

Algebra Lineare 11/10/17

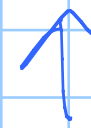
2.3.15 : divisione tra polinomi

dati $f(x), g(x) \in \mathbb{R}[x]$ con $\deg(g(x)) > 0$

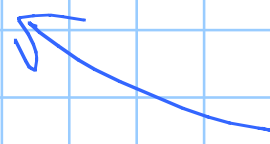
esistono unici $q(x), r(x)$ t.c.

$$f(x) = q(x) \cdot g(x) + r(x) \quad \text{e} \quad \deg(r(x)) < \deg(g(x))$$


dividendo


quoziente


divisore


resto

(analogo al caso $\mathbb{Z}$).

Es: $f(x) = 7x^5 - 4x^3 + 2x^2 - 9$

$$g(x) = x^3 - 5x^2 - x + 1$$

$$\begin{array}{r|l} 7x^5 & x^3 - 5x^2 - x + 1 \\ - 4x^3 + 2x^2 & \\ - 9 & \\ \hline -7x^5 + 35x^4 + 7x^3 - 7x^2 & \\ \hline 35x^4 + 7x^3 - 7x^2 & \\ - 9 & \end{array}$$

$7x^2 + 35x + 178$
quoziente

$$-35x^4 + 175x^3 + 35x^2 - 35x - 9$$

$$\begin{array}{r} 178x^3 + 30x^2 - 35x - 9 \\ -178x^3 + 890x^2 + 178x - 178 \end{array}$$

$$920x^2 + 143x - 187$$

resto

2.1.3. Consideriamo $F_2 = \{0, 1\}$ con queste operaz.:

$$0 + 0 = 0 \quad 0 + 1 = 1 \quad 1 + 0 = 1 \quad 1 + 1 = 0$$

$$0 \cdot 0 = 0 \quad 0 \cdot 1 = 0 \quad 1 \cdot 0 = 0 \quad 1 \cdot 1 = 1$$

Verificare che $\bar{F}_2$ è un campo.

Associative del $+$ ($\exists$):

$$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \{0, 1\}$$

(8 casi)

$$0 + (1 + 1) = (0 + 1) + 1$$

$$\downarrow$$
$$0 + 0 = 0$$

$$\underbrace{\quad}_{1+1=0} \quad \checkmark$$

tutte verifiche facili (regole spiegate da
 $0 = \text{parità}$ $1 = \text{disparità}$)

2.3.19 : Siano X, Y insiemi finiti con lo stesso numero n di elementi. Allora:

- (1) Se $f: X \rightarrow Y$ è iniettiva, è anche surgettiva.
- (2) Se $f: X \rightarrow Y$ è surgettivo, è anche iniettiva.

(1) Per induzione su $n \geq 1$.

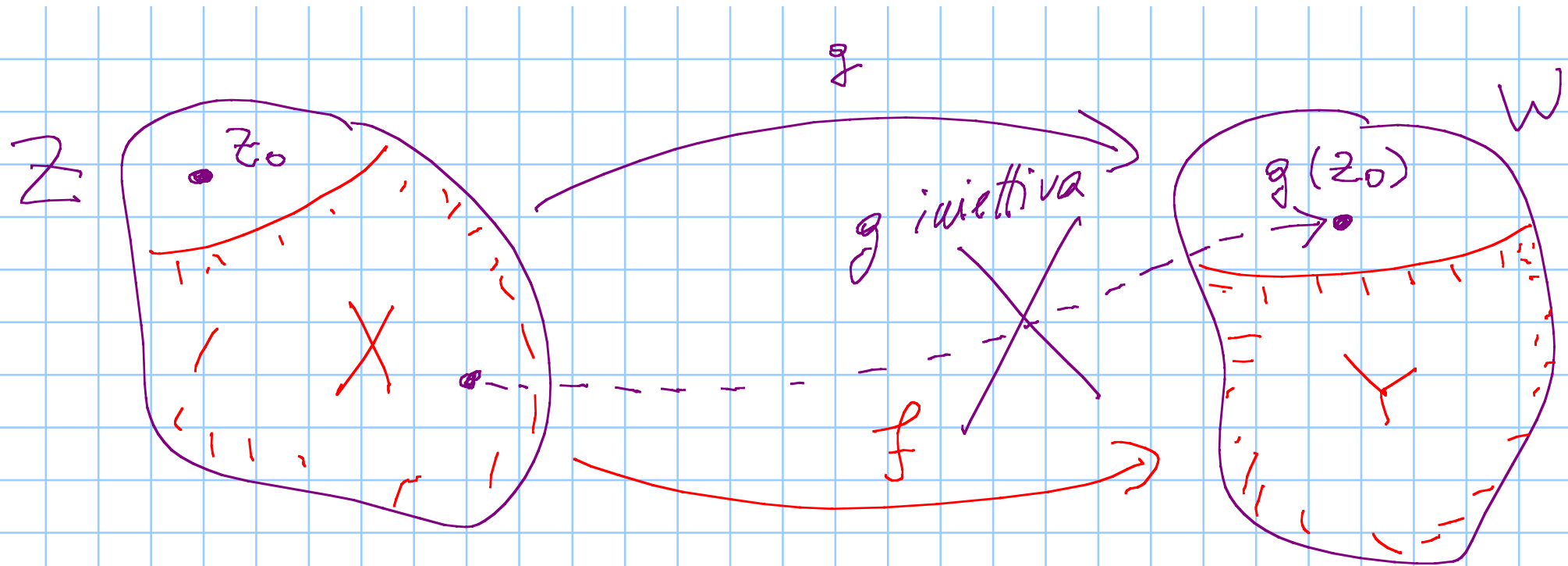
Ogni $f: \{*\} \rightarrow \{*\}$ è sempre sia iniettiva sia surgettiva.

Ipotesi induttive: supponiamo che ogni

$f: X \rightarrow Y$ iniettiva con X, Y aventi n elementi
sia anche surgettiva.

Prendiamo una $g: Z \rightarrow W$ iniettiva con
 Z, W aventi $n+1$ elementi; tesi: g surgettiva

Scego $z_0 \in Z$ e considero $X = Z \setminus \{z_0\}$;



Posso definire $f : X \rightarrow Y$ ponendo $f(x) = g(x)$
 $(Y = W \setminus \{g(z_0)\})$, $\forall x \in X$

f è ancora iniettiva, X, Y hanno n elementi
 $\Rightarrow f$ surgettiva $\Rightarrow g$ surgettiva.

(2) Considero $f: X \rightarrow Y$ surgettiva; X, Y n elem.

Definisco una $g: Y \rightarrow X$ così:

per ogni $y \in Y$ scelgo $x \in X$ t.c. $f(x) = y$
e pongo $g(y) = x$. Affermo che g è

iniettiva: se $g(y_1) = x$ e $g(y_2) = x$;
per costruzione ho $f(x) = y_1$ e $f(x) = y_2$
dunque $y_1 = y_2$. La (1) garantisce che
 g è surgettiva $\Rightarrow$ invertibile. Dunque
 $f = g^{-1}$ è bigettiva.

Richiamo: $f: X \rightarrow Y$ è invertibile se

esiste $g: Y \rightarrow X$ t.c. $g \circ f = id_X$ e $f \circ g = id_Y$,
dove

$$id_X: X \rightarrow X$$

$$id_X(x) = x$$

$$id_Y: Y \rightarrow Y$$

$$id_Y(y) = y ;$$

tale g è detta inversa di f .

Oss: (1) f è invertibile $\iff$ è biettiva

(2) Per concludere che g è l'inversa di f non basta sapere una sola delle proprietà $f \circ g = \text{id}_Y$ o $g \circ f = \text{id}_X$.

Esempio: $X = Y = \mathbb{N}$; $f, g: \mathbb{N} \rightarrow \mathbb{N}$

$$f(m) = m + 1 \quad g(m) = \begin{cases} 0 & \text{se } m = 0 \\ m - 1 & \text{se } m \geq 1 \end{cases}$$

f iniettiva non surg. 

g non iniettiva $\supset$ sur $\leftarrow$ non invertibili

Pero: $(g \circ f)(n) = g(f(n)) = g(n+1) = n$
 $\Rightarrow g \circ f = \text{id}_{\mathbb{N}}$

(3) Se so già che f è invertibile
una sola delle due relazioni
 $g \circ f = \text{id}_X$ oppure $f \circ g = \text{id}_Y$

implica l'altra e dunque che $g = f^{-1}$.

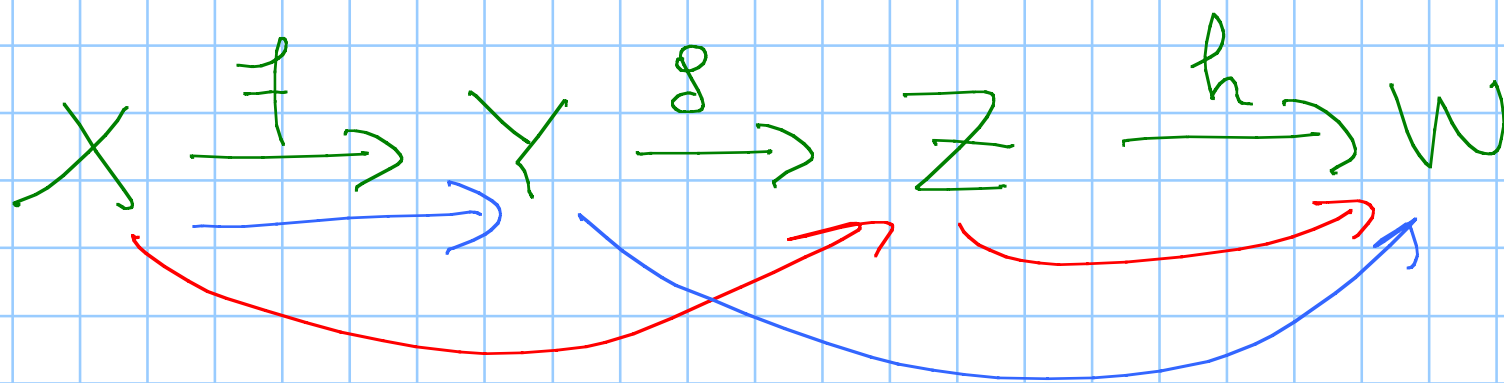
$$g \circ f = \text{id}_X \Rightarrow (g \circ f) \circ f^{-1} = \text{id}_X \circ f^{-1}$$

$$\Rightarrow g \circ (f \circ f^{-1}) = f^{-1} \Rightarrow g \circ \text{id}_Y = f^{-1} \Rightarrow g = f^{-1}$$

↑
• associativa

$$(\text{id}_X \circ f^{-1})(y) = \text{id}_X(f^{-1}(y)) = f^{-1}(y)$$

$$\begin{aligned}
 f \circ g &= \text{id}_Y \Rightarrow f^{-1} \circ (f \circ g) = f^{-1} \circ \text{id}_Y \\
 &\Rightarrow (f^{-1} \circ f) \circ g = f^{-1} \\
 &\Rightarrow \text{id}_X \circ g = f^{-1} \Rightarrow g \circ f^{-1}
 \end{aligned}$$



$$\underline{h \circ (g \circ f)} \neq \underline{(h \circ g) \circ f}$$

hanno dominio X e codom. W

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

$$\parallel$$

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

$$\parallel$$

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

$$h(g'(f(x)))$$

$$h(g(f(x)))$$

$$\equiv$$

2.3.20 : $m \in \mathbb{N}$ $m \geq 2$ fissato

$$\mathbb{F}_m = \{0, 1, \dots, m-1\}$$

con queste operazioni (aritmetica modulo m):

le operazioni solite in cui ogni numero $k \in \mathbb{N}$ viene sostituito dal resto della divisione $k : m$.

Es: $m = 8$ $F_8 = \{0, 1, 2, \dots, 7\}$

$$2 + 3 = 5$$

$$5 + 4 = 1$$

$$2 \cdot 4 = 0$$

$$5 \cdot 7 = 3$$

Fatto: valgono sempre le proprietà (1)-(9)
di campo tranne la (6) esistenza
dell'inverso moltiplicativo.

Valgono tutte tranne (2) - opposto - e (6):

"nelle proprietà valide su $\mathbb{Z}$ basta sostituire
ogni numero con suo resto delle div. per m "

$$(2) \quad -k = m-k \quad \{0, 1, \dots, m-1\}$$

$$(m=8, -5=3)$$

Fatto: (6) vale se e solo se m è primo.

$$(6) \quad m=15 \quad k=8 \quad 8^{-1}=2$$

$K = 5$ je esiste 5^{-1} anzi

$$5 \cdot 5^{-1} = 1 \Rightarrow 3 \cdot (5 \cdot 5^{-1}) = 3 \cdot 1 = 3$$

$$\parallel \\ (3 \cdot 5) \cdot 5^{-1} = 0 \cdot 5^{-1} = 0$$

assunto

$$m = 7$$

$$1^{-1} = 1$$

$$3^{-1} = 5$$

$$5^{-1} = 3$$

$$2^{-1} = 4$$

$$4^{-1} = 2$$

$$6^{-1} = 1.$$

————— 0 —————

V sp. vett. su $\mathbb{R}$; $\mathcal{B} = (v_1, \dots, v_m)$ si dice base se
 $v_1, \dots, v_m$ generano V e sono lin. indep.

ovvero se ogni $v \in V$ si scrive in modo unico
come $v = \alpha_1 v_1 + \dots + \alpha_m v_m$ — Tale $\alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \in \mathbb{R}^m$
è detto vettore delle coordinate di V rispetto a $\mathcal{B}$
e indicato con $[v]_{\mathcal{B}}$ —

Esempi:

• base canonica di $\mathbb{R}^m$

$$\mathcal{E}_m = (e_1^{(m)}, \dots, e_m^{(m)}) \quad \text{dove}$$

$$e_j^{(m)} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j \quad \left. \vphantom{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}} \right\} m$$

$$m=3 \quad \mathcal{E}_3 = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

Notazione : se m è chiaro dal contesto
 scrivo $e_j \in \mathbb{R}^m$ non $e_j^{(m)}$.

$$e_3 \in \mathbb{R}^4 \quad \text{è} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Prova che ogni $x \in \mathbb{R}^m$ si scrive in modo unico

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \boxed{x_1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \boxed{x_2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + \boxed{x_m} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$\Rightarrow \text{è base e } [x]_{\mathcal{E}_m} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = x.$$

• $M_{m \times m}(\mathbb{R})$ Base canonica

$$\Sigma_{m \times m} = \left\{ E_{ij}^{(m \times m)} : i = 1 \dots m \quad j = 1 \dots m \right\}$$

dove E_{ij} ha 1 al posto i, j
e 0 altrove

con ordinamento lexicografico (come dizionario)

$$E_{11}, E_{12}, \dots, E_{1m}, E_{21}, E_{22}, \dots, E_{2m}, E_{31}, \dots$$

$$\underline{Es}: M_{3 \times 2}(\mathbb{R})$$

$$\begin{pmatrix} \sqrt{3} & -1 \\ 4 & 7 \\ 19 & 4/3 \end{pmatrix} = \boxed{\sqrt{3}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \boxed{-1} \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \boxed{4} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} \\ + \boxed{7} \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} + \boxed{19} \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} + \boxed{4/3} \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\left([A]_{\mathbb{R}^{n \times m}} \right)_{ij} = (A)_{ij}$$

• $\mathbb{R}_{\leq d}[t]$ base canonica
 $1, t, t^2, \dots, t^d$

Dato $p(t) \in \mathbb{R}_{\leq d}[t]$, cioè
 $p(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_d t^d$ devo scrivere

$$p(t) = \boxed{a_0} \cdot 1 + \boxed{a_1} \cdot t + \boxed{a_2} t^2 + \dots + \boxed{a_d} t^d$$

$$\boxed{p(t)}_{(1, t, \dots, t^d)} = i \text{ coeff. di } p(t).$$

————— 0 —————

Prop: se V ha base $\mathcal{B} = (v_1, \dots, v_m)$
 la funzione $[\cdot]_{\mathcal{B}} : V \longrightarrow \mathbb{R}^m$
 $v \longmapsto [v]_{\mathcal{B}}$

è biettiva e preserva le operazioni di sp. vett.:

$$1) [\underline{0}]_{\mathcal{B}} = \underline{0}$$

$$2) [\underline{v+w}]_{\mathcal{B}} = [\underline{v}]_{\mathcal{B}} + [\underline{w}]_{\mathcal{B}}$$

$$3) [\underline{\alpha \cdot v}]_{\mathcal{B}} = \alpha \cdot [\underline{v}]_{\mathcal{B}}$$

in V

in $\mathbb{R}^n$

Dunque: V è "uguale" a $\mathbb{R}^m$ come sp. vett.

Q: per $m \neq n$, $\mathbb{R}^m$ e $\mathbb{R}^n$ sono uguali
come spaz. vett.?

[No]

Attenzione: Sono uguali come insiemi
(esistono bipezzioni tra loro).

Dimo (Prop) :

iniettiva : $[v]_{\mathcal{B}} = [w]_{\mathcal{B}}$, le chiamo α

$$\Rightarrow v = \alpha_1 v_1 + \dots + \alpha_m v_m$$

$$w = \alpha_1 v_1 + \dots + \alpha_m v_m \Rightarrow w = v$$

surgettiva : $\alpha \in \mathbb{R}^m$ cerco v t.c. $[v]_{\mathcal{B}} = \alpha$

Scelgo $v = x_1 v_1 + \dots + x_m v_m$

Operaz: facciamo $[v+w]_{\mathcal{B}} = [v]_{\mathcal{B}} + [w]_{\mathcal{B}}$:

Supponiamo

$$[v]_{\mathcal{B}} = x$$

$$[w]_{\mathcal{B}} = y$$

Cioè

Cioè

$$v = x_1 v_1 + \dots + x_m v_m$$

$$w = y_1 v_1 + \dots + y_m v_m$$

Devo vedere che $[v+w]_{\mathcal{B}} = x+y$; ma

$$v+w = (x_1+y_1)v_1 + \dots + (x_n+y_n)v_n$$

$\Rightarrow [v+w]_{\mathcal{B}}$ ha componente j -esima
uguale a x_j+y_j

$$\Rightarrow [v+w]_{\mathcal{B}} = x+y.$$

