Algebra Lineare 16/10/13

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

$\mathcal{B} = (v_1, \dots, v_n)$ è base se $\forall v \in V \; \exists! \, x \in \mathbb{R}^n$ t.c. $v = x_1 v_1 + \dots + x_n v_n$

In tal caso $x = [v]_{\mathcal{B}}$ (coord. di v rispetto $\mathcal{B}$).

Prop: $\phi_{\mathcal{B}} : V \longrightarrow \mathbb{R}^n$, $v \longmapsto [v]_{\mathcal{B}}$ è biiettiva e conserva le operazioni.

Def: $\psi_{\mathcal{B}} : \mathbb{R}^n \to V$

$$x \longmapsto x_1 v_1 + \dots + x_n v_n$$

Prop: $\mathcal{B}$ base $\Rightarrow \psi_{\mathcal{B}}$ bijective

($\exists \Rightarrow \psi_{\mathcal{B}}$ surj ; $! \Rightarrow \psi_{\mathcal{B}}$ inj.)

Chiaramente $\psi_{\mathcal{B}} = \phi_{\mathcal{B}}^{-1} \Rightarrow \phi_{\mathcal{B}}$ bijective.

Preserva le operaz:

- $\phi_{\mathcal{B}}(0) = 0 \quad : \quad 0 = 0 \cdot v_1 + \dots + 0 \cdot v_n$

$\in V \quad \in \mathbb{R}^n \qquad \in V \quad \in \mathbb{R} \qquad \in \mathbb{R}$

$$\Longrightarrow [0]_{\mathcal{B}} = 0 \qquad \checkmark$$

- $\phi_{\mathcal{B}}(v+w) \overset{?}{=} \phi_{\mathcal{B}}(v) + \phi_{\mathcal{B}}(w)$

  $x = [v]_{\mathcal{B}}$ cioè $v = x_1 v_1 + \dots + x_n v_n$

  $y = [w]_{\mathcal{B}}$ cioè $w = y_1 v_1 + \dots + y_n v_n$

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

è espr. di $v+w$ come comb. lin. di $v_1, \dots, v_n$

$$\Longrightarrow [v+w]_{\mathcal{B}} = x+y \qquad \checkmark$$

- $\phi_{\mathcal{B}}(\lambda v) = \lambda \cdot \phi_{\mathcal{B}}(v)$. ✓

VIII

($\phi_{\mathcal{B}}$ "identifica" V e $\mathbb{R}^n$ come sp. vett.)

Oss: $\mathcal{B} = (v_1, \dots, v_n)$ base $\iff$ $v_1, \dots, v_n$ lin. ind. e generano

Teo: $\mathcal{B}_1, \mathcal{B}_2$ basi di $V \Rightarrow$ hanno stesso numero di el.

Prop: $v_1, \dots, v_n$ l.i. $\in Span(w_1, \dots, w_m) \Rightarrow n \leq m$

Verifica che Prop $\Rightarrow$ Teo:

Siano $\mathcal{B}_1 = (v_1, \dots, v_n)$ basi di V

$\mathcal{B}_2 = (w_1, \dots, w_m)$

$v_1, \dots, v_n$ l.i. $\in V = Span(w_1, \dots, w_m) \xRightarrow{Prop} n \leq m$

$w_1, \dots, w_m$ l.i. $\in V = Span(v_1, \dots, v_n) \xRightarrow{Prop} m \leq n$

$\Longrightarrow m = n$. ▨

Prop: $v_1, \dots, v_n$ l.i. $\in Span(w_1, \dots, w_m) \Rightarrow n \leq m$

Dim: La dimostro per induzione su n:

$P(n)$ = "comunque prendi $v_1, \dots, v_n \in V$ l.i.
e $w_1, \dots, w_m \in V$ t.c. $v_1, \dots, v_n \in Span(w_1, \dots, w_m)$
si ha $n \leq m$"

Passo base: $n = 0$ ($0 \leq m$ ovvio)

$n = 1$: v_1 l.i.: l'unico caso in cui $\alpha_1 \cdot v_1 = 0$ è $\alpha_1 = 0$

$\Rightarrow v_1 \neq 0$; $v_1 \in \underbrace{Span(w_1, \dots, w_m)}_{\text{se } m=0 \text{ è } \{0\} \,:\, \underline{\text{No}} \Rightarrow m \geq 1}$

$\| \; 0$

Passo induttivo: ipotesi $\mathcal{P}(n)$;

tesi $\mathcal{P}(n+1)$: "$x_0, \dots, x_n$ l.i. $\in Span(y_1, \dots, y_k) \Rightarrow n+1 \leq k$"

So che $x_j = \sum_{i=1}^{k} \lambda_{ji} y_i$ _ Noto che $x_0 \neq 0$

(altrimenti $1 \cdot x_0 + 0 \cdot x_1 + \dots + 0 \cdot x_n = 0$ viola ipotesi $x_1, \dots, x_n$ l.i.)

$\| \; 0$

Dunque qualche a_{0i} è $\neq 0$; cambiando l'ordine degli y_i supponga $a_{01} \neq 0$. Pongo:

$$v_j = x_j - \frac{a_{j1}}{a_{01}} \cdot x_0 \qquad j = 1, \dots, n$$

Affermo:

•) $v_1, \dots, v_n$ l.i. •) $v_1, \dots, v_n \in \mathrm{Span}(y_2, \dots, y_k)$

Da ciò segue per $P(n)$ che $n \leq k-1$ cioè $n+1 \leq k$ dunque la tesi induttiva. Le dimostro:

•) $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$

$\Rightarrow \alpha_1 (x_1 - (\dots) x_0) + \dots + \alpha_m (x_m - (\dots) x_0) = 0$

$\Rightarrow (\dots) x_0 + \alpha_1 x_1 + \dots + \alpha_m x_m = 0$ wie $x_0, \dots, x_m$ l. i.

$\Rightarrow (\dots) = \alpha_1 = \dots = \alpha_m = 0$. Ok

••) $v_j = x_j - \frac{\lambda_{j1}}{\lambda_{01}} \cdot x_0$

$= \sum_{i=1}^{k} \lambda_{ji} y_i - \frac{\lambda_{j1}}{\lambda_{01}} \cdot \sum_{i=1}^{m} \lambda_{0i} y_i$

$= \lambda_{j1} \cdot y_1 + \sum_{i=2}^{k} \lambda_{ji} y_i - \frac{\lambda_{j1}}{\lambda_{01}} \cdot \lambda_{01} y_1 - \sum_{i=2}^{k} \frac{\lambda_{j1}}{\lambda_{01}} \cdot \lambda_{0i} y_i$

$$= \sum_{i=2}^{k} (\dots)\, y_i \,.$$

VIII

Def: se V ha base finita allora $\dim_{\mathbb{R}}(V) =$ num. di el. di qualsiasi base

altrimenti $\dim_{\mathbb{R}}(V) = +\infty$.

Es: $\dim(\mathbb{R}^n) = n$, $\dim(M_{m\times n}(\mathbb{R})) = m \cdot n$,

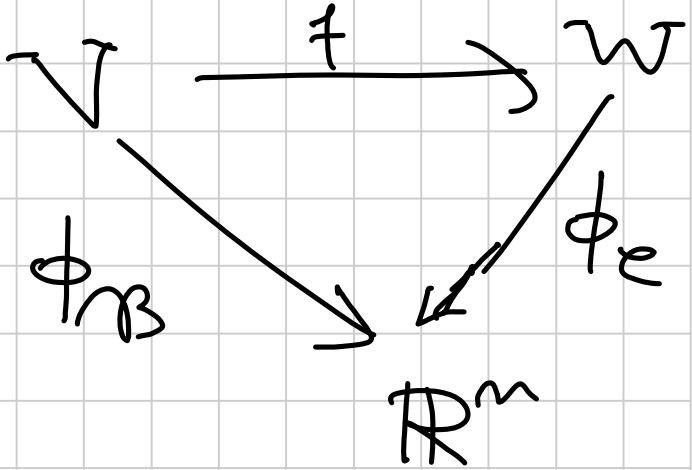
$\dim(\mathbb{R}_{\le d}[x]) = d+1$, $\dim(\mathbb{R}[x]) = +\infty$.

Prop: V, W di $\dim < +\infty$;

$\exists f: V \to W$ biiettive $\iff \dim_{\mathbb{R}} V = \dim_{\mathbb{R}} W$.
che rispetta le operazioni

Dim: $\Longrightarrow$: Se $\mathcal{B} = (v_1, \dots, v_n)$ è base di V
allora $(f(v_1), \dots, f(v_n))$ è base di W.

$\Longleftarrow$: $\mathcal{B} = (v_1, \dots, v_n)$ base di V
$\mathcal{C} = (w_1, \dots, w_m)$ base di W allora



$f = \phi_{\mathcal{C}}^{-1} \circ \phi_{\mathcal{B}}$. ☐

Prop: $\dim_{\mathbb{R}}(V) = m$;

•) $v_1, \dots, v_k \in V$ lin. indip. $\Rightarrow k \leq m$

••) $v_1, \dots, v_k$ generano $V \Rightarrow k \geq m$

Dim: Se $w_1, \dots, w_m$ è base di V

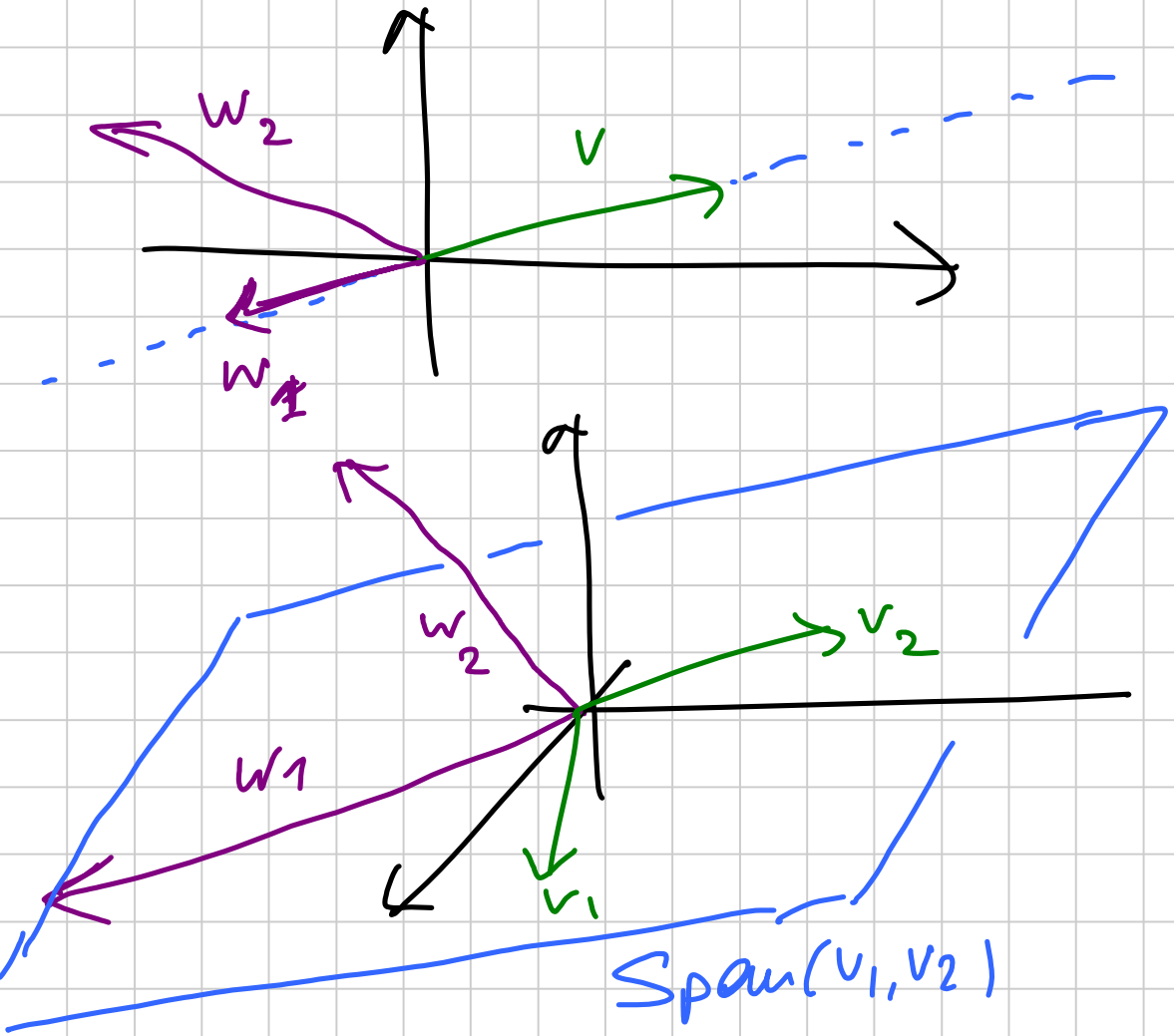
•) $v_1, \dots, v_k$ l.i. $\in \mathrm{Span}(w_1, \dots, w_n) \xRightarrow{\text{Prop}} k \leq n$

••) $w_1, \dots, w_n$ l.i. $\in V = \mathrm{Span}(v_1, \dots, v_k) \xRightarrow{\text{Prop}} n \leq k$. ☒

"Come costruire basi di V."

<u>Lem</u>: Siano $v_1, \dots, v_n$ l.i., $v_0 \in V$.

$v_0, v_1, \dots, v_n$ l.i. $\iff v_0 \notin \mathrm{Span}(v_1, \dots, v_n)$



v, w_1 lin. dip.

v, w_2 lin. indip.

v_1, v_2, w_1 lin. dip.

v_1, v_2, w_2 lin. indip.

$v_0, v_1, \dots, v_n$ l.i. $\iff v_0 \notin \mathrm{Span}(v_1, \dots, v_n)$

$\Rightarrow$ Se p.a. $v_0 \notin \mathrm{Span}(v_1, \dots, v_n)$

allora $v_0 = \alpha_1 v_1 + \dots + \alpha_n v_n$

allora $1 \cdot v_0 - \alpha_1 v_1 - \dots - \alpha_n v_n = 0$

$\neq$

0

viola ipotesi $v_0, \dots v_n$ l.i.

$\Leftarrow$ Supponiamo $\alpha_0 v_0 + \alpha_1 v_1 + \dots + \alpha_n v_n = 0$.

$\alpha_0 = 0 \Rightarrow \alpha_1 v_1 + \cdots + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$ ✓

$\alpha_0 \neq 0 \Rightarrow v_0 = -\frac{\alpha_1}{\alpha_0} v_1 - \cdots - \frac{\alpha_n}{\alpha_0} v_n \in \mathrm{Span}(v_1, \ldots, v_n)$

NO

∎

Esercizi (4/10/13)

9) $F_2 = \{0, 1\}$

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

operazioni: commutative ✓

$\exists$ elementi neutri ✓

$\exists$ opposti + inversi ✓

Associatività: $a \oplus (b \oplus c) \stackrel{?}{=} (a \oplus b) \oplus c$

$\forall\ a, b, c \in F_2$. Ad esempio:

$a = 0,\ b = 1,\ c = 0$

$$0 \oplus (1 \oplus 0) \overset{\checkmark}{=} (0 \oplus 1) \oplus 0$$

$$0 \oplus \underbrace{(1 \oplus 0)}_{1} = \underbrace{(0 \oplus 1)}_{1} \oplus 0$$

$$1 = 1$$

Altre possibilità: stessa verifica

Distributività: $a, b, c \in F_2$

$$a \odot (b \oplus c) \stackrel{?}{=} (a \odot b) \oplus (a \odot c)$$

$\forall\, a, b, c \in F_2$

Esempio: $a = 1,\ b = 0,\ c = 1$

$$1 \odot (0 \oplus 1) \stackrel{\checkmark}{=} (1 \odot 0) \oplus (1 \odot 1)$$

$$1 \odot 1 = 1 \qquad 0 \oplus 1 = 1$$

$$1 = 1$$

$$1 \odot 0 = 0 \qquad 1 \odot 1 = 1$$

$$0 \oplus 1 = 1$$

10) $f: \mathbb{N} \longrightarrow \mathbb{N}^2 \quad f(n) = (n^2, 3n-2)$

iniettività: $\exists\ n_1, n_2 \in \mathbb{N}, n_1 \neq n_2$ con $f(n_1) = f(n_2)$?

$f(n_1) = (n_1^2, 3n_1 - 2) = f(n_2) = (n_2^2, 3n_2 - 2)$

$\Rightarrow 3n_1 - 2 = 3n_2 - 2 \Rightarrow n_1 = n_2$

$\Rightarrow$ f iniettiva

Surgettività: dato $(a,b) \in \mathbb{N}^2$,

$\exists\, ?\ n \in \mathbb{N}$ t.c. $f(n) = (a,b)$?

$\|$

$(n^2, 3n-2)$

Chiaramente $(3,0) \notin \mathrm{Im}(f) = f(\mathbb{N})$

perché 3 non è un quadrato.

$\Rightarrow$ f non è surgettiva

$$\Delta = \{ (m,n) \in \mathbb{N}^2 \mid m = n \}$$

"tale che"

$$f^{-1}(\Delta) = \{ n \in \mathbb{N} \mid f(n) \in \Delta \}$$

"controimmagine di Δ"

$$f(n) = (n^2, 3n-2)$$

$$\Leftrightarrow \quad n^2 = 3n - 2$$

$\Leftrightarrow \quad n^2 - 3n + 2 = 0$

le radici reali di $\uparrow$ sono:

$$\frac{3 \pm \sqrt{9-8}}{2} \begin{cases} 2 \\ 1 \end{cases} \in \mathbb{N}$$

$$\Rightarrow f^{-1}(\Delta) = \{1, 2\} \subseteq \mathbb{N}$$

11) $D = \{\text{numeri naturali dispari}\}$

$= \{1, 3, 5, 7, \dots\}$

$g : D \longrightarrow \mathbb{N}$ bigettiva ?

$m \longmapsto \dfrac{m+1}{2}$

$1 \longmapsto 1$

$3 \longmapsto 2$

$5 \longmapsto 3$

g iniettiva? $\quad g(m_1) = g(m_2)$

$\Leftrightarrow \quad \frac{m_1 + 1}{2} = \frac{m_2 + 1}{2} \Leftrightarrow m_1 = m_2$

$\Rightarrow$ g iniettiva ✓

g surgettiva? $\quad n \in \mathbb{N} \Rightarrow \exists\, m$ t.c.

$n = g(m)$?

$$n = \frac{m+1}{2} \iff m = 2n - 1$$

$$\Rightarrow g(2n-1) = n \Rightarrow g \text{ surgettiva}$$

$$\Rightarrow g \text{ bigettiva}$$

12) X, Y insiemi, $|X| = |Y| = n$

$f: X \to Y$ iniettiva ↖ ↑ "numero di elementi"

<u>$n = 0$</u> : $X = Y = \emptyset$

non c'è nulla da dim. per il passo base

$$\begin{array}{ccc} X & \ni & x \\ \cup & & \cup \\ Y & \ni & f(x) \end{array}$$

$$f|_{X\setminus\{x\}} : X\setminus\{x\} \longrightarrow Y\setminus\{f(x)\}$$

$X\setminus\{x\}$ è ben definito perché, essendo f iniettiva, x è l'unico elemento di X che va in $f(x)$.

è ancora iniettiva

$|X \setminus \{x\}| = |Y \setminus \{f(x)\}| = n-1$

$\Rightarrow$ (ipotesi induttiva: $f|_{X \setminus \{x\}}$ è surgettiva su $Y \setminus \{f(x)\}$)

$\Rightarrow f$ è surgettiva

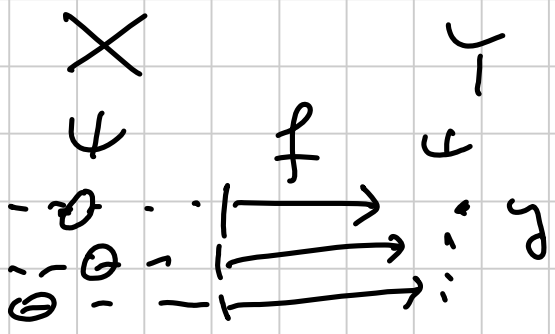
$\Rightarrow$ per induzione, f surgettiva

Seconda parte:

$|X| = |Y| = n$, $f : X \to Y$ surgettiva:

$\forall\ y \in Y,\ \exists\ x$ t.c. $f(x) = y$

voglio definire un'applicazione iniettiva $g : Y \to X$



$y \longmapsto x$, scelto a caso tra quello con immagine y

g è iniettiva "per costruzione":

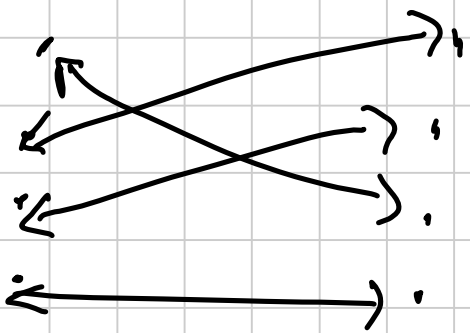
$$g(y_1) = g(y_2) \Rightarrow f(g(y_1)) = f(g(y_2))$$

$$\Rightarrow (\text{per la prima parte}) \; g \text{ è bigettiva}$$

$$Y \underset{g^{-1}}{\overset{g}{\rightleftarrows}} X \qquad \text{bigettiva: } \forall x \in X \quad \exists! \, y \in Y \text{ t.c. } g(y) = x$$

$\Rightarrow$ posso definire $g^{-1} : X \to Y$

$x \longmapsto y$



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

$g \circ g^{-1} = id_X$

Ma $f \circ g = id_Y \Rightarrow$

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

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

f ↑ è iniettiva:

$g \circ g^{-1} = id_X$

$g^{-1}(x_1) = g^{-1}(x_2) \Rightarrow g(g^{-1}(x_1)) = g(g^{-1}(x_2))$

$x_1 \qquad\qquad x_2$

Ultima parte: $|X| = n$

$f : X \to X$ f iniettiva $\Rightarrow$ surgettiva (per la prima parte)

f surgettiva $\Rightarrow$ f iniettiva (per la seconda parte) _

13) $F_n = \{0, 1, 2, \dots, n-1\}$.

$a \oplus b :=$ resto della divisione $(a+b) : n$

$$a + b = q \cdot n + a \oplus b$$

$$a \oplus b \in F_n$$

$$a \cdot b = q' \cdot n + a \odot b$$

$$a \odot b \in F_n$$

$a + b = b + a$, $a \cdot b = b \cdot a$

$\Rightarrow a \oplus b = b \oplus a$, $a \odot b = b \odot a$

chiaramente 0, 1 sono gli ovvi elementi neutri.

Associatività:

$$a \oplus (b \oplus c) \stackrel{?}{=} (a \oplus b) \oplus c$$

$$a + b \oplus c = q_1 \cdot n + a \oplus (b \oplus c)$$

$$b + c = q_2 \cdot n + b \oplus c$$

$$\Rightarrow a + b + c - q_2 \cdot n = q_1 \cdot n + a \oplus (b \oplus c)$$

$$a + b + c = (q_1 + q_2) \cdot n + a \oplus (b \oplus c)$$

resto di $(a+b+c) : n$

$$a \oplus b + c = q_3 \cdot n + (a \oplus b) \oplus c$$

$$a + b = q_4 \cdot n + a \oplus b$$

$$\Rightarrow a + b + c = (q_3 + q_4) \cdot n + (a \oplus b) \oplus c$$

"resto della divisione $(a+b+c) : n$"

l'associatività del prodotto, stessa maniera.

distributività: analoga verifica

Opposti: 0 ha opposto 0

$a \neq 0$ ha opposto $n - a$

Inversi: n primo.

$a \in F_n$, $a \neq 0$

$$\begin{aligned} F_n &\longrightarrow F_n \\ b &\longmapsto a \odot b \end{aligned}$$

è iniettiva:

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

$$a \cdot b_1 = q_1 \cdot n + a \odot b_1$$

$$a \cdot b_2 = q_2 \cdot n + a \odot b_2$$

$$a \cdot (b_1 - b_2) = n \cdot (q_1 - q_2)$$

↑ primo

$n > a$

$\Rightarrow$ n divide $b_1 - b_2$ $\Rightarrow$ $b_1 - b_2 = 0$

$\Rightarrow$ l'applicazione iniettiva $\Rightarrow$

è surgettiva $\Rightarrow$ $1 = a \odot b$

$\uparrow$ è l'inverso di a!

Se n è composto, $n = a_1 \cdot a_2$,

$a_1, a_2 > 1 \Rightarrow a_1 \odot a_2 = 0$ in $\mathbb{F}_n$

se F_n fosse un campo,

$$a_1 \odot a_2 = 0 \implies$$

$$(a_1 \odot a_2) \odot a_2^{-1} = 0 \odot a_2^{-1} = 0$$

$$\parallel$$

$$a_1 \odot (a_2 \odot a_2^{-1})$$

$$\parallel$$

$$1 \quad " \quad a_1$$