Algebra Lineare 11/10/16

V sp. vett. su $\mathbb{R}$

<u>Prop</u>: Se $A \subset V$ esiste unico W t.c.

1) W è stsp. vett.

2) $W \supset A$

3) se Z è stsp e $Z \supset A$ allora $Z \supset W$.

Dim: Unicità: suppongo che W_1 e W_2 soddisfino 1+2+3.

Applico la 3 con $W = W_1$ e $Z = W_2$

(per ipotesi W_1 soddisfa 3, ma W_2 soddisfa 1+2

$\Rightarrow$ quindi posso usarlo come Z in 3)

$\Rightarrow W_2 \supset W_1$.

Ripeto lo stesso a ruoli scambiati e trovo $W_1 \supset W_2$

$\Rightarrow W_1 = W_2$.

<u>Esistenza</u> : affermo che $W = \bigcap \{$tutti i sottosp. di V che contengono $A\}$ va bene.

0. la def. ha senso perché V è un sottosp. di sé stesso e $V \supset A \Rightarrow$ l'$\bigcap$ è non vuota.

1. W è sottosp. perché intersez. di sottosp. ✓
2. $W \supset A$ ✓
3. $Z \supset A$ sottosp. $\Rightarrow$ è tra quelli che

compaiono nell'$\cap$ che dà $W \Rightarrow Z \supset W$. $\boxtimes$

<u>Oss</u>: Ogni V sp. vett. ha sempre due sottosp. banali: $\{0\}$, V.

<u>Def</u>: Il più piccolo sttsp. che contiene A (cioè il W della Prop) si chiama generato di A, indicato con $\mathrm{Span}(A)$. Se $\mathrm{Span}(A) = W$ diremo che A è un insieme di generatori per W.

Prop: $\operatorname{Span}(\{v_1, \dots, v_n\})$
$$= \{\lambda_1 v_1 + \dots + \lambda_n v_n : \quad \lambda_1, \dots, \lambda_n \in \mathbb{R}\}$$

Dim: sia $L = \{\lambda_1 v_1 + \dots + \lambda_n v_n : \dots\}$.

Devo vedere 1 + 2 + 3

1. $\quad$ 1. $\quad 0 \cdot v_1 + \dots \cdot 0 \cdot v_n = 0 \Rightarrow 0 \in L$

2+3. $\quad v = \lambda_1 v_1 + \dots + \lambda_n v_n \in L$

$\quad w = \mu_1 v_1 + \dots + \mu_n v_n \in L$

$$\alpha v + \beta w = \underbrace{(\alpha \lambda_1 + \beta \mu_1)}_{\substack{\uparrow \\ \mathbb{R}}} v_1 + \dots + \underbrace{(\alpha \lambda_n + \beta \mu_n)}_{\substack{\cup \\ \mathbb{R}}} \cdot v_n$$

$$\Rightarrow \alpha v + \beta w \in L$$

2. $L \supset \{v_1, \dots, v_n\}$:

$$v_j = \boxed{0} \cdot v_1 + \boxed{0} \cdot v_2 + \dots + \boxed{1} \cdot v_j + \dots \boxed{0} \cdot v_n$$

3. Se Z è stsp e $Z \supset \{v_1, \dots, v_n\}$ allora $Z \supset L$.

Prendo $v = \lambda_1 v_1 + \ldots + \lambda_n v_n \in L$; devo vedere che $v \in Z$;
infatti $v_1, \ldots, v_n \in Z$, Z sottosp.

$\Rightarrow \lambda_1 v_1 + \lambda_2 v_2 \in Z$

$\Rightarrow (\lambda_1 v_1 + \lambda_2 v_2) + \lambda_3 v_3 \in Z$

$\Rightarrow \ldots \quad \lambda_1 v_1 + \ldots + \lambda_n v_n \in Z$. $\boxed{///}$

<u>Esercizio</u>: verificare che vale il fatto più generale:

$$\mathrm{Span}(A) = \{ \lambda_1 v_1 + \dots + \lambda_n v_n : \ n \in \mathbb{N}, \ \lambda_1, \dots, \lambda_n \in \mathbb{R}, \ v_1, \dots, v_n \in A \}.$$

Oss: (1) Se W è stsp. di V

$$\mathrm{Span}(W) = W$$

(2) $\mathrm{Span}(\mathrm{Span}(A)) = \mathrm{Span}(A)$

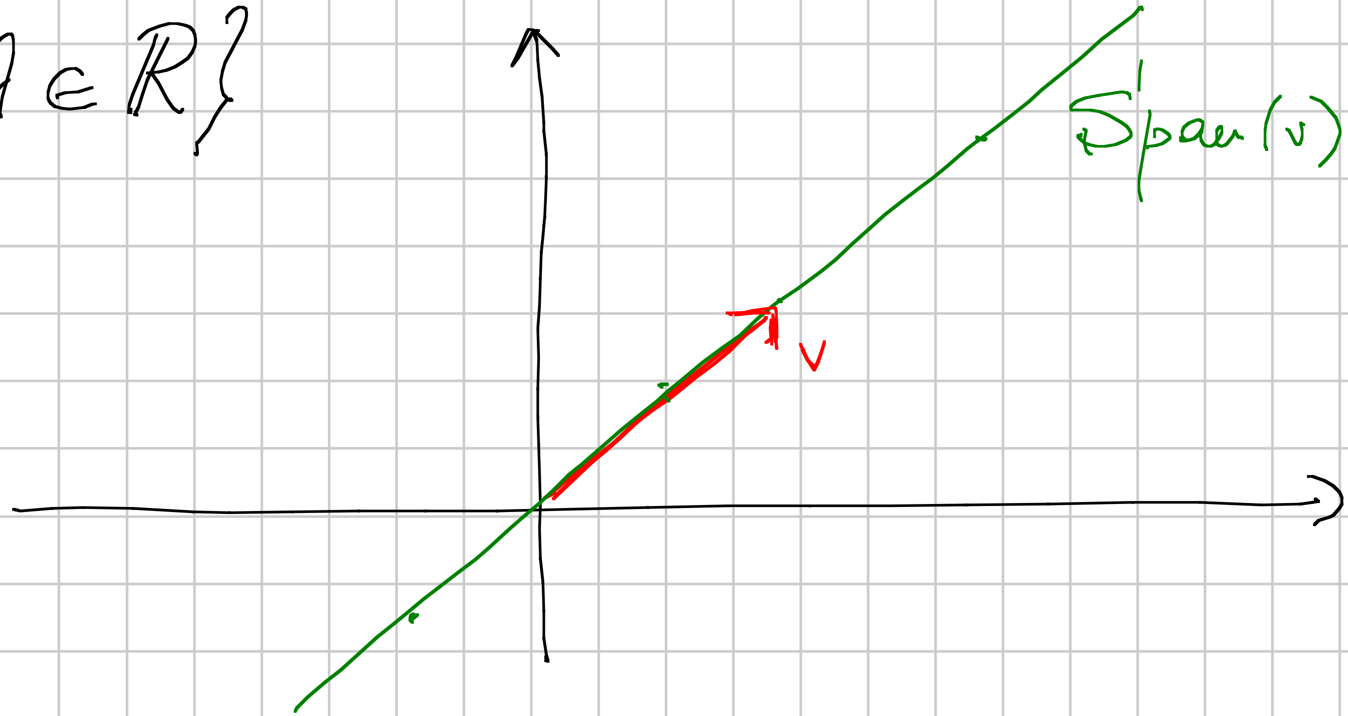
(3) $\mathrm{Span}(\emptyset) = \{0\}$

(4) Span(v) (dovrebbe essere Span$(\{v\})$)

$$\| $$

$\{\lambda \cdot v : \lambda \in \mathbb{R}\}$

se $v \neq 0$



se $v = 0$ $\quad Span(0) = \{0\}$.

(5) $Span(v_1, v_2) = \{\lambda_1 v_1 + \lambda_2 v_2 \; : \; \lambda_1, \lambda_2 \in \mathbb{R}\}$

$V = \mathbb{R}^3$

- $v_1 = v_2 = 0 \qquad Span(0) = \{0\}$
- $v_1 = 0, \; v_2 \neq 0 \qquad Span(v_1, v_2) = Span(v_2)$

  $=$ retta dei multipli di v_2

- $v_1 \neq 0, \; v_2 \neq 0, \quad v_2 = k v_1 \quad$ (cioè $v_2 \in Span(v_1)$)

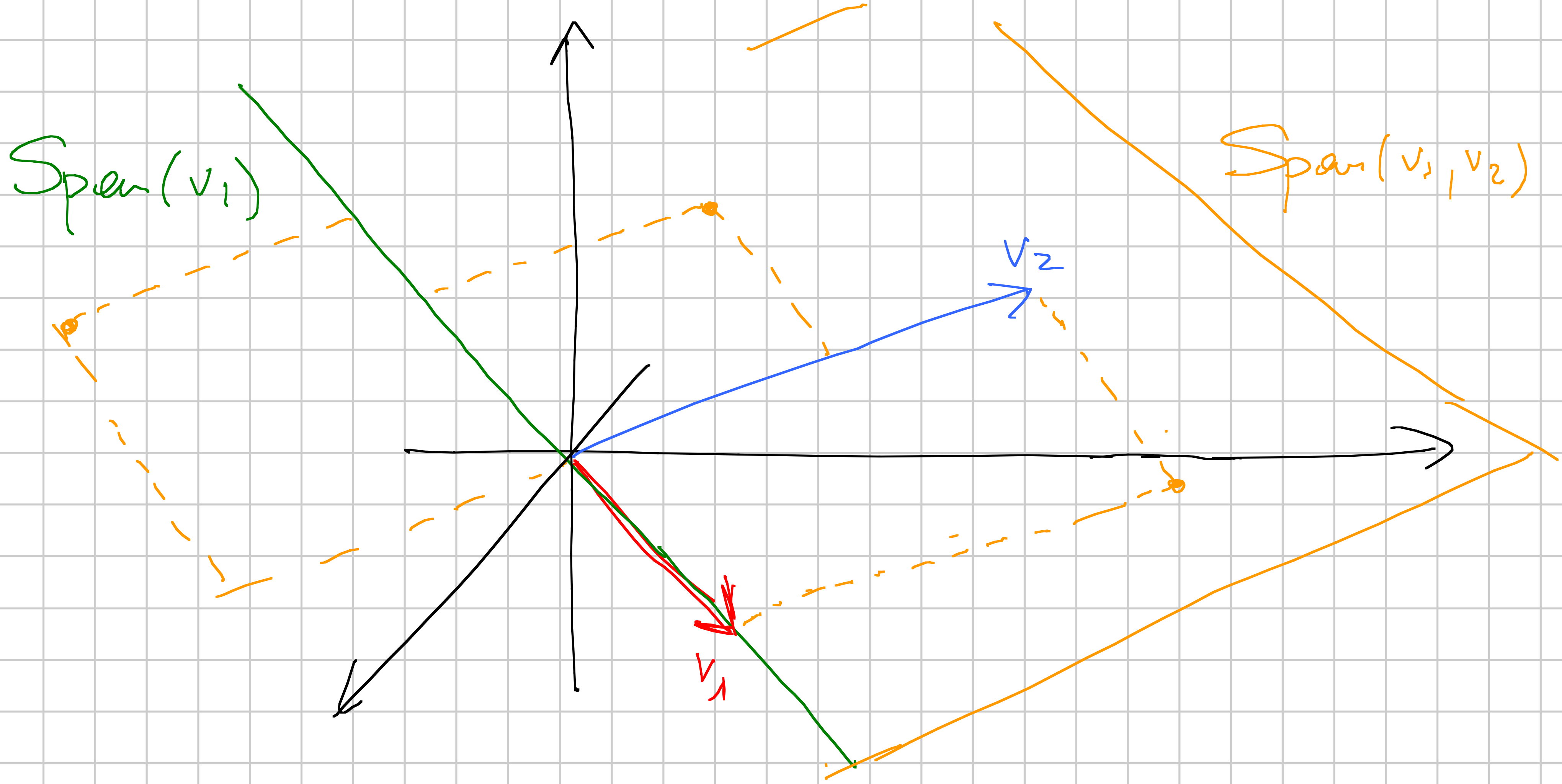
$$\lambda_1 v_1 + \lambda_2 v_2 = (\lambda_1 + k v_2) \cdot v_1$$

$$\Rightarrow \mathrm{Span}(v_1, v_2) = \mathrm{Span}(v_1)$$

retta dei multipli di v_1

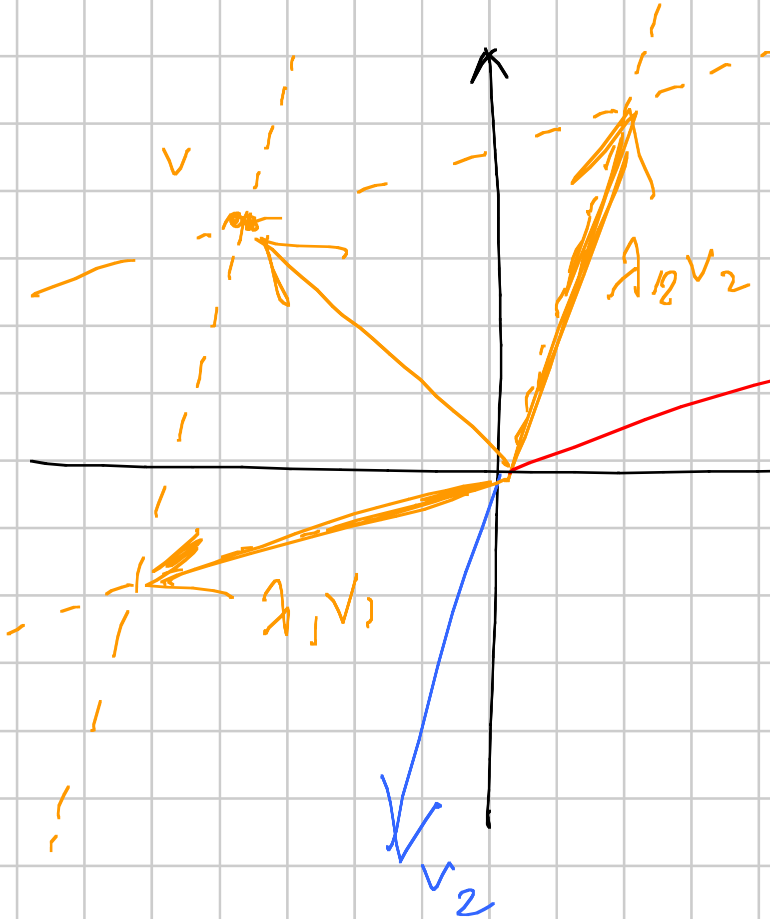
(= retta dei multipli di v_2)

- $v_1 \neq 0$, $v_2 \notin \mathrm{Span}(v_1)$



Span(v1)
Span(v1, v2)
v2
v1

Zu $\mathbb{R}^2$:



$v = \lambda_1 v_1 + \lambda_2 v_2$

$\operatorname{Span}(v_1, v_2) = \mathbb{R}^2$

Scoperta: due vettori di $\mathbb{R}^2$ non multipli l'uno dell'altro (il che esclude che uno sia 0) generano $\mathbb{R}^2$.

(6) $\mathrm{Span}(v_1, v_2, v_3)$

- $v_1 = 0$ viene $\mathrm{Span}(v_2, v_3)$
- $v_1 \neq 0$, $v_2 \in \mathrm{Span}(v_1)$ viene $\mathrm{Span}(v_1, v_3)$

- $v_1 \neq 0$, $v_2 \notin \mathrm{Span}(v_1)$, $v_3 \in \mathrm{Span}(v_1, v_2)$

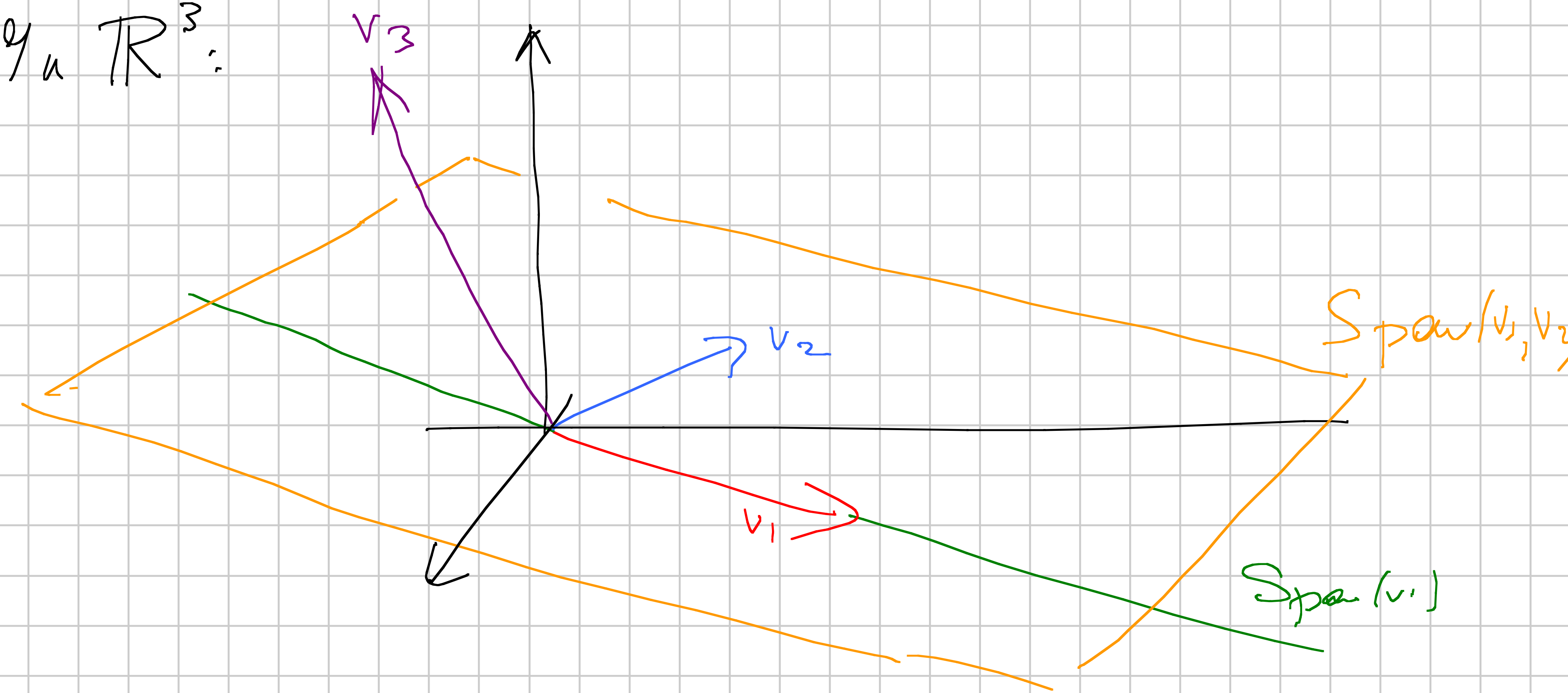
allora $v_3 = \alpha_1 v_1 + \alpha_2 v_2$

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = (\lambda_1 + \alpha_1 \lambda_3) v_1 + (\lambda_2 + \alpha_2 \lambda_3) v_2$$

$\Longrightarrow$ vive Span(v_1, v_2)

- $v_1 \neq 0$, $v_2 \notin \mathrm{Span}(v_1)$, $v_3 \notin \mathrm{Span}(v_1, v_2)$

In $\mathbb{R}^3$:



Verificare che allora ogni vett. di $\mathbb{R}^3$ si scrive come

$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 \Longrightarrow v_1, v_2, v_3$ sono generatori di $\mathbb{R}^3$.

Visto: $\text{Span}(v_1, \ldots, v_n) = \{ \lambda_1 v_1 + \ldots + \lambda_n v_n : \lambda_1, \ldots, \lambda_n \in \mathbb{R} \}$

Q: l'espressione di $v \in \text{Span}(v_1, \ldots, v_n)$ come comb lin è unica?

Es: $v_1 = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad v_2 = \begin{pmatrix} 4 \\ -5 \end{pmatrix}$

$$v = 7 \cdot v_1 - 4 \cdot v_2 = \begin{pmatrix} 14 \\ 21 \end{pmatrix} + \begin{pmatrix} -16 \\ 20 \end{pmatrix} = \begin{pmatrix} -2 \\ 41 \end{pmatrix}$$

$v \in \mathrm{Span}(v_1, v_2)$. Esistono altre espressioni?

$$v = \lambda_1 v_1 + \lambda_2 v_2 \Rightarrow \begin{pmatrix} -2 \\ 41 \end{pmatrix} = \lambda_1 \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 4 \\ -5 \end{pmatrix}$$

$$= \begin{pmatrix} 2\lambda_1 + 4\lambda_2 \\ 3\lambda_1 - 5\lambda_2 \end{pmatrix}$$

$$\Rightarrow \begin{cases} 2\lambda_1 + 4\lambda_2 = -2 \\ 3\lambda_1 - 5\lambda_2 = 41 \end{cases} \Rightarrow \begin{cases} \lambda_1 = -2\lambda_2 - 1 \\ -6\lambda_2 - 3 - 5\lambda_2 = 41 \end{cases}$$

$$\Rightarrow \begin{cases} -11\lambda_2 = 44 \\ \lambda_1 = -2\lambda_2 - 1 \end{cases} \Rightarrow \begin{cases} \lambda_2 = -4 \\ \lambda_1 = 7 \end{cases}$$

Espressione è unica

Es: $v_1 = \begin{pmatrix} 3 \\ 7 \end{pmatrix}$ $v_2 = \begin{pmatrix} -5 \\ 3 \end{pmatrix}$ $v_3 = \begin{pmatrix} 12 \\ -7 \end{pmatrix}$

$$v = 0 \cdot \begin{pmatrix} 3 \\ 7 \end{pmatrix} + 4 \cdot \begin{pmatrix} -5 \\ 3 \end{pmatrix} + 3 \cdot \begin{pmatrix} 12 \\ -7 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} -20 \\ 12 \end{pmatrix} + \begin{pmatrix} 36 \\ -21 \end{pmatrix} = \begin{pmatrix} 16 \\ -9 \end{pmatrix}$$

Espressione è unica?

$$(*) \quad \lambda_1 \begin{pmatrix} 3 \\ 7 \end{pmatrix} + \lambda_2 \begin{pmatrix} -5 \\ 3 \end{pmatrix} + \lambda_3 \cdot \begin{pmatrix} 12 \\ -7 \end{pmatrix} = \begin{pmatrix} 16 \\ -9 \end{pmatrix}$$

$$\overset{?}{\Rightarrow} \quad \lambda_1 = 0 \quad \lambda_2 = 4 \quad \lambda_3 = 3$$

$$(*) \iff \begin{cases} 3\lambda_1 - 5\lambda_2 + 12\lambda_3 = 16 \\ 7\lambda_1 + 3\lambda_2 - 7\lambda_3 = -9 \end{cases}$$

$$\iff \begin{cases} \lambda_1 = \frac{1}{3}(5\lambda_2 - 12\lambda_3 + 16) \\ 7(5\lambda_2 - 12\lambda_3 + 16) + 9\lambda_2 - 21\lambda_3 = -27 \end{cases}$$

$$\iff \begin{cases} \lambda_1 = \dots \\ 44\lambda_2 - 105\lambda_3 = -139 \end{cases}$$

Posso scegliere ad es

- $\lambda_2 = -\frac{139}{44}$ $\lambda_3 = 0$ $\lambda_1 = \frac{1}{3} \cdot 5 \cdot -\frac{139}{44}$

- $\lambda_2 = 0$ $\lambda_3 = \frac{139}{105}$ $\lambda_1 = \frac{1}{3} \cdot -12 \cdot \frac{139}{44}$

- $\lambda_1 = 0$ $\lambda_2 = 4$ $\lambda_3 = 3$

$\Longrightarrow$ espressione <u>non</u> unica.

Q : un el. di $\mathrm{Span}(v_1, \dots, v_n)$ ha espr. unica?

$\tilde{Q}$: $0 \in \mathrm{Span}(v_1, \dots, v_n)$ ha

$0 \cdot v_1 + \dots + 0 \cdot v_n$ come unica espressione?

Def: diciamo che $v_1, \dots, v_n$ sono linearmente indipendenti se l'unica espressione di 0 è $0 \cdot v_1 + \dots + 0 \cdot v_n$, cioè se l'unica comb. lin.

che ha risultato nullo è quello a coeff tutti nulli.

<u>Prop</u>: $v_1, \dots, v_n$ lin. indip

$$\Updownarrow$$

ogni $v \in \mathrm{Span}(v_1, \dots, v_n)$ ha espressione unica come loro comb. lin.

<u>Dim</u>: $\Uparrow$ ovvio.

$\Downarrow$ Supponiamo $\lambda_1 v_1 + \dots + \lambda_n v_n = \mu_1 v_1 + \dots + \mu_n v_n$;

allora $(\lambda_1 - \mu_1) v_1 + \dots + (\lambda_n - \mu_n) \cdot v_n = 0$;

ho trovato comb. lin. con risultato 0

dunque per l'ipotesi i coeff sono tutti nulli:

$$\lambda_1 - \mu_1 = \dots = \lambda_n - \mu_n = 0$$

dunque $\mu_1 = \lambda_1, \dots, \mu_n = \lambda_n$ cioè

le due espressioni sono uguali. $\blacksquare$

$\boxed{2.3.15}$

- $f : \{\text{nat. pari}\} \longrightarrow \{\text{nat. dispari}\}$

  $f(n) = n+1$

- $g : \mathbb{N} \longrightarrow \{\text{nat. pari}\}$ $\qquad g(n) = 2n$

- $h : \mathbb{N} \longrightarrow \mathbb{Z}$ $\qquad$ cioè : conta $\mathbb{Z}$

$$h : \begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 \end{array}$$

$$h(n) = (-1)^{n+1}\left[\frac{n+1}{2}\right]$$

$\boxed{2.3.16}$ o) X, Y con n elementi

$f : X \to Y$ iniettiva $\Longrightarrow$ surgettiva.

Dimo per induzione su n.

PB $(n=0)$ $n = 1$ tutte le f bigettive (unica)

PI Sia vero che ogni $f : X \to Y$ iniettiva con X, Y n el. è surgettiva.

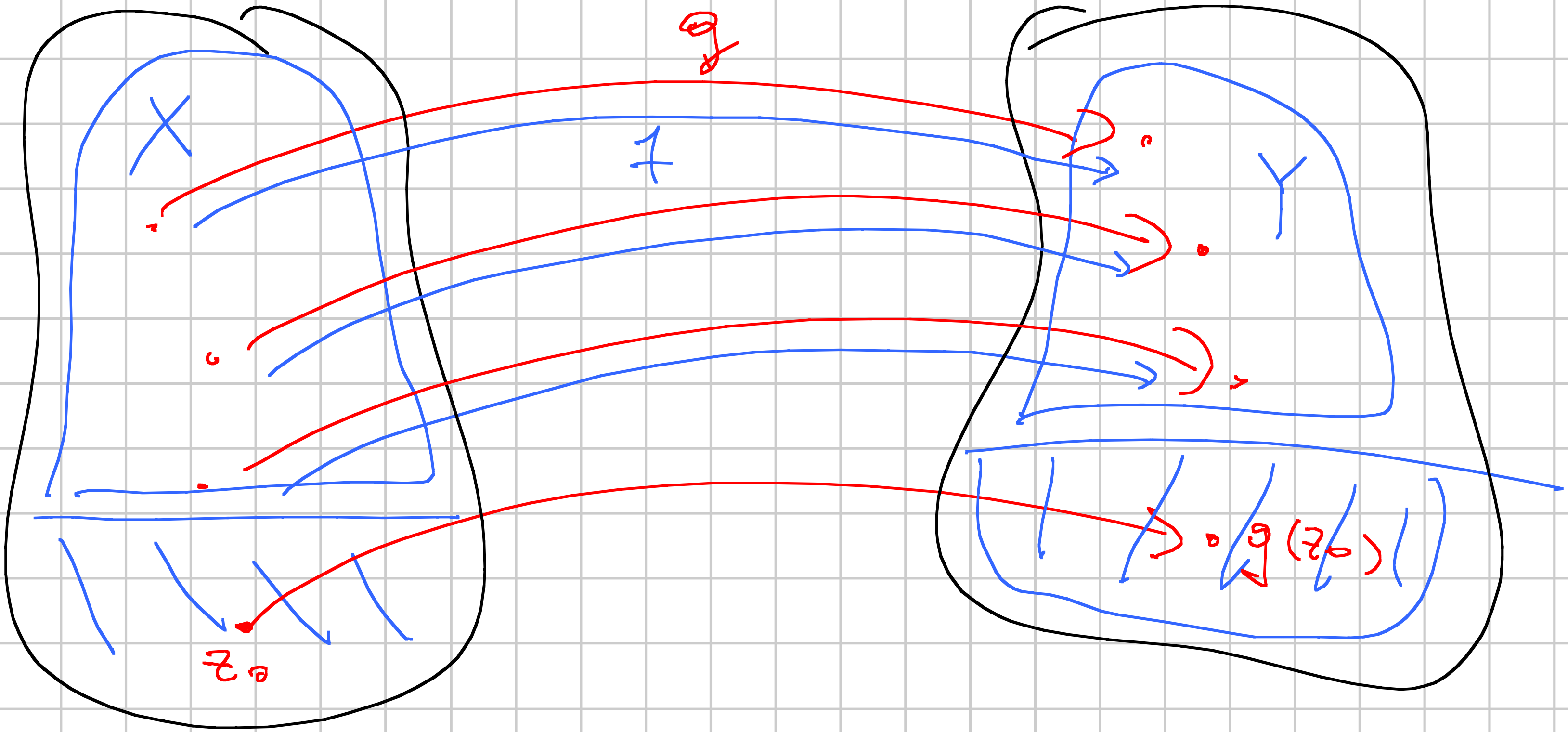
Prendo $g : Z \to W$ iniettiva con Z, W $n+1$ el.

Scelgo $z_0 \in Z$ e pongo $X = Z \setminus \{z_0\}$;

pongo $Y = W \setminus \{g(z_0)\}$ e osservo che

ponendo $f(x) = g(x)$ $\forall x \in X$ ho una

funzione da X a Y:



g iniettiva $\Rightarrow$ f iniettiva;

ipotesi induttiva $\Longrightarrow$ f surgettiva

$\mathrm{Im}(f) = Y$

$\Longrightarrow$ $\mathrm{Im}(g) = \mathrm{Im}(f) \cup \{g(z_0)\} = Z$

$\Longrightarrow$ g surgettiva.

•) $f: X \to Y$ surgettiva, X, Y n el. $\Longrightarrow$ f iniettiva.

$\forall y \in Y \; \exists x$ t.c. $y = f(x)$; scelgo un tale x

a caso e definisco $x = g(y)$. Ho trovato

$g : Y \to X$ t.c. $f(g(y)) = y \quad \forall y$

$\Rightarrow f \circ g = id_Y \Rightarrow g$ iniettiva

$\Rightarrow$ g bijettiva (dunque invertibile)
(visto sopra)

$\Rightarrow (f \circ g) \circ g^{-1} = id_Y \circ g^{-1}$

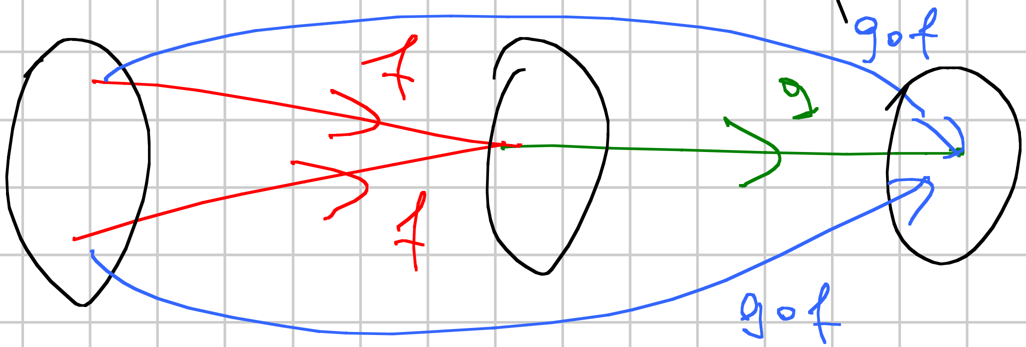
$\Rightarrow f \circ id_Y = g^{-1} \Rightarrow f = g^{-1}$

$\Rightarrow f$ invertibile; in particolare, iniettiva.

Oss:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & Y \arrow[r, "g"] & Z \end{tikzcd}$$

se $g \circ f$ è iniettiva allora f è iniettiva :



$\ast$ $g \circ f$ è surgettiva allora g è surgettiva.

$\boxed{2.3.17}$ Sia $n \geq 2$; $F_n = \{0, \dots, n-1\}$

= i possibili resti della divisione per n

- $a \oplus b$ = resto di $(a+b) : n$
- $a \odot b$ = resto di $(a \cdot b) : n$

Es: $n = 7$

$$3 \oplus 2 = 5$$
$$4 \oplus 5 = 2$$
$$3 \odot 2 = 6$$
$$4 \odot 5 = 6$$

Fatto: valgono tutte le proprietà di campo tranne l'esistenza dell'inverso; vediamo ad es. la distributiva:

$$a \odot (b \oplus c) = a \odot b \oplus a \odot c$$

Oss: calcolando una espressione con $\oplus$ e $\odot$ se eseguo la divisione per n (e prendo il resto) solo in fondo trovo lo stesso risultato (i multipli di n non scartati strada facendo si scartano con l'ultima divisione.

Dunque devo vedere che

$$a \cdot (b+c) \quad e \quad a \cdot b + a \cdot c$$

hanno stesso resto divisi per n: sono uguali!

Se n non è primo non vale l'esistenza dell'inverso moltiplicativo:

Oss: se trovo a, b con $a \odot b = 0$

ma $a \neq 0, b \neq 0$ allora a non può essere invertibile: se $\exists a^{-1}$

$$0 = a^{-1} \odot 0 = a^{-1} \odot (a \odot b) =$$

$$= (a^{-1} \odot a) \odot b = 1 \odot b = b$$

contraddizione

Es: $n = 6$ $\qquad F_6 = \{0, 1, 2, 3, 4, 5\}$

$$2 \odot 3 = 0$$

Invece: se n è primo allora ogni $a \in \mathbb{F}_n$
$a \neq 0$ ammette inverso $\Rightarrow \mathbb{F}_n$ campo.

Per trovare l'inverso di tale a fissato considero

$$f : \mathbb{F}_n \longrightarrow \mathbb{F}_n$$
$$b \longmapsto a \odot b.$$

Affermo che f è iniettiva; sapendo ciò trovo che è surgettiva $\Longrightarrow 1 \in \mathrm{Im}(f) \Longrightarrow \exists b$ t.c. $a \odot b = 1$

trovato inverso!

Iniettiva: siano $b_1, b_2 \{0, \dots, n-1\}$ t.c.

$$a \odot b_1 = a \odot b_2$$

$$\Longrightarrow a \odot (b_1 - b_2) = 0$$

$$\Longrightarrow a \cdot (b_1 - b_2) \text{ è multiplo di } n$$

Però $0 < a < n$, $0 \leq |b_1 - b_2| < n$

$\Longrightarrow$ poiché n è primo ciò può accadere solo se $|b_1 - b_2| = 0$; perciò iniettività.