in M_{mn}(\mathbb{K}),\ {}^tA \in M_{nm}(\mathbb{K})$$

Esempi:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}^t = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Proprietà delle trasposte

1. $A^{tt} = A$
2. $(\alpha A + \beta B)^t = \alpha A^t + \beta B^t$
3. $(AB)^t = B^t A^t$

Nomenclatura

- **Matrici simmetriche**

$$S_n^+ = \{A \in M_n(\mathbb{K}) | A = A^t\}$$

- **Matrici antisimmetriche**

$$S_n^- = \{A \in M_n(\mathbb{K}) | A = -A^t\}$$

> ⚠️ Questo vale solamente per le matrici simmetriche.

Esercizio svolto: $S_n^{\pm}$ sono **sottospazi** di $M_n(\mathbb{K})$.

Dobbiamo dimostrare che se $A, B \in S_n^+$ e $\alpha, \beta \in \mathbb{K}$ allora $\alpha A + \beta B \in S_n^+$.

- **Ipotesi**: $A = A^t, B = B^t$

$$(\alpha A + \beta B)^t \overset{2.}{=} \alpha A^t + \beta B^t = \alpha A + \beta B$$

Similarmente se $A, B \in S_n^-, A^t = -A, B = -B^t$

$$(\alpha A + \beta B)^t = \alpha A^t + \beta B^t = \alpha(-A) + \beta(-B) = -(\alpha A + \beta B)$$

Esercizi svolti

4. Trovare generatori per S_2^+, S_2^-
    - S_n^+

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \Rightarrow \begin{cases} a = a \\ b = c \\ c = b \\ d = d \end{cases} \to b = c$$

quindi $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_2^+$ se e solo se è del tipo

$$\begin{aligned} \begin{pmatrix} a & b \\ b & d \end{pmatrix} &= \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \\ &= ae_{11} + b(e_{12} + e_{21}) + de_{22} \end{aligned}$$

Quindi $S_2^+ = \mathrm{Span}(e_{11}, e_{12} + e_{21}, e_{22})$.

- S_2^-

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = -\begin{pmatrix} a & c \\ b & d \end{pmatrix} \Rightarrow \begin{cases} a = -a \\ b = -c \\ c = -b \\ d = -d \end{cases} \to \begin{cases} 2a = 0 \\ b = -c \\ 2d = 0 \end{cases} \to \begin{cases} a = 0 \\ b = -c \\ d = 0 \end{cases}$$

quindi $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_2^-$ se e solo se è del tipo:

$$\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} = b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Quindi $S_2^- = \mathrm{Span}(e_{12} - e_{21})$.

<u>Procedimento generale</u>:

- Dimostro che è un sottospazio;
- Quando so che è lo è cerco di capire quali sono le condizioni che ho per avere un elemento in quel sottospazio;
- Quasi sempre la trasposta viene trasferita in un sistema lineare;

- Cerco di capire come esprimerla tramite elementi fissati, quindi separo le lettera.

5. $\mathbb{K}_d[t] = \{p(t) \in \mathbb{K}[t] | \deg p(t) \leq d\}$.

   $\mathbb{K}_d[t]$ è un sottospazio vettoriale di $\mathbb{K}[t]$ e $\mathbb{K}_d[t] = \mathrm{Span}(1, t, t^2, ..., t^d)(*)$

   Il fatto che $\mathbb{K}_d[t]$ sia un sottospazio è chiaro dalla relazione

$$\deg(\alpha p(t) + \beta q(t)) \leq \max\{\deg p(t), \deg q(t)\}$$

   La relazione $(*)$ è data dal fatto che $p(t) \in \mathbb{K}_d[t]$ si scrive come

$$p(t) = \sum_{i=0}^{d} a_i t^i$$

Osservazioni varie

1. $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ generano $\mathbb{R}^2$.

   Devo vedere che ogni $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$ è **combinazione lineare** di $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

   A sua volta, questo significa che per ogni $\begin{pmatrix} a \\ b \end{pmatrix}$ esistono x_1, x_2 tali che

$$x_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

   che è il **sistema lineare di matrice completa**

$$\begin{pmatrix} 1 & 1 & a \\ 1 & -1 & b \end{pmatrix}$$

   Risolviamolo:

$$\begin{pmatrix} 1 & 1 & a \\ 1 & -1 & b \end{pmatrix} \to \begin{pmatrix} 1 & 1 & a \\ 0 & 1 & \frac{a-b}{2} \end{pmatrix} \to \begin{pmatrix} 1 & 0 & \frac{a+b}{2} \\ 0 & 1 & \frac{a-b}{2} \end{pmatrix}$$

   che rappresenta il sistema:

$$\begin{cases} x_1 = \frac{a+b}{2} \\ x_2 = \frac{a-b}{2} \end{cases}$$

2. $\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix} \begin{pmatrix}1\\0\end{pmatrix}$ generano $\mathbb{R}^2$.

Devo vedere che:

$$x_1\begin{pmatrix}1\\1\end{pmatrix} + x_2\begin{pmatrix}1\\-1\end{pmatrix} + x_3\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}$$

Scriviamo la marice completa e risolviamo il sistema ottenuto:

$$\begin{pmatrix}1 & 1 & 1 & a\\ 1 & -1 & 0 & b\end{pmatrix} \to \begin{pmatrix}1 & 1 & 1 & a\\ 0 & -2 & -1 & b-1\end{pmatrix} \to$$
$$\begin{pmatrix}1 & 1 & 1 & a\\ 1 & 1 & \frac{1}{2} & \frac{a-b}{2}\end{pmatrix} \to \begin{pmatrix}1 & 0 & \frac{1}{2} & \frac{a+b}{2}\\ 0 & 1 & \frac{1}{2} & \frac{a-b}{2}\end{pmatrix}$$

Che forma il seguente sistema:

$$\begin{cases} x_1 = \frac{a+b}{2} + \frac{1}{2}t\\ x_2 = \frac{a-b}{2} + \frac{1}{2}t\\ x_3 = t\end{cases}$$

Vettori linearmente indipendenti e linearmente dipendenti

Definzione - Vettori linearmente indipendenti

I **vettori** $v_1, ..., v_n$ si dicono **linearmente indipendenti** se

$$\alpha_1 v_1 + ... + \alpha_n v_n = 0_V \Rightarrow \alpha_1 = \alpha_2 = ... = \alpha_k = 0_{\mathbb{K}}$$

In altri termini, l'unica combinazione lineare che esprime 0_V in termini di $v_1, ..., v_n$ è quella **banale** (ovvero $\alpha_1 = \alpha_2 = ... = \alpha_k = 0_{\mathbb{K}}$)

Definizione - Vettori linearmente dipendenti

I **vettori** $v_1, ..., v_n$ sono **linearmente dipendenti** se non sono linearmente indipendenti, ovvero se **esistono scalari non tutti nulli** $\alpha_1, ..., \alpha_n$ tali che $\alpha_1 + v_1 + ... + \alpha_n v_n = 0_v$.

Osservazioni facili:

1. Se un insieme di vettori **contiene il vettore nullo** è **linearmente dipendente**.
   Supponiamo che sia il primo $\{v_1 = 0, v_2, ..., v_k\}$. Allora posso scrivere:

$$\underbrace{1 \cdot v_1}_{=0} + 0_{\mathbb{K}} v_2 + ... + 0_{\mathbb{K}} v_k = 0_{\mathbb{K}}$$

2. Se un insieme di vettori **contiene due vettori proporzionali** allora è **linearmente dipendente**.
   Supponiamo di avere $\{v_1, v_2 = \alpha v_1, v_3, ..., v_k\}$. Allora posso prendere:

$$-\alpha v_1 + \underbrace{1 v_2}_{\alpha v_1} + 0 v_3 + ... + 0 v_k = 0$$

3. Se $\{v_1, ..., v_k\}$ sono **linearmente dipendenti**, anche $\{v_1, ..., v_k, v_{k+1}, ..., v_n\}$ sono **linearmente dipendenti**. (esercizio)

Proposizione

$v_1, ..., v_k$ sono **linearmente dipendenti** se e solo se **uno di essi è combinazione lineare degli altri**.

Dimostrazione: supponiamo $v_1, ..., v_k$ sono **linearmente dipendenti**. Allora esistono scalari non tutti nulli $\alpha_1, ..., \alpha_k$ tali che $\alpha_1 v_1 + ... + \alpha_k v_k = 0$.
Sia $\alpha_i \neq 0$:

$$\alpha_i v_i = -\alpha_1 v_1 ... - \alpha_{i-1} v_{i-1} - \alpha_{i+1} v_{i+1} ... - \alpha_k v_k$$
$$v_i = -\frac{\alpha_1}{\alpha_i} v_1 ... - \frac{\alpha_{i-1}}{\alpha_i} v_{i-1} - \frac{\alpha_{i+1}}{\alpha_i} v_{i+1} ... - \frac{\alpha_k}{\alpha_i} v_k$$

quindi $v_i \in \mathrm{Span}(v_1, ..., v_{i-1}, v_{i+1}, ..., v_k)$ $(*)$.

Viceversa supponiamo che valga $(*)$. Allora

$$v_i = \beta_1 v_1 + ... + \beta_{i-1} v_{i-1} + \beta i + 1 v_{i+1} + ... + \beta_k v_k$$
$$\beta_1 v_1 + ... + \beta_{i-1} v_{i-1} - v_i + \beta i + 1 v_{i+1} + ... + \beta_k v_k = 0$$

gli scalari di questa combinazione linerare sono $\beta_1, ..., \beta_{i-1}, -1, \beta_{i+1}, ..., \beta_k$, quindi **non sono tutti nulli**, pertanto $v_1, ..., v_k$ sono linearmente dipendenti.

Proposizione

Se $v_1, ..., v_k$ sono **linearmente dipendenti**, allora

$$\alpha_1 v_1 + ... + \alpha_k v_k = \beta_1 v_1 + ... + \beta_k v_k \; (\blacksquare)$$

implica $\alpha_1 = \beta_1, \alpha_2 = \beta_2, ..., \alpha_k = \beta_k$.

Dimostrazione: La (■) so riscrive

$$(\alpha_1 - \beta_1)v_1 + ... + (\alpha_k - \beta_k)v_k = 0$$

Poichè $v_1, ..., v_k$ sono **linearmente indipendenti**, risulta

$$\alpha_1 - \beta_1 = \alpha_2 - \beta_2 = ... = \alpha_k - \beta_k = 0$$

da cui $\alpha_1 = \beta_1, \alpha_2 = \beta_2, ..., \alpha_k = \beta_k$.

Definizione

Un sottoinsieme $S \subset V$ si dice **indipendente** se ogni **sottoinsieme finito** è composto da **vettori linearmente indipendenti**.

Definizione - Base di uno spazio vettoriale

Una **base** di uno **spazio vettoriale** V è un **insieme indipendente di generatori**.

Teorema - Ogni spazio vettoriale ammette base

Ogni **spazio vettoriale** ammette **una base**.

> ⚠️ Faremo vedere che se V è **finitamente generato** da un **sistema finito di generatori** si può estrarre una base; inoltre dimostreremo che **tutte le basi** hanno lo **stesso numero di elementi**, che sarà detto **dimensione** dello spazio vettoriale.

Proposizione

Sia V uno **spazio vettoriale finitamente generato**. $\{v_1, ..., v_n\}$ è una base di V se e solo se ogni vettore di V si scrive **in modo unico** come combinazione lineare di $v_1, ..., v_n$.

Dimostrazione: se $\{v_1, ..., v_n\}$ è una base e $v \in V$, risulta $v \in \mathrm{Span}(v_1, ..., v_n)$ perché $\{v_1, ..., v_n\}$ è un **insieme di generatori**; inoltre, per la proposizione precedente, essendo $v_1, ..., v_n$ **linearmente indipendenti**

$$x_1v_1 + ... + x_nv_n = y_1v_1 + ... + y_nv_n \Rightarrow x_i = y_i \ \forall i$$

Viceversa se $\{v_1, ..., v_n\}$ ha le **proprietà descritte nell'enunciato**, è chiaro che $\mathrm{Span}(v_1, ..., v_n) = V$. Facciamo vedere che $v_1, ..., v_n$ sono **linearmente indipendenti**

$$\begin{gathered}\alpha_1 v_1 + ... + \alpha_n v_n = 0_V \\ 0 \cdot v_1 + ... + 0 \cdot v_n = 0_V\end{gathered}$$

Poichè la scrittura di ogni vettore come combinazione lineare di $v_1, ..., v_n$ è **unica**, deduciamo $\alpha_1 = 0, ..., \alpha_n = 0$.

Osservazione: fissata la base $B = \{v_1, ..., v_n\}$ di V, ogni vettore v si scive in modo unico come $v = x_1 v_1 + ... + x_n v_n$.
Quindi è ben definita una funzione $F : V \to \mathbb{K}^n$

$$F(v) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \leftarrow \text{vettore delle coordinate di } V \text{ rispetto a } B$$

Esempio: $V = \mathbb{R}^2,\ B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\},\ \overline{B} = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$

$$F_B \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \end{pmatrix} \qquad F_{\overline{B}} \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\begin{pmatrix} 5 \\ 3 \end{pmatrix} = 5 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 3 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 5 \\ 3 \end{pmatrix} = 4 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Osservazioni

Gli esempi di insiemi di genertori visiti nei casi $1. \to 5.$ sono in realtà basi per gli spazi in questione.

1. $V = \mathbb{K}^n$, $\{e_1, ..., e_n\}$ sono **linearmente dipendenti** quindi sono una **base** e $\dim \mathbb{K}^n = n$.

   Suppongo $x_1 e_1 + ... + x_n e_n = 0$.
   Devo vedere che $x_1 = x_2 = ... = x_n = 0$.

$$x_1 e_1 + ... + x_n e_n = 0 \to x_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + ... + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Quindi $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow x_i = 0 \; \forall i$.

2. $V = M_{mn}(\mathbb{K}),\ \{e_{ij} | 1 \leq i \leq m,\ 1 \leq j \leq n\}$ sono **linearmente indipendenti**, quindi $\dim V = m \cdot n$ (in particolare $\dim M_n = n^2$)

$$\sum_{i,j} a_{ij} e_{ij} = 0$$

quindi

$$\begin{pmatrix} a_{11} & ... & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & ... & a_{mn} \end{pmatrix} = \begin{pmatrix} 0 & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & ... & 0 \end{pmatrix}$$

5. $\{1, t, ..., t^d\}$ sono una base di $\mathbb{K}_d[t]$, dunque $\dim \mathbb{K}_d[t] = d + 1$

$$a_0 \cdot 1 + a_1 t + ... + a_d t^d = 0_{\mathbb{K}[t]}$$
$$\Rightarrow a_0 = a_1 = ... = a_d = 0$$

4. $\dim S_2^+ = 3 \qquad \dim S_2^- = 1$.

Lezione 25 - 28/11/2022

Proposizione - Base insieme massimale di vettori linearmente indipendenti

Se $B = \{v_1, ..., v_n\}$ è una **base** dello **spazio vettoriale** V, allora B è un **insieme massimale** di vettori **linearmente indipendenti**.

Dimostrazione: devo verificare che per ogni $v \in V$ $v, v_1, ..., v_n$ sono **linearmente dipendenti**. Poiché B è una base, è in particolare un **insieme di generatori**, dunque esistono **scalari** $\alpha_1, ..., \alpha_n$ tali che

$$v = \alpha_1 v_1 + ... + \alpha_n v_n$$

Pertanto $\{v, v_1, ..., v_n\}$ sono **linearmente dipendenti**.

Lemma

Sia B un **sottoinsieme finito** dello **spazio vettoriale** V. Se $\text{Span } B$ contiene un sistema di generatori per V, allora $V = \text{Span } B$, cioè B è **esso stesso un insieme di generatori**.

Dimostrazione: sia $A \subset \text{Span } B$ tale che $\text{Span } A = V$. Sia $A = \{w_1, ..., w_s\}$ allora ogni $v \in V$ è del tipo

$$v = \sum_{i=1}^{s} a_i w_i$$

Ma $A \subset \text{Span } B$, per cui se $B = \{v_1, ..., v_r\}$,

$$w_i = \sum_{j=1}^{r} b_{ij} v_j$$

e dunque

$$v = \sum_{i=1}^{s} a_i w_i = \sum_{i=1}^{s} \sum_{j=1}^{r} a_i b_{ij} v_j$$

Proposizione

Sia $A = \{v_1, ...v_k\}$ un **insieme di generatori** per lo **spazio vettoriale** V. Sia $B \subseteq A$ un **insieme massimale di vettori linearmente indipendenti**. Allora B è una **base** di V.

Corollario

Se V è **finitamente generato**, allora **esiste una base** di V.

Dimostrazione: a meno di cambiare l'ordine dei vettori, possiamo assumere che $B = \{v_1, ..., v_r\}, r \leq k$ (ovvero i primi r vettori di A). Basta vedere che $\text{Span } B = V$. Per il **lemma**, basta vedere che $A \subseteq \text{Span } B$.
Sia $w \in A$, che possiamo assumere **non** in B. Per **massimalità**, $w, v_1, .., v_r$ sono **linearmente dipendenti**, quindi esistono **scalari non tutti nulli** $\alpha, \alpha_1, ..., \alpha_r$ tali che

$$\alpha w + \alpha_1 v_1 + ... + \alpha_r v_r = 0$$

Se $\alpha = 0$, si ha $\alpha_1 v_1 + ... + \alpha_r v_r = 0$ che implica $\alpha_1 = ... = \alpha_r = 0$ per l'**indipendenza lineare** dei $v_1, ..., v_r$. Ma questo non è possibile, quindi $\alpha \neq 0$ e

$$w = -\frac{\alpha_1}{\alpha} v_1 ... - \frac{\alpha_r}{\alpha} v_r \in \text{Span } B$$

come volevamo.

Costruzione di una base

Sia $A = \{v_1, ..., v_r\}$ e $\text{Span } A = V$.

Se $V = 0$ allora OK.

Se $V \neq 0$ allora $\exists v_i \in A, v_i \neq 0$. Se $\{v_i, v_j\}$ sono **linearmente dipendenti** $\forall j$, $\{v_j\}$ è una **base**. Altrimenti esiste $v_j \in A$ tale che $\{v_i, v_j\}$ è **linearmente dipendente**. Se $\{v_i, v_j, v_k\}$ sono **linearmente dipendenti** $\forall k$ allora $\{v_i, v_j\}$ è una **base**. E così via.

> ⚠️ N.B.: Sia $A = \{v_1, ..., v_n\}$ un **insieme di generatori**. Se sono **linearmente indipendenti**, sono una base. Altrimenti sono **linearmente dipendenti** ed esiste v_i tale che $v_i \in \text{Span}(v_1, ..., v_{i-1}, v_{i+1}, ..., v_n)$. Ma $\text{Span}(v_1, ..., v_n) = \text{Span}(v_1, ..., v_{i-1}, v_{i+1}, ..., v_n)$. Se ora $v_1, ..., v_{i-1}, v_{i+1}, ..., v_n$ sono **linearmente indipendenti**, sono una **base**. Altrimenti esiste $v_j = \text{Span}(v_1, .., v_{i-1}, v_{i+1}, ..., v_{j-1}, v_{j+1}, ..., v_n)$ e così via.

Teorema - Teorema del completamento a base

Sia $B = \{v_1, ..., v_n\}$ una **base** di uno **spazio vettoriale** V e siano $w_1, ..., w_p,\ p \leq n$ vettori **linearmente indipendenti**. Allora esistono $n - p$ vettori di B che insieme a $w_1, ..., w_p$ formano una base di V.

Dimostrazione: procediamo per **induzione** su p.
Sia $p = 1$. Poiché $v_1, ..., v_n$ è una base di V, esistono **scalari** $\alpha_1, ..., \alpha_n$ tali che

$$w_1 = \alpha_1 v_1 + ... + \alpha_n v_n \quad (*)$$

Per ipotesi $\{w_1\}$ è **indipendente**, cioè $w_1 \neq 0$, quindi gli α_i **non sono tutti nulli** e possiamo assumere $\alpha_1 \neq 0$, quindi

$$v_1 = \frac{1}{\alpha_1} w_1 - \frac{\alpha_2}{\alpha_1} v_2 - \frac{\alpha_3}{\alpha_1} v_3 ... - \frac{\alpha_n}{\alpha_1} v_n$$

Dunque $B \subset \text{Span}(w_1, v_2, ..., v_n)$. Per il **lemma**, $\{w_1, v_2, ..., v_n\}$ è un **insieme di generatori**. Dimostriamo che sono **linearmente indipendenti**. Sia

$$\beta_1 w_1 + \beta_2 w_2 + ... + \beta_n v_n = 0$$

Dobbiamo dimostrare che $\beta_1 = \beta_2 = ... = \beta_n = 0$. Per faremo usiamo $(*)$. Otteniamo

$$\beta_1(\alpha_1 v_1 + ... + \alpha_n v_n) + \beta_2 v_2 + ... + \beta_n v_n = 0$$
$$\beta_1 \alpha_1 v_1 + (\beta_1 \alpha_1 + \beta_2) v_2 + ... + (\beta_1 \alpha_n + \beta_n) v_n = 0$$

Ma $\{v_1, ..., v_n\}$ è un insieme **linearmente indipendente**, quindi

$$\begin{cases} \beta_1 = 0 \\ \beta_1 \alpha_2 + \beta_2 = 0 \\ \vdots \\ \beta_1 \alpha_n + \beta_n = 0 \end{cases} \qquad \begin{cases} \beta_1 = 0 \\ \beta_2 = 0 \\ \vdots \\ \beta_n = 0 \end{cases}$$

Supponiamo ora la **tesi vera** per $p - 1$ vettori e dimostriamola per p vettori.

Per **ipotesi induttiva**, possiamo trovare $n - (p - 1) = n - p + 1$ vettori, che a meno di cambiare nome possiamo assumere essere $v_p, ..., v_n$, tali che

$$\{w_1, ..., w_{p-1}, v_p, ..., v_n\}$$

è una **base** di V. Come prima

$$w_p = \alpha_1 w_1 + ... + \alpha_{p-1} w_{p-1} + \alpha_p v_p + ... + \alpha_n v_n$$

Gli α_i con $p \leq i \leq n$ **non sono tutti nulli**, altrimenti troveremo una relazione di **dipendenza** tra $w_1, ..., w_p$. Supponiamo allora $\alpha_p \neq 0$ e scriviamo

$$v_p = \frac{1}{\alpha_p} w_p - \frac{\alpha_1}{\alpha_p} w_1 ... - \frac{\alpha_{p-1}}{\alpha_p} w_{p-1} - \frac{\alpha_{p+1}}{\alpha_p} v_{p+1} ... - \frac{\alpha_n}{\alpha_p} v_n$$

Dunque $v_p \in \mathrm{Span}(w_s, ..., w_p, v_{p+1}, ..., v_n)$, pertanto tali vettori sono un insieme di **generatori**. Per provare l'**indipendenza lineare**, scriviamo

$$\beta_1 w_1 + ... + \beta_p w_p + \beta_{p+1} v_{p+1} + ... + \beta_n v_n = 0$$

dove $w_p = \alpha_p v_p + \alpha_1 w_1 + ... + \alpha_{p-1} w_{p-1} + \alpha_{p+1} v_{p+1} + ... + \alpha_n v_n$. Quindi

$$\begin{aligned} &(\beta_1 + \beta_p \alpha_1) w_1 + ... + (\beta_{p-1} + \beta_p \alpha_{p-1}) w_{p-1} + \beta_p \alpha_p v_p \\ &\qquad + (\beta_{p+1} + \beta_p \alpha_{p+1}) v_{p+1} + ... + (\beta_n + \beta_p \alpha_n) v_m n = 0 \end{aligned}$$

Per ipotesi induttiva $w_1, ..., w_{p-1}, v_p, v_{p+1}, ..., v_n$ sono una base di V, pertanto

$$\begin{cases} \beta_1 + \beta_p \alpha_1 = 0 \\ \vdots \\ \beta_{p-1} + \beta_p \alpha_{p-1} = 0 \\ \beta_p \alpha_p = 0 \overset{\alpha_p \neq 0}{\Rightarrow} \beta_p = 0 \\ \vdots \\ \beta_n + \beta_p \alpha_n = 0 \end{cases} \quad \text{Risostituendo} \quad \begin{cases} \beta_1 = 0 \\ \vdots \\ \beta_{p-1} = 0 \\ \beta_p = 0 \\ \vdots \\ \beta_n = 0 \end{cases}$$

Teorema

Se V è uno **spazio vettoriale** finitamente generato, due qualsiasi basi hanno lo **stesso numero di elementi**.

Definizione - Dimensione

Il **numero di elementi** di una qualsiasi **base** di uno **spazio vettoriale** V **finitamente generato** si chiama **dimensione** di V e si denota con $\dim V$.

Dimostrazione (Teorema): Siano B_1, B_2 due **basi** di V, con $|B_1| = h, |B_2| = k$. Se per assurdo $h > k$, il **teorema** dice che esistono $h - k$ vettori di B_1 che aggiunti a B_2 danno una base. Ma B_2 è **già una base**, quindi un **insieme massimale** di vettori linearmente indipendenti.

Corollari

1. Se $\dim V = n$, n **vettori indipendenti** sono una base.
2. Se $\dim V = n$, n generatori sono una base.
3. Se $\dim V = n$, $w_1, ..., w_p \in V$. Se $p > n, w_1, ..., w_p$ sono **linearmente dipendenti**.

Osservazione

La notazione di **dipendenza** e **indipendenza lineare** dipende in modo **essenziale** da $\mathbb{K}$. In effetti è più corretto scrivere che i vettori $v_1, ..., v_n$ sono **linearmente indipendenti su** $\mathbb{K}$ se

$$\alpha_1 v_1 + ... + \alpha_n v_n = 0 \Rightarrow \alpha_1 = ... = \alpha_n = 0 \quad (\alpha_i \in \mathbb{K})$$

In particolare la **dimensione** di V dipende da $\mathbb{K}$ ed è più corretto scriverle come $\dim_{\mathbb{K}} V$.

Esempio:

- $V = \mathbb{C},\ \mathbb{K} = \mathbb{C}$. Una **base** può essere data da $\{1\}$:

$$\underbrace{z}_{\text{vettore}} = \underbrace{z}_{\text{scalare}} \cdot \underbrace{1}_{\text{vettore}}$$

- $V = \mathbb{C},\ \mathbb{K} = \mathbb{R}$. Una **base** di $\mathbb{C}$ su $\mathbb{R}$ è data da $\{1, i\}$:

$$z = \underbrace{a}_{\text{scalare reale}} \cdot \underbrace{1}_{\text{vettore}} + \underbrace{b}_{\text{scalare reale}} \cdot \underbrace{i}_{\text{vettore}}$$

  Si ha: $\dim_{\mathbb{C}} \mathbb{C} = 1,\ \dim_{\mathbb{R}} \mathbb{C} = 2$.

Similarmente $\dim_{\mathbb{C}} M_2(\mathbb{C}) = 4,\ \dim_{\mathbb{R}} M_2(\mathbb{C}) = 8$:

- Su $\mathbb{C}$

$$\begin{pmatrix} i & 2 \\ 3 & 4i \end{pmatrix} = i \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + 3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + 4i \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- Su $\mathbb{R}$

$$\begin{pmatrix} i & 2 \\ 3 & 4i \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix} + 2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + 3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + 4 \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix}$$

$$\begin{pmatrix} a + ib & * \\ * & * \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix} + ...$$

Lezione 26 - 01/12/2022

Ricordiamo il vettore delle coordinate

Ricordiamo che se V è uno **spazio vettoriale** di **dimensione** n su $\mathbb{K}$ e $B = \{v_1, ..., v_n\}$ è una **base** di V, ogni vettore di V si scrive in modo **unico** come

$$v = x_1 v_1 + x_2 v_2 + ... + x_n v_n \quad x_i \in \mathbb{K}$$

e pertanto è definita una funzione

$$\begin{aligned} \phi_B &: V \to \mathbb{K}^n \\ v \mapsto (v)_B &= \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \leftarrow \text{Vettore delle coordinate di } V \text{rispetto a } B \end{aligned}$$

Definizione - Applicazione lineare

Siano V, V' **spazi vettoriali** su $\mathbb{K}$. Un'**applicazione lineare** (o omomorfismo di spazi vettoriali) da V a V' è un'**applicazione** $F : V \to V'$ tale che

$$F(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 F(v_1) + \alpha_2 F(v_2) \quad \begin{aligned} &\forall v_1, v_2 \in V \\ &\forall \alpha_1, \alpha_2 \in \mathbb{K} \end{aligned}$$

Diciamo che F è un **isomorfismo** se F è **biunivoca**.

Esempio: $\phi_B : V \to \mathbb{K}^n$ è un **isomorfismo**. Abbiamo già visto che è biunivoca.
Se $v = \alpha_1 v_1 + ... + \alpha_n v_n$ e $w = \beta_1 v_1 + ... + \beta_n v_n$

$$\begin{aligned} \alpha v + \beta w &= \alpha(\alpha_1 v_1 + ... + \alpha_n v_n) + \beta(\beta_1 v_1 + ... + \beta_n v_n) = \\ &= (\alpha\alpha_1 + \beta\beta_1) v_1 + ... + (\alpha\alpha_n + \beta\beta_n) v_n \end{aligned}$$

$$\begin{aligned}\phi_B(\alpha v+\beta w) &= (\alpha v+\beta w)_B = \\ &= \begin{pmatrix}\alpha\alpha_1+\beta\beta_1\\ \alpha\alpha_2+\beta\beta_2\\ \vdots\\ \alpha\alpha_n+\beta\beta_n\end{pmatrix} = \\ &= \alpha\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}+\beta\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix} = \alpha\phi_B(v)+\beta\phi_B(w)\end{aligned}$$

Trovare basi

$U \underbrace{\subseteq}_{\text{sottospazio}} \mathbb{K}^n,\ U=\mathrm{Span}(v_1,...,v_k)$. Come trovo una **base** di U?

- 1° metodo:

  $$\begin{pmatrix}v_1\\ \vdots\\ v_k\end{pmatrix} \overset{\text{riduzione}}{\rightsquigarrow} \begin{pmatrix}v_1'\\ \vdots\\ v_k'\\ 0\\ \vdots\\ 0\end{pmatrix}$$

  Allora $\{v_1',...,v_k'\}$ è una **base** di U. Infatti, le operazioni di riga non cambiano lo Span e abbiamo già dimostrato che le righe non nulle di una matrice a scala sono **linearmente indipendenti**.

  Esempio:

  Sia $U=\mathrm{Span}(\begin{pmatrix}1\\1\\0\\1\end{pmatrix},\begin{pmatrix}3\\1\\-2\\5\end{pmatrix},\begin{pmatrix}1\\0\\-1\\2\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\end{pmatrix})\subseteq\mathbb{R}^4$

  $$\begin{aligned}\begin{pmatrix}1&1&0&1\\3&1&-2&5\\1&0&-1&2\\0&0&1&1\end{pmatrix}&\sim\begin{pmatrix}1&1&0&1\\0&-2&-2&2\\0&-1&-1&1\\0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&0&1\\0&1&1&-1\\0&1&1&-1\\0&0&1&1\end{pmatrix}\\ &\sim\begin{pmatrix}1&1&0&1\\0&1&1&-1\\0&0&0&0\\0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&0&1\\0&1&1&-1\\0&0&1&1\\0&0&0&0\end{pmatrix}\end{aligned}$$

  Una base di U può essere $\left\{\begin{pmatrix}1\\1\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\\-1\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\end{pmatrix}\right\}$

- 2° metodo: Costruisco la matrice A che ha i v_i per colonne e riduco per righe. La base cercata è data dalle **colonne** di A **corrispondenti ai pivot**.

  Rivediamo l'esempio precedente utilizzando questo metodo:

$$\begin{pmatrix} 1 & 3 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & -2 & -1 & 1 \\ 1 & 5 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 1 & 0 \\ 0 & -2 & -1 & 0 \\ 0 & -2 & -1 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 1 & 0 \\ 0 & 1 & \frac{1}{2} & 0 \\ 0 & 1 & \frac{1}{2} & -1 \\ 0 & 1 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 3 & 1 & 0 \\ 0 & 1 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 1 & 0 \\ 0 & 1 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Una base possibile è quindi quella formata dalla **prima**, **seconda** e **quarta** colonna(della matrice originale) in quanto sono le **colonne dei pivot nella matrice in forma a scala**.

Quindi $\left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ -2 \\ 5 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\}$.

In generale, si fissa una base di V e si **lavora con le corrispondenti coordinate**.

Esempio: $V = \mathbb{R}_3[t],\ U = \mathrm{Span}(t + t^2, t + t^3, 2t + t^2 + t^3)$.

Fisso $B = \{1, t, t^2, t^3\}$ come base di V. Allora si ha

$$(p_1)_B = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \quad (p_2)_B = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \quad (p_3)_B = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Una **base** di U è data dai **polinomi** p_4, p_5 le cui coordinate rispetto a B sono

$$\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$$

⚠️ Queste sono le **coordinate**! Quindi l'esercizio non è finito in quanto dobbiamo trovare i **polinomi**.

I polinomi sono:

$$p_4 = 0 \cdot 1 + 1 \cdot t + 1 \cdot t^2 + 0 \cdot t^3 = t + t^2$$
$$p_5 = 0 \cdot 1 + 0 \cdot t + 1 \cdot t^2 + (-1) \cdot t^3 = t^2 - t^3$$

Somma e intersezione di sottospazi

V **spazio vettoriale** su $\mathbb{K}$. U, W **sottospazi** di V.

Proposizione

$U \cap W$ e $U + W = \{u + w | u \in U, w \in W\}$ sono **sottospazi** di V.

Dimostrazione: siano $v_1, v_2 \in U \cap W,\ \alpha_1, \alpha_2 \in \mathbb{K}$.

Devo dimostrare che $\alpha_1 v_1 + \alpha_2 v_2 \in U \cap W$ $(*)$.

Per ipotesi U è un **sottospazio**, quindi, poiché $v_1, v_2 \in U$

$$(1) \quad \alpha_1 v_1 + \alpha_2 v_2 \in U$$

Similarmente, W è **sottospazio**, quindi poiché $v_1, v_2 \in W$

$$(2) \quad \alpha_1 v_1 + \alpha_2 v_2 \in W$$

Mettendo insieme $(1), (2)$ otteniamo $(*)$.

Per dimostrare che $U + W$ è un **sottospazio**, prendiamo $v_1, v_2 \in U + W$ e scalari $\alpha_1, \alpha_2 \in \mathbb{K}$ e mostriamo che

$$\alpha_1 v_1 + \alpha_2 v_2 \in U + W$$

Per **ipotesi**:

$$\begin{aligned} v_1 &= u_1 + w_1 \quad & u_1 \in U, w_1 \in W \\ v_2 &= u_2 + w_2 \quad & u_1 \in U, w_2 \in W \end{aligned}$$

Si ha quindi:

$$\begin{aligned} \alpha_1 v_1 + \alpha_2 v_2 &= \alpha_1(u_1 + w_1) + \alpha_2(u_2 + w_2) = \\ &= \underbrace{\alpha_1 u_1 + \alpha_2 u_2}_{u_3 \in U} + \underbrace{\alpha_1 w_1 + \alpha_2 w_2}_{w_3 \in W} \in U + W \end{aligned}$$

Proposizione

Se $U = \text{Span}(u_1, ..., u_k),\ W = \text{Span}(w_1, ..., w_h)$ allora

$$U + W = \text{Span}(u_1, ..., u_k, w_1, ..., w_h)$$

> ⚠️ N.B.: Non è vero che se $\{u_1, ..., u_k\}$ è una **base** di U, $\{w_1, ..., w_h\}$ è una **base** di W allora $\{u_1, ..., u_k, w_1, ..., w_h\}$ è una **base** di $U + W$: è solo, in generale, un **insieme di generatori**.

Dimostrazione: Dato $x \in U + W,\ x = u + w,\ u \in U,\ w \in W$ con $u = \alpha_1 u_1 + ... + \alpha_k u_k$ e $w = \beta_1 w_1 + ... + \beta_h w_h$

$$y = u + w = \alpha_1 u_1 + ... + \alpha_k u_k + \beta_1 w_1 + ... + \beta_h w_h$$

Teorema - Teorema di Grassmann

Sia V uno **spazio vettoriale** di **dimensione finita** e siano U, W due suoi **sottospazi**. Allora

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Dimostrazione: Sia $\{v_1, ..., v_s\}$ una **base** di $U \cap W$. Posso completarla con vettori $u_{s+1}, ..., u_k$ a una base di U e con vettori $w_{s+1}, ..., w_h$ a una **base** di W ($\dim U \cap W = s, \dim U = k, \dim W = h$).
Dico che $B = \{v_1, ..., v_s, u_{s+1}, ..., u_k, w_{s+1}, ..., w_h\}$ è una **base** di $U + W$. Questo conclude perché, se questo è vero

$$\begin{aligned} \dim U + W &= s + k - s + h - s = k + h - s = \\ &= \dim U + \dim W - \dim(U \cap W) \end{aligned}$$

1. B è un **insieme di generatori** per $U+W$.

   Prendo $v \in U+W$, allora $v = u+w, u \in U, w \in W$

$$\begin{aligned} u =& \alpha_1 v_1 + ... + \alpha_s v_s + \alpha_{s+1} u_{s+1} + ... + \alpha_k u_k \\ w =& \beta_1 v_1 + ... + \beta_s v_s + \beta_{s+1} w_{s+1} + ... + \beta_h w_h \\ u+w =& (\alpha_1 + \beta_1) v_1 + ... + (\alpha_s + \beta_s) v_s + \alpha_{s+1} u_{s+1} + \\ & + \alpha_k u_k + \beta_{s+1} w_{s+1} + ... + \beta_h w_h \end{aligned}$$

2. B è un **insieme indipendente**.

$$x_1 v_1 + ... + x_s v_s + y_{s+1} u_1 + ... + y_k u_k + z_{s+1} w_1 + ... + z_h w_h = 0$$

   Questo mi dice che il vettore:

$$(*)\ \underbrace{a = x_1 v_1 + ... + x_s v_s + y_{s+1} u_1 + ... + y_k u_k}_{a \in V} = \underbrace{-z_{s+1} w_1 ... - z_h w_h}_{a \in W}$$

   Questo implica proprio che $a \in U \cap W$. Inoltre

$$\begin{aligned} & a = x_1 v_1 + ... + x_s v_s + y_{s+1} u_1 + ... + y_k u_k \\ & \Rightarrow y_{s+1} = ... = y_k = 0 \end{aligned}$$

   Allora $(*)$ diviene $x_1 v_1 + ... + x_s v_s = -z_{s+1} w_1 ... - z_h w_h$ il che significa

$$x_1 v_1 + ... + x_s v_s + z_{s+1} w_1 + ... + z_h w_h = 0$$

   Ma $\{v_1, ..., v_s, w_{s+1}, ..., w_h\}$ sono una **base** di W quindi

$$x_1 = ... = x_s = z_{s+1} = ... = z_h = 0$$

Esercizio

Siano

- $U = \left\{ \underline{x} \in \mathbb{R}^4 \mid \begin{cases} x_1 + x_2 = 0 \\ x_3 - x_4 = 0 \end{cases} \right\}$
- $W = \left\{ \underline{x} \in \mathbb{R}^4 \mid \begin{cases} x_1 + x_2 + x_3 - x_4 = 0 \\ x_1 - x_3 + 2x_4 = 0 \end{cases} \right\}$

Trovare basi per $U, W, U \cap W$.

- Base per U

  Il sistema sotto forma di matrice è già in forma a gradini, quindi risolviamo semplicemente il sistema.

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} \to \begin{cases} x_1 = -x_2 \\ x_3 = x_4 \end{cases} \to \begin{cases} x_1 = -t \\ x_2 = t \\ x_3 = s \\ x_4 = s \end{cases}$$

  Quindi

$$\begin{pmatrix} -t \\ t \\ s \\ s \end{pmatrix} = t \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + s \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Una **base** di U è $\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\}$.

- Base per W

  Rendiamo la matrice associata al sistema in forma a gradini

$$\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 0 & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & -1 & -2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & 1 & 2 & -3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 2 & -3 \end{pmatrix}$$

  Risolviamo ora il sistema:

$$\begin{cases} x_1 = x_3 - 2x_4 \\ x_2 = -2x_3 + 3x_4 \end{cases} \quad \begin{cases} x_1 = t - 2s \\ x_2 = -2t + 3s \\ x_3 = t \\ x_4 = s \end{cases} \to t \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} -2 \\ 3 \\ 0 \\ 1 \end{pmatrix}$$

  Una **base** per W è $\left\{ \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 3 \\ 0 \\ 1 \end{pmatrix} \right\}$.

- Base per $U \cap W$

  $U \cap W$ è descritto dal seguente sistema:

$$\begin{cases} x_1 + x_2 = 0 \\ x_3 - x_4 = 0 \\ x_1 + x_2 + x_3 - x_4 = 0 \\ x_1 - x_3 + 2x_4 = 0 \end{cases}$$

  Portiamo ora la matrice associata in forma a gradini:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 1 & -2 \\ 1 & 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & -2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

  E risolviamo il sistema:

$$\begin{cases} x_1 = -x_4 \\ x_2 = x_4 \\ x_3 = x_4 \end{cases} \quad \begin{cases} x_1 = -t \\ x_2 = t \\ x_3 = t \\ x_4 = t \end{cases} \quad U = \mathrm{Span} \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Equazioni cartesiane

Sia U un **sottospazio** di $\mathbb{K}^n$. Diciamo che U è descritto da **equazioni cartesiane** se

$$U = \{x \in \mathbb{K}^n \mid AX = 0\}$$

per qualche matrice $A \in M_{mn}(\mathbb{K})$.

Trovare equazioni cartesiane

Se U è assegnato tramite una sua base $\{u_1, ..., u_k\}$ basta imporre che

$$\operatorname{rk}\begin{pmatrix} u_1 \\ \vdots \\ u_k \\ x_1 \dots x_n \end{pmatrix} = k$$

> ℹ️ Ricordiamo che rk indica il **rango** della matrice.

Esempi:

1. Sia $U = \operatorname{Span}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}\right)$ con $\dim U = 2$.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ x_1 & x_2 & x_3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & x_1 - x_2 & x_3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & x_3 + x_2 - x_1 \end{pmatrix}$$

   Il **rango** è 2 se e solo se $x_3 + x_2 - x_1 = 0$. $U = \{\underline{x} \in \mathbb{R}^3 | \ x_3 + x_2 - x_1 = 0\}$.

2. Sia $U = \operatorname{Span}\left(\begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}\right\}$

$$\begin{pmatrix} 1 & 2 & 1 \\ x_1 & x_2 & x_3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & x_2 - 2x_1 & x_3 - x_1 \end{pmatrix}$$

   Quindi $\begin{cases} x_2 - 2x_1 = 0 \\ x_3 - x_1 = 0 \end{cases}$.

3. Sia $U = \operatorname{Span}\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \end{pmatrix}\right) \subseteq \mathbb{R}^4$

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & x_2 & x_3 - x_1 & x_3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & x_3 - x_1 - x_2 & x_4 + x_2 \end{pmatrix}$$

   Quindi $\begin{cases} x_3 - x_1 - x_2 = 0 \\ x_3 + x_2 = 0 \end{cases}$.

Definizione - Somma diretta

Siano U, W **sottospazi** dello **spazio vettoriale** V. Diciamo che la somma $U + W$ è **diretta** (notazione $U \oplus W$) se $U \cap W = \{0\}$.

Osservazioni:

1. Dalla formula di **Grassmann**:

$$\dim U \oplus W = \dim U + \dim W$$

   In questo caso (e solo in questo!) l'unione di una base di U e l'unione di una base di W è una base di $U + W$.

2. In $U \oplus W$, ogni vettore di $U + W$ si scrive in **modo unico** come $u + w, u \in U, w \in W$

   Infatti, se

$$u + w = u' + w' \quad \begin{aligned} u, u' \in U \\ w, w' \in W \end{aligned}$$

   Si ha che

$$u - u' = w - w' \in U \cap W = \{0\}$$
$$\Rightarrow u = u' \text{ e } w = w'$$

Proposizione

Sia V uno **spazio vettoriale**, U un **sottospazio** di V. Esiste un **sottospazio** U di V tale che

$$V = U \oplus U'$$

> ⚠️ U' prende il nome di **complementare**.

Dimostrazione: sia $\{u_1, ..., u_k\}$ una base di U. **Copletiamola** con vettori $\{u'_1, ..., u'_h\}$ a una base di V. Posto

$$U' = \text{Span}(u'_1, ..., u'_h)$$

risulta $V = U \oplus U'$.

Come si completa un insieme indipendente a una base

Sia $\{u_1, ..., u_k\}$ un **insieme indipendente di vettori** di $\mathbb{K}^n$. Allora la matrice A che ha $u_1, ..., u_k$ per **righe** ha esattamente k **pivot**. Per completare $u_1, ..., u_k$ a una base basta **ridurre a scala** A e aggiungere a $u_1, ..., u_k$ gli $n - k$ **vettori** della **base canonica non** corrispondenti a pivot.

Esempio:

$$\begin{matrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{matrix} \end{matrix}$$

> ⚠️ I due vettori al di fuori delle parentesi sono quelli che sono stati aggiunti e sono e_2 ed e_4 mentre i primi 3 vettori sono rispettivamente u_1, u_2 e u_3.

$\{u_1, u_2, u_3, e_2, e_4\}$ è una **base** di $\mathbb{R}^5$.

Osservazione: Per dimostrare che $V = U \oplus W$ si deve far vedere che

1. $V = U + W$
2. $U \cap W = \{0\}$

Definizione

Sia V uno **spazio vettoriale** e $U_1, ..., U_s$ siano **sottospazi** di V. Diciamo che V è **somma diretta** di $U_1, ..., U_s$

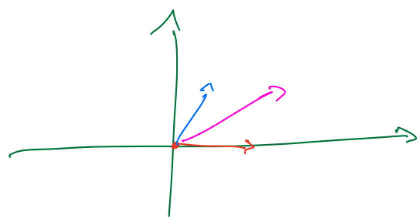
$$V = U_1 \oplus ... \oplus U_s$$

se ogni vettore $v \in V$ si scrive in modo unico come

$$v = u_1 + ... + u_s \quad u_i \in U_i \quad 1 \leq i \leq s$$

Osservazioni:

1. $\{u_1, ..., u_s\}$ è una base di $U \iff U = \mathbb{K}_{u_1} \oplus \mathbb{K}_{u_2} \oplus ... \oplus \mathbb{K}_{u_s}$
2. I **complementari** non sono unici!



$$U \oplus U' = U \oplus U''$$
$$\not\Rightarrow U' = U''$$

Lezione 27 - 02/12/2022

Definizione - Funzione lineare

Siano U, W **spazi vettoriali**. Una funzione $f : V \to W$ è **lineare** se

$$f(\alpha v + \beta v') = \alpha f(v) + \beta f(v') \quad \begin{array}{l} \forall \alpha, \beta \in \mathbb{K} \\ \forall v, v' \in V \end{array}$$

Osservazioni:

1. Notiamo che f è in particolare un **omomorfismo di gruppi**, quindi necessariamente

$$f(0_V) = 0_W$$

Dunque se $f(0_v) \neq 0_W$, f **non è lineare**.
Però $f : \mathbb{R} \to \mathbb{R}$ con $f(x) = x^2$ è tale che $f(0) = 0$, ma non è lineare, infatti:

$$\begin{aligned} f(1+1) = f(2) = 4 \\ f(1) + f(1) = 1 + 1 = 2 \end{aligned}$$

2. $f : \mathbb{K}^m \to \mathbb{K}^n$ è lineare se e solo se

$$f \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} p_1(\underline{x}) \\ \vdots \\ p_n(\underline{x}) \end{pmatrix}$$

ove i $p_i(\underline{x})$ sono **polinomi omogenei di primo grado** in $x_1, ..., x_m$ con **termine noto nullo**.

Esempi:

- Esempio valido:

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + 5x_2 \\ x_2 + 4x_3 - x_1 \\ x_3 \\ x_3 + 2x_2 \end{pmatrix} \qquad \mathbb{R}^3 \to \mathbb{R}^4$$

  L'esempio è valido in quanto sono tutti **polinomi omogenei di grado 1.**

- **Esempio non valido**:

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 x_2 \\ x_1 \\ x_3 \end{pmatrix}$$

  Non è valido in quanto $x_1 x_2$ non è un polinomio di primo grado.

<u>Esempi</u>:

1. Sia $A \in M_{mn}(\mathbb{K})$ e $L_A : \mathbb{K}^n \to \mathbb{K}^m$

$$L_A(X) = AX$$

   è lineare:

$$L_A(\alpha X + \beta Y) = A(\alpha X + \beta Y) = \alpha AX + \beta AY = \alpha L_A(X) + \beta L_A(Y)$$

2. Sia $V = \mathbb{K}[t]$ e $F(p(t)) = p'(t)$ (derivata)

$$(\alpha p(t) + \beta q(t)) = \alpha p'(t) + \beta q'(t)$$

Nomenclatura - Operatore lineare

Un'applicazione lineare $V \to V$ è chiamata **operatore lineare**:

$$\begin{aligned} \mathrm{Hom}(V, W) &= \{f : V \to W | f \text{ è lineare}\} \\ \mathrm{End}(V) &= \mathrm{Hom}(V, V) \end{aligned}$$

⚠️ End sta per **endomorfismi**.

<u>Osservazione</u>: $\mathrm{Hom}(V, W)$ è a sua volta un **sottospazio vettoriale**. Infatti ponendo

$$
\begin{array}{ll}
(f+g)(v) = f(v) + g(v) & f, g \in \mathrm{Hom}(V, W) \\
(\alpha f)(v) = \alpha f(v) & \alpha \in \mathbb{K}
\end{array}
$$

si dota $\mathrm{Hom}(V, W)$ di una **struttura di spazio vettoriale**.
Bisogna verificare che $f + g, \alpha f$ **sono lineari** (esercizio).

Ker e Im per le applicazioni lineari

Come nel caso dei gruppo, ad un'applicazione lineare $f : V \to W$ si possono associare due **sottospazi vettoriali**:

$$
\begin{aligned}
\mathrm{Ker}(F) &= \{v \in V \mid f(v) = 0_w\} \\
\mathrm{Im}(f) &= \{w \in W \mid \exists v \in V : f(v) = w\}
\end{aligned}
$$

Esercizio: dimostriamo che $\mathrm{Ker}\ f, \mathrm{Im}\ f$ sono **sottospazi**:

- $\mathrm{Ker}\ f$: siano $v_1, v_2 \in \mathrm{Ker}\ f,\ \alpha_1, \alpha_2 \in \mathbb{K}$.

  Tesi: $\alpha_1 v_1 + \alpha_2 v_2 \in \mathrm{Ker}\ f$

$$
f(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 \underbrace{f(v_1)}_{=0} + \alpha_2 \underbrace{f(v_2)}_{=0} = 0
$$

- $\mathrm{Im}\ f$: siano $w_1, w_2 \in \mathrm{Im}\ f,\ \alpha_1, \alpha_2 \in \mathbb{K}$.

  Ipotesi: $w_1 = f(v_1),\ w_2 = f(v_2)$

  Tesi: $\alpha_1 w_1 + \alpha_2 w_2 \in \mathrm{Im}\ f$

$$
\alpha_1 w_1 + \alpha_2 w_2 = \alpha_1 f(v_1) + \alpha_2 f(v_2) = f(\alpha_1 v_1 + \alpha_2 v_2)
$$

Teorema - Teorema di nullità più rango

Sia V uno **spazio vettoriale di dimensione finita** e $f : V \to W$ un'**applicazione lineare**. Allora

$$
\dim V = \dim \mathrm{Ker}\ f + \dim \mathrm{Im}\ f
$$

Dimostrazione: sia $\{v_1, ..., v_k\}$ una **base** di $\mathrm{Ker}\ f$. Completiamola con vettori $\{v_{k+1}, ..., v_n\}$ a una base di V ($\dim V = n$). Poniamo

$$
w_{k+1} = f(v_{k+1}), ..., w_n = f(v_n)
$$

Dico che $B = \{w_{k+1}, ..., w_n\}$ è una **base** di $\text{Im } f$. Se questi è vero ho concluso perché

$$\dim \text{Im } f = |B| = n - k = \dim V - \dim \text{Ker } f$$

Ora resta da dimostrare che B è un **insieme di generatori per** $\text{Im } f$ e **un insieme indipendente**.

1. B è un **insieme di generatori per** $\text{Im } f$**:**

   $w \in \text{Im } f$**.** Allora $v \in V : f(v) = w$. Ma $\{v_1, ..., v_n\}$ è una base di V, quindi

$$v = \alpha_1 v_1 + ... + \alpha_k v_k + \alpha_{k+1} v_{k+1} + ... + \alpha_n v_n$$
$$w = ...$$

2. B è un **insieme indipendente**

$$\beta_{k+1} w_{k+1} + ... + \beta_n w_n = 0$$
$$\beta_{k+1} f(v_{k+1}) + ... + \beta_n f(v_n) = 0$$
$$f(\beta_{k+1} v_{k+1} + ... + \beta_n v_n) = 0$$
$$\beta_{k+1} v_{k+1} + ... + \beta_n v_n \in \text{Ker } f$$
$$\beta_{k+1} v_{k+1} + ... + \beta_n v_n = \gamma_1 v_1 + ... + \gamma_k v_k$$
$$\gamma_1 v_1 + ... + \gamma_k v_k - \beta_{k+1} v_{k+1} ... - \beta_n v_n = 0$$

   Ma B è una **base** di V, quindi

$$\gamma_1 = ... = \gamma_n = \beta_{k+1} = ... = \beta_n = 0$$

Iniettività e suriettività delle applicazioni lineari

1. $f : V \to W$ lineare è **iniettiva** $\iff \text{Ker } f = \{0\}$
2. $f : V \to W$ lineare è **suriettiva** $\iff \text{Im } f = W$

Dimostrazione di 1.: se $\text{Ker } f = \{0\}$ e $f(v) = f(w)$ allora $f(v) - f(w) = 0$ e $f(v - w) = 0$ cioè $v - w \in \text{Ker } f = \{0\} \Rightarrow v - w = 0 \Rightarrow v = w$.
Viceversa se f è **iniettiva** e $v \in \text{Ker } f$, allora

$$f(v) = 0 = f(0) \Rightarrow v = 0$$

Corollario del teorema di nullità più rango

Sia $f \in \text{Hom}(V, W)$:

1. Se $\dim V > \dim W$, f non può essere **iniettiva**;
2. Se $\dim V < \dim W$, f non può essere **suriettiva**;
3. Se $\dim V = \dim W$, allora f è **iniettiva** se e solo se è **suriettiva**.

Dimostrazioni: $3.$ segue da $1.$ e da $2.$

1. se f è **iniettiva**, $\dim \operatorname{Ker} f = 0$

$$\dim V = \dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim \operatorname{Im} f \leq \dim W$$

   contro l'ipotesi.

2. se f è **suriettiva**, $\dim \operatorname{Im} f = \dim W$

$$\dim V = \dim \operatorname{Ker} f + \dim W \geq \dim W$$

   contro l'ipotesi.

Spazi vettoriali quoziente

Sia V uno **spazio vettoriale** e $W \subset V$ un **sottospazio**. W è un **sottogruppo** di V, normale perché V è abeliano, quindi possiamo considerare il **gruppo quoziente** V/W che dotiamo di una struttura di **spazio vettoriale** ponendo

$$\alpha(x+W) = \alpha x + W$$

La definizione è **ben posta**: se $x+W = y+W$, allora $\alpha x + W = \alpha y + W$. Infatti

$$x+W = y+W \iff x-y \in W$$

$\alpha(x-y) = \alpha x - \alpha y \in W$, cioè $\alpha x + W = \alpha y + W$.

Proposizione

Se V ha **dimensione finita** e W è un **sottospazio** di V, allora

$$\dim V/W = \dim V - \dim W$$

Dimostrazione: sia $\{w_1, ..., w_k\}$ una **base** di W. Completiamola con vettori $u_{k+1}, ..., u_n$ a una base di V. Dico che $\{u_{k+1} + W, ..., u_n + W\}$ è una base di V/W. In effetti questo è un **caso particolare del teorema di nullità più rango** "applicato??" a

$$V \xrightarrow{\pi} V/W$$
$$x \mapsto x + W$$

Teorema - Teorema di omomorfismo per spazi vettoriali

Sia $f : V \to W$ lineare.
Esiste un unico **isomorfismo** $\overline{f} : V/\mathrm{Ker}\ f \to \mathrm{Im}\ f$ tale che, se $\pi : V \to V/\mathrm{Ker}\ f$

$$f = \overline{f} \circ \pi$$

$$\begin{tikzcd}
V \arrow[r, "f"] \arrow[d, "\pi"'] & \mathrm{Im}\, f \subseteq W \\
V/_{\mathrm{Ker}\, f} \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

$\overline{f}(x + \mathrm{Ker}\ f) = f(x)$

$$\begin{aligned}
\overline{f}(\alpha(x + \mathrm{Ker}\ f) + \beta(y + \mathrm{Ker}\ f)) &= \overline{f}(\alpha x + \beta y + \mathrm{Ker}\ f) = \\
&= f(\alpha x + \beta y) = \\
&= \alpha f(x) + \beta f(y) = \\
&= \alpha \overline{f}(x + \mathrm{Ker}\ f) + \beta \overline{f}(y + \mathrm{Ker}\ f)
\end{aligned}$$

Lezione 29 - 12/12/2022

Principio di estensione per linearità

Proposizione

Sia $\{v_1, ..., v_n\}$ una **base** di V e siano $w_1, ..., w_n$ arbitrari **vettori** di W. Allora esiste un'unica **applicazione lineare** $F : V \to W$ tale che

$$F(v_i) = w_i \qquad 1 \leq i \leq n \tag{1}$$

Dimostrazione: sia $v \in V$, con

$$v = \sum_{i=1}^{n} a_i w_i$$

poniamo

$$F(v) = \sum_{i=1}^{n} a_i w_i$$

È chiaro che F verifica la relazione (1). Dobbiamo vedere che F è **lineare**, ovvero che

$$F(\alpha v + \beta v') = \alpha F(v) + \beta F(v')$$

Siano

$$v = \sum_i a_i v_i \qquad v' = \sum_i a'_i v_i$$

Si ha che

$$\alpha v + \beta v' = \alpha \sum_i a_i v_i + \beta \sum_i a'_i v_i = \sum_i (\alpha a_i + \beta a'_i) v_i$$

quindi

$$F(\alpha v + \beta v') = \sum_i (\alpha a_i + \beta a'_i) w_i$$
$$\alpha F(v) + \beta F(v') = \alpha \sum_i a_i w_i + \beta \sum_i a'_i w_i$$

Come si può vedere $F(\alpha v + \beta v') = \alpha F(v) + \beta F(v')$.

Dimostriamo infine che se $G : V \to W$ è lineare e $G(v_i) \stackrel{(1)}{=} w_i, 1 \leq i \leq n$, allora $F = G$.

Sia $v = \sum_i a_i v_i$

$$F(v) = \sum_i a_i w_i \stackrel{(1)}{=} \sum_i a_i G(v_i) \stackrel{(*)}{=} G(\sum_i a_i v_i) = G(v)$$

In $(*)$ è stato usato il fatto che G è **lineare**.

Osservazioni su Hom

Ricordiamo la definizione di Hom:

$$\mathrm{Hom}(V, W) = \{f : V \to W | f \text{ è lineare}\}$$

Osservazioni:

1. $\mathrm{Hom}(V, W)$ è uno **spazio vettoriale**

$$(S + T)(v) = S(v) + T(v)$$
$$\alpha \in \mathbb{K} \qquad (\alpha S)(v) = \alpha S(v)$$

2. $S \in \operatorname{Hom}(U, V),\ T \in \operatorname{Hom}(v, W)$ allora $T \circ S \in \operatorname{Hom}(U, W)$

$$\begin{tikzcd} U \arrow[r, "S"] \arrow[rr, bend right, "T \circ S"'] & V \arrow[r, "T"] & W \end{tikzcd}$$

$$\begin{aligned}(T \circ S)(\alpha u_1 + \beta u_2) &= T(S(\alpha u_1 + \beta u_2)) = T(\alpha S(u_1) + \beta S(u_2)) = \\ &= \alpha T(S(u_1)) + \beta T(S(u_2)) = \\ &= \alpha (T \circ S)(u_1) + \beta (T \circ S)(u_2)\end{aligned}$$

3. Esercizio: sia $T : V \to W$ **lineare biunivoca**. Allora $T^{-1} : W \to V$ è lineare.
4. Ricordiamo che un **isomorfismo** $V \to W$ è un'**applicazione lineare** biunivoca.

Proposizione

Siano U, V **spazi vettoriali finitamente generati**. Allora $U \cong\ V$ se e solo se $\dim U = \dim V$.

Lemma

1. Se $f : U \to V$ è **lineare e iniettiva** e $u_1, ..., u_k$ sono **linearmente indipendenti**, allora $f(u_1), ..., f(u_k)$ sono **linearmente indipendenti**.
2. Se $f : U \to V$ è **lineare e suriettiva** e $u_1, ..., u_k$ sono **generatori** per U, allora $f(u_1), ..., f(u_k)$ sono **generatori** per V.
3. Se $f : U \to V$ è **lineare biunivoca** e $\{u_1, ..., u_k\}$ è una **base** di U, allora $\{f(u_1), ..., f(u_k)\}$ è una **base** di V (in altri termini, un **isomorfismo** manda basi in basi).

Dimostrazioni:

1. Devo dimostrare che

$$\alpha_1 f(u_1) + ... + \alpha_k f(u_k) = 0 \Rightarrow \alpha_1, ..., \alpha_k = 0$$

ma $\alpha_1 f(u_1) + ... + \alpha_k f(u_k) = f(\alpha_1 u_1 + ... + \alpha_k u_k) = 0$ è equivalente a dire

$$\alpha_1 u_1 + ... + \alpha_k u_k \in \operatorname{Ker}(f) = \{0\}$$

che è vero perché f è iniettiva, quindi

$$\alpha_1 u_1 + ... + \alpha_k u_k = 0$$
$$\Rightarrow \alpha_1 = ... = \alpha_k = 0$$

L'implicazione è data dal fatto che gli u_i sono **linearmente indipendenti**.

2. Sia $v \in V$, poiché f è **suriettiva**, esiste $u \in U$ tale che $v = f(u)$. Ma $u = \alpha_1 u_1 + ... + \alpha_k u_k$ poiché $u_1, ..., u_k$ sono **generatori** per U, quindi

$$v = f(u) = f(\alpha_1 u_1 + ... + \alpha_k u_k) = \alpha_1 f(u_1) + ... + \alpha_k f(u_k)$$

3. Segue da $1)$ e $2)$.

<u>Dimostrazione delle proposizione</u>: dal lemma, se $U \cong V$ e $\phi : U \to V$ è un **isomorfismo**, ϕ manda **basi in basi**, quindi $\dim U = \dim V$.

Viceversa, sia $\dim U = \dim V = n$. Fissiamo **basi** $B = \{u_1, ..., u_n\}$ su U e $B' = \{v_1, ..., v_n\}$ su V. Abbiamo isomorfismi

$$\begin{tikzcd}
U \arrow[rr, "\varphi_{B'}^{-1} \circ \varphi_B"] \arrow[dr, "\varphi_B"'] & & V \arrow[dl, "\varphi_{B'}"] \\
& \mathbb{K}^n &
\end{tikzcd}$$

Applicazioni lineari e matrici

Abbiamo appena visto che se V è **finitamente generato** e $B = \{v_1, ..., v_n\}$ è una base di V, ho un isomorfismo $\phi_B : V \to \mathbb{K}^n$

$$\phi_B(v) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (v)_B \quad \text{se} \quad v = \sum_{i=1}^{n} x_i v_i$$

Vedremo adesso che fissando **due basi**, una $B = \{v_1, ..., v_n\}$ in V e una $C = \{w_1, ..., w_m\}$ in W, un'**applicazione lineare** $f : V \to W$ si può rappresentare tramite una matrice $A \in M_{mn}$, dipendente da B, C. In altri termini, costruiamo un **isomorfismo**

$$\mathrm{Hom}(V, W) \cong\ M_{mn}(\mathbb{K})$$

Come sopra, sia $B = \{v_1, ..., v_n\}$ una base di V, $C = \{w_1, ..., w_m\}$ una base di W, $f : V \to W$ lineare

Definizione

La matrice di f rispetto a B presa come **base di partenza** in V e a C presa come **base di arrivo** in W è la matrice le cui colonne sono le **coordinate** rispetto a C delle immagini tramite f dei **vettori** di B.

Notazione: ${}_C(f)_B$

$${}_C(f)_B = (a_{ij}) \qquad f(v_i) = \sum_{j=1}^{m} a_{ij} w_j \qquad 1 \le i \le n$$

Esempio: $V = \mathbb{R}_2[t],\ W = \mathbb{R}_3[t],\ f : V \to W$

$$f(p(t)) = t^2 p'(t+1)$$

Trovare ${}_C(f)_B$ con $B = \{1, t, t^2\},\ C = \{1, t, t^2, t^3\}$

$$\begin{aligned} f(1) &= 0 = 0 = 0 \cdot 1 + 0 \cdot t + 0 \cdot t^2 + 0 \cdot t^3 \\ f(t) &= t^2 = t^2 = 0 \cdot 1 + 0 \cdot t + 1 \cdot t^2 + 0 \cdot t^3 \\ f(t^2) &= t^2 \cdot 2(t+1) = 2t^3 + 2t^2 = 0 \cdot 1 + 0 \cdot t + 2 \cdot t^2 + 2 \cdot t^3 \end{aligned}$$

Quindi

$${}_C(f)_B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}$$

Esempio: $f : \mathbb{R}^3 \to \mathbb{R}^3$, con f definita nel modo seguente

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 \\ x_3 - x_1 \\ x_1 + 2x_2 + x_3 \end{pmatrix}$$

Siano le basi $B = C = \{e_1, e_2, e_3\}$. Dobbiamo calcolare

$$f\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \qquad f\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} \qquad f\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

Dobbiamo ora prendere i coefficienti, ovvero, prendendo come esempio il primo caso

$$f\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} = \underline{1} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + (\underline{-1}) \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \underline{1} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

⚠️ Avendo preso la base standard, i coefficienti sono proprio le colonne del risultato della funzione.

Quindi, in conclusione

$${}_B(f)_B = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix} = A$$

<u>N.B.</u>: In questo caso $f = L_A$, infatti

$$L_A(X) = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 \\ -x_1 + x_3 \\ x_1 + 2x_2 + x_3 \end{pmatrix} = f(X)$$

Proviamo ora cambiando base:

$$B = C = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \}$$

e la f definita sempre nello stesso modo.

$$f\begin{pmatrix}1\\0\\0\end{pmatrix}=\begin{pmatrix}1\\-1\\1\end{pmatrix}=2\begin{pmatrix}1\\0\\0\end{pmatrix}+(-2)\begin{pmatrix}1\\1\\0\end{pmatrix}+1\begin{pmatrix}1\\1\\1\end{pmatrix}$$
$$f\begin{pmatrix}1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\-1\\3\end{pmatrix}=1\begin{pmatrix}1\\0\\0\end{pmatrix}+(-4)\begin{pmatrix}1\\1\\0\end{pmatrix}+3\begin{pmatrix}1\\1\\1\end{pmatrix}$$
$$f\begin{pmatrix}1\\1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\4\end{pmatrix}=0\begin{pmatrix}1\\0\\0\end{pmatrix}+(-4)\begin{pmatrix}1\\1\\0\end{pmatrix}+4\begin{pmatrix}1\\1\\1\end{pmatrix}$$

⚠️ Attenzione! Dobbiamo trovare quegli α, β, γ che risolvono il sistema, ovvero, nell'esempio del primo caso, dobbiamo trovare:

$$f\begin{pmatrix}1\\0\\0\end{pmatrix}=\begin{pmatrix}1\\-1\\1\end{pmatrix}=\alpha\begin{pmatrix}1\\0\\0\end{pmatrix}+\beta\begin{pmatrix}1\\1\\0\end{pmatrix}+\gamma\begin{pmatrix}1\\1\\1\end{pmatrix}$$

Nel nostro caso sono stati trovati “a mano”, altrimenti andrebbero messi a sistema e risolverlo.

Quindi

$$_B(f)_B=\begin{pmatrix}2&1&0\\-2&-4&-4\\1&3&4\end{pmatrix}$$

Cambio di base

Cosa significa concettualmente trovare $_C(f)_B$?

$$
\begin{tikzcd}
V \arrow[r, "f"] \arrow[d, "\varphi_B"', "\cong"] & W \arrow[d, "\varphi_C", "\cong"'] \\
\mathbb{K}^n \arrow[r, "L_A"] & \mathbb{K}^m
\end{tikzcd}
$$

Chiamiamo $A = {}_C(f)_B$.

Supponiamo ora di avere $g \circ f$:

$$
\begin{tikzcd}
V \arrow[r, "f"] \arrow[rr, bend left, "g \circ f"] \arrow[d, "\varphi_B"', "\cong"] & W \arrow[r, "g"] \arrow[d, "\varphi_C", "\cong"'] & U \arrow[d, "\varphi_D", "="'] \\
\mathbb{K}^n \arrow[r, "L_A"] \arrow[rr, bend right, "L_C"'] & \mathbb{K}^m \arrow[r, "L_B"] & \mathbb{K}^s
\end{tikzcd}
$$

Chiamiamo $B = {}_D(g)_C$. Si ha proprio che $L_C = L_B \circ L_A$.

Questo significa che

$$
\begin{aligned}
L_C(X) = L_B(L_A(X)) \qquad & \forall X \\
CX = BAX \qquad & \forall X \\
C = BA \qquad &
\end{aligned}
$$

Questo spiega il **prodotto righe per colonne** che è la naturale reincarnazione della composizione di funzioni.

<u>Domanda</u>: sia data $f : V \to W$ **lineare** e siano B, B' **basi** di V e C, C' **basi** di W. Che relazione c'è tra ${}_C(f)_B$ e ${}_{C'}(f)_{B'}$?
Si capisce bene tramite il **diagramma commutativo**:

$$
\begin{tikzcd}
V \arrow[r, "\mathrm{id}_V"] \arrow[rrr, bend left, "f"] \arrow[d, "\varphi_{B'}"'] & V \arrow[r, "f"] \arrow[d, "\varphi_B"] & W \arrow[r, "\mathrm{id}_W"] \arrow[d, "\varphi_C"'] & W \arrow[d, "\varphi_{C'}"] \\
\mathbb{K}^n \arrow[r, "L_D"] \arrow[rrr, bend right, "L_F"'] & \mathbb{K}^n \arrow[r, "L_A"] & \mathbb{K}^m \arrow[r, "L_E"] & \mathbb{K}^m
\end{tikzcd}
$$

Abbiamo:

- $A = {}_C(f)_B$
- $D = {}_B(\mathrm{Id}_V)_{B'}$
- $E = {}_C(\mathrm{Id}_W)_{C'}$
- $F = {}_{C'}(f)_{B'}$

Dal diagramma risulta

$$
\begin{aligned}
L_F &= L_E \circ L_A \circ L_D \\
&= L_{EAD} \\
F &= EAD
\end{aligned}
$$

Che da vita a

Formula del cambiamento di base

$$ {}_{C'}(f)_{B'} = {}_{C'}(\mathrm{Id}_W)_C \ {}_C(f)_B \ {}_B(\mathrm{Id}_V)_{B'} $$

Caso speciale: $f : V \to V,\ B = C,\ B' = C'$. La formula scritta sopra diventa:

$$ {}_{B'}(f)_{B'} = {}_{B'}(\mathrm{Id}_V)_B \ {}_B(f)_B \ {}_B(\mathrm{Id}_V)_{B'} $$

Poniamo $N = {}_{B'}(\mathrm{Id}_V)_B$. Dimostriamo che N è **invertibile** e $N^{-1} = {}_B(\mathrm{Id}_V)_{B'}$ per cui

$$ {}_{B'}(f)_{B'} = N \ {}_B(f)_B \ N^{-1} $$

Definizione - Matrici quadrate simili

Due **matrici quadrate** A, B si dicono **simili** se esiste una **matrice invertibile** N tale che

$$A = NBN^{-1}$$

Questo dimostra il seguente teorema:

Teorema - Due matrici sono simili se e solo se rappresentano lo stesso operatore lineare

Due **matrici** $n \times n$ sono **simili** se e solo se rappresentano lo **stesso operatore lineare** su uno **spazio vettoriale** di **dimensione** n.

Esercizio:

$$_B(f)_B = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix} \qquad B = \{e_1, e_2, e_3\}$$
$$_{B'}(f)_{B'} = \begin{pmatrix} 2 & 1 & 0 \\ -1 & -4 & -4 \\ 1 & 3 & 4 \end{pmatrix} \qquad B' = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \}$$

Poniamo ora $N = {}_{B'}(\mathrm{Id}_V)_B$, abbiamo quindi

$$_{B'}(f)_{B'} = N \, _B(f)_B N^{-1}$$

Calcoliamo N^{-1} e N:

$$N^{-1} = {}_B(\mathrm{Id}_V)_{B'} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = -1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - 1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Quindi

$$N = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

Infine abbiamo:

$$\begin{array}{ccc} N & {}_B(f)_B & N^{-1} \\ \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array} =$$

$$= \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ -2 & -4 & -4 \\ 1 & 3 & 4 \end{pmatrix}$$

Lezione 31 - 15/12/2022

Ripasso matrice invertibile

Sia $A \in M_n(\mathbb{K})$. Ricordo che A si dice **invertibile** se esiste $B \in M_n(\mathbb{K})$ tale che

$$AB = BA = I_n$$

<u>Esercizio</u>: A è **invertibile** se e solo se $L_A : \mathbb{K}^n \to \mathbb{K}^n$ è **invertibile**.

Introdurremo una funzione $\det : M_n(\mathbb{K}) \to \mathbb{K}$ con la fondamentale proprietà che

$$A \text{ è invertibile} \Leftrightarrow \det A \neq 0$$

Alla fine enunceremo le seguenti equivalenze:

1. $\det A \neq 0$
2. $\text{rk } A = n$
3. Le **righe** di A sono **indipendenti**
4. Le **colonne** di A sono **indipendenti**
5. A è **invertibile**

Determinante

Sia $A = (a_{ij}) \in M_n(\mathbb{K})$

$$(*) \qquad \det A = \sum_{\sigma \in S_n} (-1)^{p(\sigma)} a_{1\sigma(1)} \cdot ... \cdot a_{n\sigma(n)}$$

dove $p(\sigma)$ sta ad indicare la **parità della permutazione**.

Esempio:

- $n=1,\ \det(a_{11})=a_{11}$
- $n=2$

$$\det A = \sum_{\sigma\in S_2}(-1)^{p(\sigma)}a_{1\sigma(1)}a_{2\sigma(2)} = \\ = a_{11}a_{22}-a_{12}a_{21}$$

In generale si ha

$$\det\begin{pmatrix} a & b \\ c & d\end{pmatrix} = ad-bc$$

Proprietà chiave del determinante

Vigliamo trovare proprietà che caratterizzano **univocamente** il **determinante**. Quindi consideriamo funzioni $d: M_n \to \mathbb{K}$ **pensate come funzioni delle righe**:

$$d(A) \leftrightsquigarrow d(A_1,...,A_n)$$

Le proprietà chiave sono le seguenti:

a. $d(A_1,...,A_n)=0$ se $A_i=A_j$ con $i\neq j$
b. $d(A_1,...,\alpha A_i,...,A_n)=\alpha d(A_1,...,A_i,...,A_n)$ (α “esce”)
c. $d(A_1,...,A_i'+A_i'',...,A_n)=d(A_1,...,A_i',...,A_n)+d(A_1,...,A_i'',...,A_n)$
d. $d(I_n)=1=d(e_1^t,...,e_n^t)$

Proposizione

Se d verifica le proprietà a,b,c, allora

1. Se A ha una **riga nulla** allora $d(A)=0$
2. $d(...,A_i+\lambda A_j,...,A_n)=d(A_1,...,A_n),\ \forall i\neq j,\ \forall\lambda\in\mathbb{R}$
3. $d(A_1,...,A_i,...,A_j,...,A_n)=-d(A_1,...,A_j,...,A_i,...,A_n)$
4. Se S è ottenuta da A per **riduzione di Gauss** con s **scambi di riga** allora

$$d(A)=(-1)^s d(S)$$

5. Se le righe di A sono **dipendenti** allora $d(A)=0$

Dimostrazioni:

1. Segue dalla proprietà $b.$ con $\alpha = 0$;
2. Segue da una combinazione delle proprietà a, b, c

$$d(..., A_i + \lambda A_j, ...) \overset{c.}{=} d(..., A_i, ...) + d(..., \lambda A_j, ..., A_j, ...) =$$
$$\overset{b.}{=} d(..., A_i, ...) + \lambda \underbrace{d(..., A_j, ..., A_j, ...)}_{=0 \text{ per } a.} = d(A)$$

3. Segue da una combinazione delle proprietà a, c

$$0 \overset{a.}{=} d(..., \overbrace{A_i + A_j}^{\text{posizione } i}, ..., \overbrace{A_i + A_j}^{\text{posizione } j}, ...) =$$
$$\overset{c.}{=} d(..., A_i, ..., Ai + A_j) + d(..., A_j, ..., A_i + A_j) =$$
$$= \underbrace{d(..., A_i, .., A_i, ...)}_{=0 \text{ per } a.} +$$
$$d(..., A_i, ..., A_j, ...) +$$
$$d(..., A_j, ..., A_i, ...) +$$
$$\underbrace{d(..., A_j, ..., A_j, ...)}_{=0 \text{ per } a.}$$

4. Segue dai punti $1.$ e $3.$
5. Se le **righe** di A sono **dipendenti**, qualsiasi **forma a gradini** di A ha una riga di 0. Dunque tutto segue dai punti $4.$ e $1.$

Teorema

Esiste un'unica funzione $\det : M_n(\mathbb{K}) \to \mathbb{K}$ che verifica le proprietà a, b, c, d.
In particolare $\det(A)$ coincide con $(*)$.

<u>Esercizio</u>: calcolare il determinante di

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Svolgimento:

$$
\begin{aligned}
d(a_{11}e_1^t + a_{12}e_2^t, a_{21}e_1t + a_{22}e_2^t) =& a_{11}d(e_1^t, a_{21}e_1^t + a_{22}e_2^t) + \\
& a_{12}d(e_2^t, a_{21}e_1^t + a_{22}e_2^t) = \\
& \underbrace{a_{11}a_{21}d(e_1^t, e_1^t)}_{=0} + \\
& a_{11}a_{22}d(e_1^t, e_2^t) + \\
& a_{12}a_{21}d(e2^t, e_1^t) + \\
& \underbrace{a_{12}a_{22}d(e_2^t, e_2^t)}_{=0} = \\
=& (a_{11}a_{22} - a_{12}a_{21})d(e_1^t, e_2^t) = \\
=& (a_{11}a_{22} - a_{12}a_{21})d(I_2) = a_{11}a_{22} - a_{12}a_{21}
\end{aligned}
$$

Utilizzando allo stesso modo le proprietà è facile vedere che:

$$
\det \begin{pmatrix} a_1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} = a_1 ... a_n
$$

e inoltre

$$
\det \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ & \ddots & a_5 & a_6 \\ & & \ddots & a_7 \\ & & & a_n \end{pmatrix} = \det \begin{pmatrix} a_1 & & & \\ a_2 & \ddots & & \\ a_3 & a_4 & \ddots & \\ a_5 & a_6 & a_7 & a_n \end{pmatrix} = a_1 ... a_n
$$

ovvero il **determinate** delle **matrici triangolari superiori e inferiori** è $a_1 ... a_n$.

Sviluppi di Laplace

Sia A_{ij} la matrice ottenuta da A cancellando la riga i e la colonna j.

Proposizione

- **Sviluppo di Laplace per riga**:

  Fissato $i, \ 1 \leq i \leq n$

$$
\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}
$$

- **Sviluppo di Laplace per colonne**:

  Fissato $j, \ 1 \leq j \leq n$

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$$

<u>Esempio</u>: sia

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Sviluppo lungo la **prima riga**:

$$\det A = (-1)^{1+1} a_{11} \underbrace{\det A_{11}}_{a_{22}} + (-1)^{1+2} a_{12} \underbrace{\det A_{12}}_{a_{21}} = a_{11}a_{22} + a_{12}a_{21}$$

$$A_{11} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$A_{12} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

<u>Esempio</u>: calcolare il determinante di

$$\begin{vmatrix} 3 & 4 & 2 & 1 \\ 0 & 7 & 6 & 3 \\ 1 & 1 & 2 & 4 \\ 3 & 1 & -2 & 4 \end{vmatrix}$$

Iniziamo sviluppando lungo la prima riga:

$$\begin{vmatrix} 3 & 4 & 2 & 1 \\ 0 & 7 & 6 & 3 \\ 1 & 1 & 2 & 4 \\ 3 & 1 & -2 & 4 \end{vmatrix} = 3\begin{vmatrix} 7 & 6 & 3 \\ 1 & 2 & 4 \\ 1 & -2 & 4 \end{vmatrix} + \begin{vmatrix} 4 & 2 & 1 \\ 7 & 6 & 3 \\ 1 & -2 & 4 \end{vmatrix} - 3\begin{vmatrix} 4 & 2 & 1 \\ 7 & 6 & 3 \\ 1 & 2 & 4 \end{vmatrix} =$$

$$= 3\begin{vmatrix} 7 & 6 & 3 \\ 0 & 4 & 0 \\ 0 & -2 & 4 \end{vmatrix} + 4\begin{vmatrix} 6 & 3 \\ -2 & 4 \end{vmatrix} - 2\begin{vmatrix} 7 & 3 \\ 1 & 4 \end{vmatrix} + \begin{vmatrix} 7 & 6 \\ 1 & -2 \end{vmatrix}$$

$$-3(4\begin{vmatrix} 6 & 3 \\ 2 & 4 \end{vmatrix} - 2\begin{vmatrix} 7 & 3 \\ 1 & 4 \end{vmatrix} + 1\begin{vmatrix} 7 & 6 \\ 1 & 2 \end{vmatrix}) =$$

$$= 12\begin{vmatrix} 7 & 3 \\ 0 & 4 \end{vmatrix} + 4 \cdot 30 - 2 \cdot 25 - 20 -$$

$$-3(4 \cdot 18 - 2 \cdot 25 + 8) =$$

$$= 12 \cdot 28 + 120 - 50 - 20 - 3(72 - 50 + 8) = 260$$

⚠️ Quando si calcola il determinante, le matrici vengono rappresentante usando delle **barre verticali** invece di **parentesi**.

Proprietà del determinante

1. **Teorema di Binet**

$$\det AB = \det A \cdot \det B$$

2. $\det A^t = \det A$

Relazioni tra rango e determinante

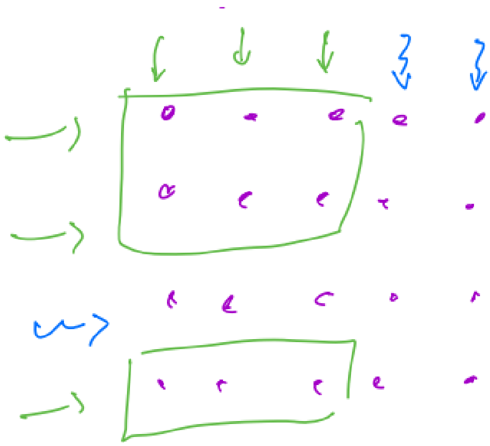
Definizione - Minore di ordine k

Sia $A \in M_{mn}(\mathbb{K})$. Un **minore** di ordine k in A è il **determinante** di una **sottomatrice quadrata** ottenuta scegliendo k righe e k colonne di A.

Teorema

$\text{rk}\, A$ è l'ordine massimo dei minori non nulli di A.

Ad esempio, dire che $A \in M_{45}(\mathbb{R})$ ha **rango** 3, significa dire che esiste un **minore** di **ordine** 3 diverso da 0 e tutti i **minori di di ordine** 4 **sono nulli**:



<u>Teorema degli orlati</u>:

Basta che siano nulli i minori 4×4 ottenuto aggiungendo una riga e una colonna alla **sottomatrice** 3×3 con **determinante non nullo**.

<u>Corollario</u>: In una matrice il **massimo numero di righe linearmente indipendenti** è uguale al **massimo numero di colonne linearmente indipendenti**.

Correzione esercizi ottava scheda

Lezione 32 - 16/12/2022

Autovettori e autovalori

Tratteremo d'ora in poi solo il caso di **operatori lineari** $T : V \to V$ con $\dim_{\mathbb{K}} V = +\infty$.

Problema: posso trovare una rappresentazione matriciale di T "ottimale", ovvero la più facile possibile (la matrice diagonale)?

Definizione

Sia $T \in \operatorname{End}(V)$. Un **vettore** $v \neq 0$ si dice **autovettore** per T di **autovalore** $\lambda \in \mathbb{K}$ se

$$T(v) = \lambda v$$

Diciamo poi che $\lambda \in \mathbb{K}$ è **autovalore** per T se $\exists v \neq 0$, tale che $T(v) = \lambda v$.

Nomenclatura: $V_\lambda = \{v \in V : T(v) = \lambda v\}$ è detto **autospazio** di T relativo all'**autovalore** λ.

N.B.: gli elementi di V_λ sono gli **autovettori** di T di **autovalore** λ e **zero**.

Esercizio: V_λ è un **sottospazio vettoriale** di V.

Siano $v_1, v_2 \in V$ e $\alpha, \beta \in \mathbb{K}$. Vogliamo vedere che

$$\alpha v_1 + \beta v_2 \in V_\lambda$$
$$T(v_1) = \lambda v_1 \qquad T(v_2) = \lambda v_2$$

Svogliamo i calcoli:

$$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2) = \alpha\lambda v_1 + \beta\lambda v_2 = \lambda(\alpha v_1 + \beta v_2)$$

Osservazione

Notiamo che $V_\lambda = \mathrm{Ker}(T - \lambda \mathrm{Id}_V)$

$$\begin{aligned} v \in \mathrm{Ker}(T - \lambda\mathrm{Id}_V) &\Leftrightarrow (T - \lambda\mathrm{Id}_V)(v) = 0 \\ &\Leftrightarrow T(v) - \lambda\mathrm{Id}_V(v) = 0 \\ &\Leftrightarrow T(v) - \lambda v = 0 \\ &\Leftrightarrow T(v) = \lambda v \end{aligned}$$

Quindi gli **autovalori** di T sono gli **scalari** di λ per cui $T - \lambda\mathrm{Id}_v$ **non è invertibile**.

Proposizione

Sia $T \in \mathrm{End}(V)$ e B una **base** di V. Allora B è composta da **autovettori** per T se e solo se ${}_B(T)_B$ è **diagonale**.

Dimostrazione: supponiamo che $B = \{v_1, ..., v_n\}$ sia una **base** di V formata da **autovettori** per T. Allora

$$\begin{aligned} T(v_1) &= \lambda_1 v_1 = \lambda_1 v_1 + 0 \cdot v_2 + ... + 0 \cdot v_n \\ T(v_2) &= \lambda_2 v_2 = 0 \cdot v_1 + \lambda_2 v_2 + 0 \cdot v_3 + ... + 0 \cdot v_n \\ &\vdots \\ T(v_n) &= \lambda_n v_n = 0 \cdot v_1 + ... + \lambda_n v_n \end{aligned}$$

Questo significa che ${}_B(T)_B$ è diagonale

$${}_B(T)_B = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

Il **viceversa** si dimostra allo stesso modo.

Definizione - Diagonalizzabilità

Diciamo che $T \in \mathrm{End}(V)$ è **diagonalizzabile** se esiste una **base** di V formata da **autovettori** per T.

Osservazione: ricordiamo che due matrici rappresentano lo **stesso operatore lineare** in basi diverse se e solo se sono **simili**.
Pertanto T è **diagonalizzabile** se la sua matrice rispetto a una qualsiasi base presa in **partenza** e in **arrivo** è **simile** a una **matrice diagonale**.

Proposizione

$T \in \mathrm{End}(V),\ B = \{v_1, ..., v_n\}$ **base** di V, $A = {}_{\mathbb{B}}(T)_{\mathbb{B}}$. Allora

1. La funzione $p_T : \mathbb{K} \to \mathbb{K}$ definita come

$$p_T(\lambda) = \det(A - \lambda I_n)$$

   non dipende dalla **base** $\mathbb{B}$.
2. p_T è un **polinomio** di grado n dove:
   - il **coefficiente direttore** è $(-1)^n$
   - il **coefficiente** di λ^{n-1} è $(-1)^{n-1} \cdot \mathrm{tr}(A)$ (traccia di A)
   - il **termine noto** è $\det A$
3. $\lambda_0 \in \mathbb{K}$ è **autovalore** di T se e solo se $p_T(\lambda_0) = 0$

Dimostrazioni:

1. devo vedere che se A, B sono simili, allora

$$\det(A - \lambda I_n) = \det(B - \lambda I_n)$$

   Se A, B sono **simili**, esiste N **invertibile** tale che $B = NAN^{-1}$

   > ⚠️ Osservazione: se A è **invertibile**, $\det(A^{-1}) = \frac{1}{\det A}$
   >
   > $$\begin{array}{ccc} & AA^{-1} = I_n & \\ \det(AA^{-1}) & = & \det(I_n) = 1 \\ \| & & \\ \det(A)\det(A^{-1} & \rightsquigarrow & \det(A^{-1}) = \frac{1}{\det A} \end{array}$$

$$
\begin{aligned}
\det(B-\lambda I_n) &= \det(NAN^{-1}-\lambda I_n) = \\
&= \det(N(A-\lambda I_n)N^{-1}) = \\
&= \det N \cdot \det(A-\lambda I_n)\cdot \det(N^{-1}) = \\
&= \cancel{\det N}\cdot \det(A-\lambda I_n)\cdot \frac{1}{\cancel{\det N}} = \det(A-\lambda I_n)
\end{aligned}
$$

2. Sia

$$
A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}
$$

con:

- $\det A = a_{11}a_{22} - a_{12}a_{21}$
- $trA = a_{11} + a_{22}$

Si ha che

$$
\begin{aligned}
det(\lambda I_2 - A) &= \det(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} - \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}) \\
&= \det \begin{pmatrix} \lambda - a_{11} & -a_{12} \\ -a_{21} & \lambda - a_{22} \end{pmatrix} \\
&= (\lambda - a_{11})(\lambda - a_{22}) - a_{12}a_{21} \\
&= \lambda^2 \underbrace{-(a_{11}+a_{12})}_{-\mathrm{tr}A} + \underbrace{a_{11}a_{12} - a_{12}a_{21}}_{\det A}
\end{aligned}
$$

In generale si procede per **induzione** su n.

3. Supponiamo che $T(v) = \lambda_0 v,\ v \neq 0$. Dobbiamo passare in coordinate:

$$
X = (v)_B \qquad A = {}_B(T)_B \qquad X \neq 0
$$

$$
\begin{aligned}
(T(v))_B &= (\lambda_0 v)_B \\
{}_B(T)_B\ (v)_B &= \lambda_0 (v)_B \\
AX &= \lambda_0 X \\
(A - \lambda_0 I_n)X &= 0
\end{aligned}
$$

Quindi il **sistema lineare omogeneo** di matrice $A - \lambda_0 I_n$ ha una soluzione **non banale**. Ma allora la matrice $A - \lambda_0 I_n$ **non ha rango massimo**. Dunque

$$\det(A-\lambda_0 I_n)=0$$

cioè $p_A(\lambda_0)=0$. Il **viceversa** si dimostra ripercorrendo la dimostrazione al contrario.

Esempio: sia

$$A=\begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ 3 & 3 & 5 \end{pmatrix}$$

$$\det(A-\lambda I_3)=0 \longrightarrow \begin{vmatrix} 3-\lambda & 1 & 1 \\ 2 & 4-\lambda & 2 \\ 3 & 3 & 5-\lambda \end{vmatrix}=0$$

Sviluppando i calcoli si ha

$$\begin{aligned}
&(3-\lambda)(4-\lambda)(5-\lambda)+6+6-3(4-\lambda)-6(3-\lambda)-2(5-\lambda)=0 \\
&(12-7\lambda+\lambda^2)(5-\lambda)-28+19\lambda=0 \\
&60-35\lambda+5\lambda^2-12\lambda+7\lambda^2-\lambda^3-28+11\lambda=0 \\
&-\lambda^3+12\lambda^2-36\lambda+32=0 \\
&\lambda^3-12\lambda^2+36\lambda-32=0 \leftarrow 2 \text{ è soluzione con Ruffini} \\
&(\lambda-2)(\lambda^2-10\lambda+16)=0 \\
&(\lambda-2)^2(8-\lambda)=0
\end{aligned}$$

Gli **autovalori** sono quindi $2, 8$.

Definizione - Molteplicità algebrica e geometrica

Sia λ un **autovalore** di $T \in \operatorname{End}(V)$.
Definiamo la **molteplicità algebrica** di λ, $m_a(\lambda)$ come la **molteplicità di λ come radice del polinomio caratteristico**.
Definiamo la **molteplicità geormetrica** di λ, $m_g(\lambda)$ come

$$m_g(\lambda)=\dim V_\lambda$$

Ricordiamo che λ è **radice** di molteplicità m del polinomio $p(t)$ e

$$p(t)=(t-\lambda)^m q(t) \qquad q(\lambda)\neq 0$$

Proposizione

$1 \leq m_g(\lambda) \leq m_a(\lambda)$ per ogni **autovalore** λ di $T \in \operatorname{End}(V)$.

Dimostrazione: $1 \leq m_g(\lambda)$ vuol dire che $\dim V_\lambda > 0$, cioè che $V_\lambda \neq \{0\}$, cioè che λ è **autovalore**.

Sia $\{v_1, ..., v_k\}$ una **base** di V_λ. Completiamola con vettori $\{v_{k+1}, ..., v_n\}$ a una base di V.
Costruiamo $_B(T)_B$: $T(v_1) = \lambda v_1, ..., T(v_n) = \lambda v_n, ...$

$$A = \left(\begin{array}{ccc|c} \lambda & & & \overbrace{\quad * \quad}^{n-k} \\ & \ddots & & \\ & & \lambda & \\ \hline & & & C \end{array}\right) \Big\} n-k$$

Il determinante sarà quindi:

$$\det(A - tI_n) = \det \left(\begin{array}{ccc|c} \lambda - t & & 0 & * \\ & \ddots & & \\ 0 & & \lambda - t & \\ \hline & & & C - tI_{n-k} \end{array}\right)$$

$$= (\lambda - t)^k \det(C - tI_{n-k})$$

dunque $m_a(\lambda) \geq k = m_g(\lambda)$.

Esempio: siano $\dim V = 4,\ \dim V_\lambda = 2,\ \{v_1, v_2\}$ **base** di V_λ, $\{v_1, v_2, v_3, v_4\}$ **base** di V.

$$\begin{array}{ll} T(v_1) = \lambda v_1 & T(v_3) = \dots \\ T(v_2) = \lambda v_2 & T(v_4) = \dots \end{array}$$

$$A = \begin{pmatrix} \lambda & 0 & a & e \\ 0 & \lambda & b & f \\ 0 & 0 & c & g \\ 0 & 0 & d & h \end{pmatrix}$$

$$\det(A - tI_n) = 0 \longrightarrow \begin{vmatrix} \lambda - t & 0 & a & e \\ 0 & \lambda - t & b & f \\ 0 & 0 & e - t & g \\ 0 & 0 & d & h - t \end{vmatrix} = 0$$

Sviluppo (di Laplace) lungo la **prima colonna** in quanto ha la **quantità maggiore di** 0:

$$(\lambda - t)\begin{vmatrix} \lambda - t & b & f \\ 0 & c - t & 0 \\ 0 & d & h - t \end{vmatrix} = 0$$

sviluppo nuovamente lungo la **prima colonna** per lo stesso motivo:

$$(\lambda - t)^2 \det \begin{pmatrix} c - t & g \\ d & h - t \end{pmatrix} = 0$$

Teorema - Diagonalizzabilità

$T \in \mathrm{End}(V)$ è **diagonalizzabile** se e solo se

1. $\sum_{\lambda \text{ autovalori di } T} m_a(\lambda) = \dim V$
2. $\forall \lambda$ autovalore di T, $m_a(\lambda) = m_g(\lambda)$

Osservazioni:

1. Se $\mathbb{K} = \mathbb{C}$ la $1.$ è **sempre verificata**
2. Se $m_a(\lambda) = 1 \ \forall \lambda$ la $2.$ è verificata.

> ⚠️ Attenzione: il fatto che gli **autovalori** siano distinti è condizione solo **sufficiente** per la diagonalizzabilità.
> Controesempio: $T = Id_V$

Inoltre possiamo dedurre che è **sufficiente** verificare la condizione $2.$ solo per gli **autovalori** λ con $m_a(\lambda) \geq 2$.

Proposizione

Autovettori relativi a **autovalori** distinti sono **linearmente indipendenti**.

Dimostrazione: siano $v_1, ..., v_n$ **autovettori** relativi ad **autovalori** $\lambda_1, ..., \lambda_k$ con $\lambda_i \neq \lambda_j$ per $i \neq j$

$$f(v_1) = \lambda_1 v_1, ..., f(v_k) = \lambda_k v_k$$

$$(1) \qquad a_1 v_1 + ... + a_k v_k = 0$$

$$f(a_1 v_1 + ... + a_k v_k) = f(0) = 0$$

$$a_1 f(v_1) + ... + a_k f(v_k) = 0$$

$$(2) \qquad a_1 \lambda_1 v_1 + ... + a_k \lambda_k v_k = 0$$

Procediamo per **induzione** su k:

Se $k = 1$ allora $v_1 \neq 0$ (perché è **autovettore**), quindi $\{v_1\}$ è **indipendente**.

Moltiplico (1) per λ_1 ottenendo

$$(3) \qquad \lambda_1 a_1 v_1 + \lambda_1 a_2 v_2 + ... + \lambda_1 a_k v_k = 0$$

Sottraggo ora (3) da (2) ottenendo

$$(\lambda_1 - \lambda_2) a_2 v_2 + ... + (\lambda_1 - \lambda_2) a_k v_k = 0$$

Questa è una combinazione lineare eguagliata a zero di $v_2, ..., v_k$, che per **induzione** sono **indipendenti**, quindi

$$(\lambda_1 - \lambda_2) a_2 = 0, ..., (\lambda_1 - \lambda_2) a_k = 0$$

Ma $\lambda_1 - \lambda_i \neq 0$ se $i \neq 1$, quindi

$$a_2 = ... = a_k = 0$$

Sostituisco ora in (1) e trovo

$$a_1 v_1 = 0$$

Ma $v_1 \neq 0$, quindi $a_1 = 0$.

Lezione 33 - 19/12/2022

Ripasso lezione precedente

$T \in \mathrm{End}(V)$, V **spazio vettoriale** e $\dim_{\mathbb{K}} V = n$

- T è **diagonalizzabile** se esiste una **base** di V formata da **autovettori** per f;
- $v \in V$, $v \neq 0$ è un **autovettore** per f di **autovalore** λ se $f(v) = \lambda v$. Abbiamo anche definito il seguente autospazio:

$$V_\lambda = \{v \in V | f(v) = \lambda v\}$$

- λ autovalore se $f - \lambda \mathrm{Id}_V$ non è **invertibile**.
  B base di V, $A = {}_B(f)_B$

$$p_A(t) = \det(A - tI_n)$$
$$\lambda \text{ autovalore} \Longleftrightarrow p_A(\lambda) = 0$$

  Gli autovalori λ hanno associati due valori:
  - $m_a(\lambda) = \text{molteplicità di } \lambda \text{ come radice di } p_A(t)$
  - $m_g(\lambda) = \dim V_\lambda$

  Si ha inoltre che $m_a(\lambda) \geq m_g(\lambda) \geq 1$.
- **Autovettori** relativi ad **autovalori** distinti sono **linearmene indipendenti**.

Teorema

$T \in \mathrm{End}(V)$ è **diagonalizzabile** su $\mathbb{K}$ se e solo se

1. $\sum_{\lambda \text{ autovalori di } T} m_a(\lambda) = \dim V$
2. $\forall \lambda$ autovalore di T, $m_a(\lambda) = m_g(\lambda)$

Dimostrazione: siano $\lambda_1, ..., \lambda_k$ i **distinti autovalori** di T.
Osserviamo che T è **diagonalizzabile** se e solo se

$$(*) \qquad V = \bigoplus_{i=1}^{k} V_{\lambda_i}$$

Se T è **diagonalizzabile** allora vale $(*)$ e quindi

$$\dim V = \sum_{i=1}^{k} \dim V_{\lambda_i} = \sum_{i=1}^{k} m_g(\lambda_i) \leq \sum_{i=1}^{k} m_a(\lambda_i) \leq \dim V$$

Quindi i $\leq$ sono $=$ e quindi vale la condizione $1.$ e anche la $2.$

> ⚠️ $0 \leq a_i \leq b_i, \ \sum a_i = \sum b_i \Rightarrow a_i = b_i \ \forall i$

Viceversa supponiamo che valgono $1.$ e $2.$ Sia

$$W = \sum_{i=1}^{k} V_{\lambda_i} = \bigoplus_{i=1}^{k} V_{\lambda_i} \subset V$$

Si ha che

$$\dim W = \sum_{i=1}^{k} \dim V_{\lambda_i} = \sum_{i=1}^{k} m_g(\lambda_i) \overset{2.}{=} \sum_{i=1}^{k} m_a(\lambda) \overset{1.}{=} \dim V$$

Dunque $W \subset V, \dim W = \dim V \Rightarrow V = W$.

Dunque $V = \bigoplus_{i=1}^{k} V_{\lambda_i}$ per $(*)$ T è **diagonalizzabile**.