Appunti per il 1° Anno - 2° Semestre - Gruppo C2

Geometria

Dalle lezioni della prof.ssa Cioffi Francesca

Anno 2023/24 - Di Tota Gaetano

Siete pregati di segnalare ogni tipo di errore!

Geometria - a.a. 2023/2024

Simboli

$\cup$ unione

$\cap$ intersezione

$\forall$ per ogni

$\exists$ esiste

$\in$ appartiene

$\notin$ non appartiene

$\vee$ o disgiunzione

$\wedge$ e congiunzione

$\Leftrightarrow$ equivalente

$\neg$ negazione

$\Rightarrow$ implica

$\subseteq$ inclusione

$\subset$ inclusione propria

$\triangle$ differenza simmetrica

$\setminus$ differenza insiemistica

$\bigcup$ unione unaria

$\bigcap$ intersezione unaria

Lezione del 04/03/2024

Vettore libero

Definizione - Vettore libero

Un vettore rappresenta lo spostamento da un punto ad un altro, esso ha come caratteristiche: direzione, verso e lunghezza.

Definizioni e Notazioni

Definizione - Simboli

- $\emptyset$ = Insieme vuoto
- $A \subseteq B \Leftrightarrow \forall x \in A (x \in B)$
- $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$
- $A \cap B \Leftrightarrow \{x \mid x \in A \wedge x \in B\}$
- $A \cup B \Leftrightarrow \{x \mid x \in A \vee x \in B\}$
- $B \setminus A \Leftrightarrow \{x \mid x \in B \wedge x \notin A\}$

Domanda - Come assegnare un'insieme?

Per assegnare degi oggetti ad un'insieme abbiamo due modi distinti

1. Elencare gli elementi che appartengono all'insieme
   $x \in A$ oppure $y \notin A$
2. Caratterizzare gli elementi che appartengono all'insieme mediante una proprietà
   $B = \{x \mid x \text{ è uno studente del corso di Geometria}\}$

Definizione - Complemento

Prendiamo $A \subseteq X$ e chiamiamo l'operazione $X \setminus A$ complemento di A in X che indichiamo con $C_X(A)$

Definizione - Leggi di De Morgan sul Complemento

Unione dei Complementi

$$C_X(A \cup B) = C_x(A) \cap C_X(B)$$

Dimostrazione

$$y \in C_X(A \cup B) \Leftrightarrow y \in X \wedge y \notin A \cup B \Leftrightarrow y \in X \wedge (y \notin A \vee y \notin B) \Leftrightarrow (y \in X \vee y \notin A) \wedge (y \in X \vee y \notin b) \Leftrightarrow y \in C_X(A) \wedge y \in C_x(B) \Leftrightarrow y \in C_X(A) \cap C_X(B)$$

Intersezione dei Complementi

$$C_X(A \cap B) = C_x(A) \cup C_X(B)$$

Dimostrazione

$$y \in C_X(A \cap B) \Leftrightarrow y \in X \wedge y \notin A \cap B \Leftrightarrow y \in X \wedge (y \notin A \vee y \notin B) \Leftrightarrow (y \in X \wedge y \notin A) \vee (y \in X \wedge y \notin b) \Leftrightarrow y \in C_X(A) \vee y \in C_x(B) \Leftrightarrow y \in C_X(A) \cup C_X(B)$$

Prodotto Cartesiano

Definizione - Prodotto Cartesiano

Siani $A, B \neq \emptyset$ allora definiamo prodotto cartesiano tra due insiemi $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

Esempio - Prodotto Cartesiano

Siano $A = \{1, 2, 3\}$ e $B = \{x, y\}$ allora otteniamo $A \times B = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$

Sia $A_1, A_2, ..., A_n \neq \emptyset$ abbiamo che $A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge ... \wedge a_n \in A_n\}$ allora

- Preso il polinomio $3x_1 - x_2 + 4x_3 + x_5 = 1$
- Definiamo l'insieme di soluzioni $S = \{(\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_4}, \overline{x_5}) \in \mathbb{R}^5 \mid 3\overline{x_1} - \overline{x_2} + 4\overline{x_3} + \overline{x_5} = 1\}$
- Dove sappiamo che $(1, 3, -1, 0, 5) \in S$

Principio di Induzione

Definizione - Principio di Induzione

$\forall n \in \mathbb{N}^*$ sia $P(n)$ un'affermazione che dipende da n allora

1. **Base induttiva**: $\exists \overline{n} \in \mathbb{N}^*(P(\overline{n} \text{ è verificata}))$
2. **Passo induttivo**: $\forall n > \overline{n}(P(n-1) \Rightarrow P(n))$

Esempio - Principio di Induzione

Sia $P(n) =$ "Se A ha n elementi allora $\mathcal{P}(A)$ ha 2^n elementi" allora abbiamo

- **Base induttiva**: $\overline{n} = 0$ allora $P(0) : A = \emptyset$ e $\mathcal{P}(A) = \{\emptyset\}$ esattamente $2^0 = 1$ elementi
- **Passo induttivo**: $\forall n > 0 P(n-1) \Rightarrow P(n)$

Siano $A = \{\alpha_1, \alpha_2, ..., \alpha_{n-1}\} \subseteq B = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ allora so che

1. $\mathcal{P}(A) = \{x \mid x \subseteq A\} = \{x \mid x \subseteq B \wedge \alpha_n \notin x\} \subseteq \mathcal{P}(B)$
2. $\mathcal{P}(B) \setminus \mathcal{P}(A) = \{x \mid x \subseteq B \wedge \alpha_n \in x\}$
3. $\mathcal{P}(B) = \mathcal{P}(A) \cup \{x \cup \{\alpha_n\} \mid x \subseteq A\}$

Concludo quindi che $\mathcal{P}(B)$ ha $2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n$ elementi

Relazione tra insiemi

Definizione - Relazione

Siano $A, B \neq \emptyset$ chiamiamo relazione (oppure corrispondenza) di A in B un sottoinsieme $\rho \subseteq A \times B$

$$\text{Sia } a \in A \text{ e } b \in B \text{ allora indichiamo } a \ \rho \ b \Leftrightarrow (a, b) \in \rho$$

Chiamiamo **relazione capovolta** la sua inversa $\overset{\frown}{\rho} = \{(b, a) \mid (a, b) \in \rho\}$

$$\forall a, b \in A(a \ \overset{\frown}{\rho} \ b \Leftrightarrow b \ \rho \ a)$$

Definizione - Relazione di equivalenza

Sia $A = B = \emptyset$ è detta relazione binaria in A ed è di equivalenza se rispetta le seguenti proprietà

1. **Riflessiva**: $\forall a \in A (a \ \rho \ a)$
   in termini di coppia ordinata $(a, a) \in \rho$
2. **Simmetrica**: $\forall a, b \in A (a \ \rho \ b \wedge b \ \rho \ a)$
   in termini di coppia ordinata $(a, b) \Rightarrow (b, a) \in \rho$
3. **Transitiva**: $\forall a, b, c \in A (a \ \rho \ b \wedge b \ \rho \ c \Rightarrow a \ \rho \ c)$
   in termini di coppia ordinata $(a, b) \in \rho \wedge (b, c) \in \rho \Rightarrow (a, c) \in \rho$

Esempio - Relazione di equivalenza

Sia $A = \{1, 3, 5\}$ allora $R = \{(1, 1), (3, 3), (5, 5), (3, 5), (5, 3)\}$

Sia $A = \mathbb{N}^*$ allora $R = \{(x, y) \mid |x - y| \text{ è pari o nullo}\}$

Sia $A = \mathbb{Z} \times \mathbb{N}^*$ allora $\rho \subseteq A \times A$ abbiamo che $\rho = \{(m, n), (m', n') \mid m \cdot n' = m' \cdot n\} = \mathbb{Q}$

Teorema - $\rho = \overset{\curvearrowleft}{\rho}$ quando ρ è di equivalenza

Sia $\rho \subseteq A \times A$ posso dimostrare una sola inclusione perché $(\overset{\curvearrowleft}{\overset{\curvearrowleft}{\rho}}) = \rho$

Dimostrazione Sia $(a, b) \in \rho \Rightarrow (b, a) \in \rho \Rightarrow (a, b) \in \overset{\curvearrowleft}{\rho}$

Domanda - Quale relazione identifica due vettori applicati uguali?

È chiamata relazione di equipollenza quella che identifica due coppie di punti sul piano che hanno stessa direzione, verso e lunghezza.

Definiamo quindi ρ che identifica due vettori applicati uguali:

- $F = \{P \mid P \text{ è un punto nello spazio della geometria elementare}\}$
- $A = F \times F = \{(P, Q) \mid P, Q \in F\}$ ottenendo l'insieme dei vettori applicati
- Sia poi $\rho \subseteq A \times A$ ottenendo $\rho = \{((P, Q), (P', Q')) \mid (P, Q) \text{ e } (P', Q') \text{ abbiamo stessa direzione, verso e lunghezza}\}$

Classe di equivalenza

Definizione - Classe di equivalenza

Sia $A \neq \emptyset$ e ρ una relazione di equivalenza su A allora chiamo classe di equivalenza

$$\forall a \in A \quad [a]_\rho := \{x \in A \mid x\ \rho\ a\}$$

Le classi di equivalenza hanno le seguenti proprietà

1. $\forall a \in a \quad a \in [a]_\rho$
2. $\forall a, b \in A \quad a \in [b]_\rho \Rightarrow [a]_\rho = [b]_\rho$
3. $\forall a, b \in A \quad [a]_\rho \cap [b]_\rho = \emptyset \vee [a]_\rho = [b]_\rho$

Dimostrazione

1. $(a, a) \in \rho$
2. Qui dobbiamo osservare una doppia inclusione
   - "$\subseteq$" $\left.\begin{array}{l} z \in [a]_\rho \Rightarrow z\ \rho\ a \Rightarrow (z, a) \in \rho \\ \text{per ipotesi } a \in [b]_\rho \Rightarrow (a, b) \in \rho \end{array}\right\} \Rightarrow (z, b) \in \rho \Rightarrow z \in [b]_\rho$
   - "$\supseteq$" $\left.\begin{array}{l} z \in [b]_\rho \Rightarrow (z, b) \in \rho \Rightarrow (b, z) \in \rho \\ \text{per ipotesi } a \in [b]_\rho \Rightarrow (a, b) \in \rho \end{array}\right\} \Rightarrow (z, a) \in \rho \Rightarrow z \in [a]_\rho$
3. Se $\exists z \in [a]_\rho \cap [b]_\rho$ allora sappiamo che $z \in [a]_\rho$ e $z \in [b]_\rho \Rightarrow [a]_\rho = [z]_\rho = [b]_\rho$

Domanda - Qual'è l'insieme delle classi di equivalenza?

Se ρ è una relazione di equivalenza su A allora definiamo insieme quoziente (oppure partizione) $\frac{A}{\rho} := \{[a]_\rho \mid a \in \rho\}$ l'insieme di tutte le classi di equivalenza, questo ci dice due cose

- $A = \bigcup_{[a] \in \frac{A}{\rho}} [a]_\rho$
- Se $[a]_\rho \cap [b]_\rho = \emptyset \Rightarrow [a]_\rho \neq [b]_\rho$

Lezione del 06/03/2024

Relazione di Parallelismo

Definizione - Relazione di Parallelismo

Siano r_1 e r_2 due rette distinte, allore diciamo che sono parallele se sono complanari, cioè se esiste un piano che contiene sia r_1 e r_2 dove la loro intersezione risulta vuota.

NOTA una retta si dice sempre parallela a se stessa.

Definiamo quindi l'insieme delle rette $A = \{r \mid \text{retta dello spazio nella geometria elementare}\}$ e su questo costruiamo $\rho \subseteq A \times A$ che definiamo usando la relazione di parallelismo $\rho = \{(r_1, r_2) \mid r_1, r_2 \text{ sono parallele}\}$

Sappiamo che la relazione di parallelismo è di equivalenza perché:

- **Riflessiva**: $\forall r \in A \quad (r, r) \in \rho$

- **Simmetrica**: $\forall r, r_1 \in A \quad (r, r_1) \in R \Rightarrow (r_1, r) \in \rho$
- **Transitiva**: $\forall r, r_1, r_2 \in A \quad (r, r_1), (r_1, r_2) \in R \Rightarrow (r, r_2) \in \rho$

Direzione e Verso

Definizione - Direzione

Per dare la definizione di direzione, dobbiamo partire da quelli di retta per poi usare questo strumento per definire le altre, vediamo come

1. **Retta**: usiamo le classi di equivalenza per definire se due rette hanno la stessa direzione, ovvero se sono parallele, quindi $[r]_\rho = \{r_1 \in A \mid r_1 \ \rho \ r\}$
2. **Vettore applicato**: due vettori applicati (P, Q) e (R, T) hanno la stessa direzione se sono contenuti in rette parallele
3. **Vettore libero**: due vettori liberi $\overrightarrow{PQ}$ e $\overrightarrow{RT}$ hanno la stessa direzione se si possono disegnare su rette parallele

Definizione - Verso

Per questa definizione dobbiamo sfruttare come strumento la retta e le classi di equivalenza, perché

- **Vettore applicato**: siano (P, Q) e (R, T) due vettori applicati paralleli, allora hanno lo stesso verso se applicando uno dei due nel punto di applicazione dell'altro, otteniamo che i due secondi estremi si trovano nella stessa parte della retta individuata rispetto al comune punto di applicazione
- **Vettore libero**: siano $\overrightarrow{PQ}$ e $\overrightarrow{RT}$ due vettori liberi paralleli, allora hanno lo stesso verso se lo hanno i loro rappresentati (P, Q) e (R, T)

Applicazione

Definizione - Applicazione

Siano $A, B \neq \emptyset$ allora definiamo una corrispondenza $f \subseteq A \times B$ che chiamiamo applicazione (oppure funzione) di A in B che indichiamo con $f : A \to B$ se verifica la seguente condizione:

$$\forall a \in A \quad \exists! b \in B \quad (a, b) \in f$$

Chiamiamo A dominio e B codominio di f, inoltre questa applicazione si dice

- **Iniettiva**: due elementi distinti di A corrispondono a due elementi distinti di B

$$\forall a, b \in A \quad f(a) = f(b) \Rightarrow a = b$$

- **Suriettiva**: ogni elemento di B è immagine di almeno un elemento di A

$$\forall b \in B \quad \exists a \in A \quad f(a) = b$$

- **Biettiva**: se è sia iniettiva che suriettiva

$$\forall b \in B \quad \exists! a \in A \quad f(a) = b$$

Definizione - Applicazione inversa

Sia $f : A \to B$ allora definiamo $f^{-1} = \{(b, a) \mid f(a) = b\}$ applicazione inversa che indichiamo con $f^{-1} : B \to A$ ed esiste quando

- $f_o f^{-1} : B \xrightarrow{f^{-1}} A \xrightarrow{f} B$ quindi $f_o f^{-1} = id_B$
- $f_o^{-1} f : A \xrightarrow{f} B \xrightarrow{f^{-1}} A$ quindi $f_o^{-1} f = id_A$

Nota - Se f è biettiva allora anche f^{-1} è biettiva

Sia $f : A \to B$ un'applicazione biettiva allora sappiamo dire per f^{-1} che è un'applicazione biettiva perché

$$f^{-1} \subseteq B \times A \text{ biettiva} \Leftrightarrow \forall b \in B \quad \exists! a \in A \quad (b, a) \in f^{-1} \Leftrightarrow \forall b \in B \quad \exists! a \in A \quad (a, b) \in f \Leftrightarrow f \subseteq A \times B \text{ è biettiva}$$

Domanda - Cosa succede se considerano l'applicazione f e f^{-1} su una singola parte?

Andiamo prima a considerare una parte del dominio e poi del codominio applicate rispettivamente all'applicazione f e poi alla sua inversa f^{-1}

- $\forall X \subseteq A \quad f(X) = \{f(a) \mid a \in X\} \subseteq B$
- $\forall Y \subseteq B \quad f^{-1}(Y) = \{a \in A \mid f(a) \in Y\} \subseteq A$

NOTA da questo deduciamo che $Im\ f = \{f(a) \mid a \in A\}$ ovvero esattamente $Im\ f := f(A)$

Definizione - Applicazione composta

Siano $f : A \to B$ e $g : B \to C$ allora possiamo definire l'applicazione composta l'unione di più applicazioni

$$g_o f : A \to C$$

Questa applicazione segue il seguente schema $A \xrightarrow{f} B \xrightarrow{g} C$ ovvero $g_0 f(a) = g(f(a))$

Domanda - Cosa posso dire sulle proprietà della composizione di applicazioni?

Se prese le singole applicazioni f e g osservando la loro composta $g_o f$ posso dire

f e g	$g_o f$
iniettiva	iniettiva
suriettiva	suriettiva
biettiva	biettiva

Lezione del 11/03/2024

Restrizione e Riduzione

Definizione - Restrizione

Una restrizione è una sostituzione del dominio con un suo sottoinsieme non vuoto, sia $f : A \to B$ e un suo sottinsieme $\emptyset \neq X \subseteq A$, chiamo restrizione di f a X l'applicazione

$$f_{|X} : X \to B \text{ con la proprietà che } \forall x \in X \quad f_{|X}(x) = f(x)$$

Definizione - Riduzione

Una riduzione è una sostituzione del codominio con un suo sottoinsieme non vuoto, sia $f : A \to B$ e un suo sottinsieme $\emptyset \neq Y \subseteq B$, chiamo riduzione di f a Y l'applicazione

$$f^{|F} : X \to Y \text{ con la proprietà che } f(X) \subseteq Y$$

Cardinalità di un'insieme

Definizione - Insiemi equipotenti

Siano A e B due insiemi, li definiamo equipotenti (ovvero hanno la stessa potenza o ordine) se esiste un'applicazione biettiva $f : A \to B$ con la proprietà che $\exists! f^{-1} : B \to A$

Nota - Potenze numerabili

Sono dette potenze numerabili tutti gli insiemi equipotenti ad $\mathbb{N}$, infatti possiamo prendere in esempio $|\mathbb{Z}| = |\mathbb{N}| = |\mathbb{Q}|$ ma sappiamo anche che $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| > |\mathbb{N}|$, da questo deduciamo che che "infinito" è solo un aggettivo e non una cardinalità.

Operazioni binarie

Definizione - Operazione binaria

Siano $A, B, C \neq \emptyset$ chiamiamo operazione binaria un'applicazione $\perp: A \times B \to C$ e ne distinguiamo due tipi

1. **Interna** quando $A = B = C$
2. **Esterna** quando $B = C$ e si dice che ha operatori in A

Domanda - Qual è insieme dei vettori liberi?

Sfruttando le classi di equivalenza e l'insieme quoziente, usiamo la relazione di equipollenza ρ e il prodotto cartesiano $F \times F$ dove F è l'insieme dei punti, definendo così l'insieme dei vettori liberi $\mathbb{V}$:

$$\frac{F \times F}{\rho} = \mathbb{V} = \{\overrightarrow{PQ} \mid P, Q \text{ sono punti dello spazio della geometria elementare}\}$$

Nota - Operazioni tra vettori liberi

Definiamo adesso le operazioni tra vettori liberi usando lo strumento delle operazioni binarie

- $+ : \mathbb{V} \times \mathbb{V} \to \mathbb{V} \quad (u, v) \rightsquigarrow w$
- $\cdot : \mathbb{R} \times \mathbb{V} \to \mathbb{V} \quad (\alpha, u) \rightsquigarrow \alpha u$

Andiamo ad osservare più nel dettaglio queste operazioni e le loro proprietà

- $+$ è un'operazione interna che restituisce un vettore libero ottenuto prendendo come rappresentati di u e v coppie del tipo $(P, Q), (Q, R)$ tali che $w = [(P, R)]$
- $\cdot$ è un'operazione esterna tale che αu è un vettore che ha stessa direzione di u, la sua lunghezza è calcolata come $|\alpha||u|$ e stesso verso se $\alpha \geq 0$ oppure opposto se $\alpha < 0$

NOTA Se $\alpha = 0 \Rightarrow \alpha u = 0 = (P, P)$ ovvero il vettore nullo con verso, direzione e lunghezza indefinita

Struttura algebrica / Spazio Vettoriale

Definizione - Struttura algebrica

Si tratta di una n-upla ($n \in \mathbb{N}$) costituita da insiemi e operazioni definite su questi insiemi.

Definizione - Gruppoide

Una struttura algebrica dalla forma $(A, \perp)$ con l'insieme $A \neq \emptyset$ e l'operazione $\perp : A \times A \to A$ della quale possiamo analizzare le seguenti proprietà:

- **Associativa** $\forall a, b, c \in A \quad (a \perp b) \perp c = a \perp (b \perp c)$
- **Commutativa** $\forall a, b \in A \quad a \perp b = b \perp a$
- **Neutro** $\exists t \in A \quad \forall x \in A \quad x \perp t = x = t \perp x$
- **Simmetrici** $\forall a \in A \quad \exists \bar{a} \in A \quad a \perp \bar{a} = t = \bar{a} \perp a$

Definizione - Gruppo

Sia data la struttura algebrica $(A, \perp)$ si dice gruppo se $\perp$ è associativa, ammette neturo e simmetrici, inoltre se è anche commutativa è detto **Abeliano**

Definizione - Anello

Sia data la struttura algebrica $(A, +, \cdot)$ con le operazioni definite così $+ : A \times A \to \quad \cdot : A \times A \to A$, allora si chiama anello se

1. $+$ è un gruppo Abeliano
2. $\cdot$ è associativa
3. $\cdot$ è distributiva rispetto a $+$

Inoltre distinguiamo anche i seguenti tipi di anelli

- **Commutativo** $\cdot$ è commutativa
- **Unitario** $\cdot$ ammette neutro
- **Campo** anello commutativo unitario dove ogni elemento, tranne lo 0_A, ha inverso rispetto a $\cdot$

Definizione - Spazio vettoriale

Sia $(A, +, \cdot)$ un campo e V un'insieme non vuoto, definiamo le seguenti operazioni

- $\boxplus : V \times V \to V$ come operazione interna
- $\boxdot : A \times V \to V$ come operazione esterna

Allora la struttura algebrica $(A, V, \boxplus, \boxdot)$ è chiamata spazio vettoriale su A quando

1. $(V, \boxplus)$ è un gruppo Abeliano
2. $\forall \alpha \in A \quad \forall u, v \in V \quad \alpha \boxdot (u \boxplus v) = (\alpha \boxdot u) \boxplus (\alpha \boxdot v)$
3. $\forall \alpha, \beta \in A \quad \forall u \in V \quad u \boxdot (\alpha + \beta) = (\alpha \boxdot u) \boxplus (\beta \boxdot u)$
4. $\forall \alpha, \beta \in A \quad \forall u \in V \quad (\alpha \cdot \beta) \boxdot u = \alpha \boxdot (\beta \boxdot u)$

5. $\forall u \in V \quad 1_A \boxdot u = u$

NOTA! Gli elementi di A sono detti scalari e gli elementi di V vettori

Teorema - Sui Gruppoidi

Sia $(A, \perp)$ un gruppoide allora sappiamo che

1. Se $\perp$ ammette neutro t esso è unico
   $\forall a \in A \quad a \perp t = x = t \perp a$
2. Se $\perp$ ammette neutro t ed è associativa, allora se $a \in A$ ha un simmetrico a', esso è unico
   $a \in A \quad \exists a' \in A \quad a \perp a' = t = a' \perp a$
3. Se $\perp$ ammette neutro t ed è associativa, con $a_1, a_2 \in A$ simmetrizzabili, allora $a_1 \perp a_2$ ha come simmetrico $a'' \perp a'$
   $a_1, a_2, \in A \quad \exists a', a'' \in A \quad a_1 \perp a' = t = a' \perp a_1 \quad a_2 \perp a'' = t = a'' \perp a_2$

Dimostrazione

1. Se esiste $t' \in A$ con le stesse proprietà di t allora abbiamo $t = t \perp t' = t'$
2. Se esiste $a'' \in A$ con le stesse proprietà di a' allora abbiamo $a' = a' \perp t = a' \perp (a \perp a'') = (a' \perp a) \perp a'' = t \perp a'' = a''$
3. $(a_1 \perp a_2) \perp (a'' \perp a') = a_1 \perp (a_2 \perp a'') \perp a' = a_1 \perp t \perp a' = a_1 \perp a' = t$

Lezione del 13/03/2024

Teorema - Sugli Spazi Vettoriali

Sia $(A, +, \cdot)$ un campo e $V = A^n$ con $n \in \mathbb{N}^*$, sappiamo che $(A, A^n, \boxplus, \boxdot)$ è uno spazio vettoriale su A, definiamo le operazioni dello spazio vettoriale:

- $\boxplus : A^n \times A^n \to A^n$
  $((a_1, \ldots, a_n 2), (b_1, \ldots, b_n)) \rightsquigarrow (a_1 + b_1, \ldots, a_n + b_n)$
- $\boxdot : A \times A^n \to A^n$
  $(\alpha, (a_1, \ldots, a_n)) \rightsquigarrow (\alpha a_1, \ldots, \alpha a_n)$

Dimostrazione per il caso in cui $n = 2$

- $(A^2, \boxplus)$ è un gruppo abeliano
  - $\boxplus$ è commutativa $\forall (a_1, a_2), (b_1, b_2) \in A^2$

$$(a_1, a_2) \boxplus (b_1, b_2) = (a_1 + b_1, a_2 + b_2) = (b_1 + a_1, b_2 + a_2) = (b_1, b_2) \boxplus (a_1, a_2)$$

  - $\boxplus$ è associativa $\forall (a_1, a_2), (b_1, b_2), (c_1, c_2) \in A^2$

$$((a_1, a_2) \boxplus (b_1, b_2)) \boxplus (c_1, c_2) = ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) = (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)) = (a_1, a_2) \boxplus ((b_1, b_2) \boxplus (c_1, c_2))$$

- $\boxplus$ ha elemento neutro $\forall(a_1, a_2) \in A^2 \quad \exists(t_1, t_2) \in A^2$

$$(a_1, a_2) \boxplus (t_1, t_2) = (a_1 + t_1, a_2 + t_2) = (a_1, a_2) \Leftrightarrow \begin{cases} a_1 + t_1 = a_1 \Leftrightarrow t_1 = 0_A \\ a_2 + t_2 = a_2 \Leftrightarrow t_2 = 0_A \end{cases} \Leftrightarrow (t_1, t_2) = (0_A, 0_A)$$

- $\boxplus$ ammette simmetrici $\forall(a_1, a_2) \in A^2 \quad \exists(a_1', a_2') \in A^2$

$$(a_1, a_2) \boxplus (a_1', a_2') = (a_1 + a_1', a_2 + a_2') = (0_A, 0_A) \Leftrightarrow \begin{cases} a_1 + a_1' = 0_A \Leftrightarrow a_1' = -a_1 \\ a_2 + a_2' = 0_A \Leftrightarrow a_2' = -a_2 \end{cases} \quad \text{in } A$$

- $\forall \alpha \in A \quad \forall(a_1, a_2), (b_1, b_2) \in A^2 \quad \alpha \boxdot ((a_1, a_2) \boxplus (b_1, b_2)) = (\alpha \boxdot (a_1, a_2)) \boxplus (\alpha \boxdot (b_1, b_2))$

$$\alpha \boxdot ((a_1, a_2) \boxplus (b_1, b_2)) = \alpha \boxdot (a_1 + b_1, a_2 + b_2) = (\alpha a_1 + \alpha b_1, \alpha a_2 + \alpha b_2) = (\alpha a_1, \alpha a_2) \boxplus (\alpha b_1, \alpha b_2) = (\alpha \boxdot (a_1, a_2)) \boxplus (\alpha \boxdot (b_1, b_2))$$

- $\forall \alpha, \beta \in A \quad \forall(a_1, a_2) \in A^2 \quad (a_1, a_2) \boxdot (\alpha + \beta) = ((a_1, a_2) \boxdot \alpha) \boxplus ((a_1, a_2) \boxdot \beta)$

$$(\alpha + \beta) \boxdot (a_1, a_2) = ((\alpha + \beta)a_1, (\alpha + \beta)a_2) = (\alpha a_1 + \beta a_1, \alpha a_2 + \beta a_2) = (\alpha a_1, \alpha a_2) \boxplus (\beta a_1, \beta a_2) = (\alpha \boxdot (a_1, a_2)) \boxplus (\beta \boxdot (a_1, a_2))$$

- $\forall \alpha, \beta \in A \quad \forall(a_1, a_2) \in A^2 \quad (\alpha \cdot \beta) \boxdot (a_1, a_2) = \alpha \boxdot (\beta \boxdot (a_1, a_2))$

$$(\alpha \cdot \beta) \boxdot (a_1, a_2) = ((\alpha \cdot \beta) \cdot a_1, (\alpha \cdot \beta) \cdot a_2) = (\alpha \cdot (\beta \cdot a_1), \alpha \cdot (\beta \cdot a_2)) = \alpha \boxdot (\beta \boxdot (a_1, a_2))$$

- $\forall(a_1, a_2) \in A^2 \quad 1_a \boxdot (a_1, a_2) = (a_1, a_2)$

$$1_A \boxdot (a_1, a_2) = (1_A \cdot a_1, 1_A \cdot a_2) = (a_1, a_2)$$

Teorema - Propietà Aritmetiche sugli Spazi Vettoriali

1. $\forall u \in V \quad \forall \alpha \in A \quad \alpha \boxdot u = \underline{0} \Leftrightarrow \alpha = 0$ oppure $u = \underline{0}$
2. $\forall \alpha \in A \quad \forall u \in V \quad -(\alpha \boxdot u) = -(\alpha) \boxdot u = \alpha \boxdot -(u)$
3. $\forall \alpha \neq 0 \quad \forall u, v \in V \quad \alpha \boxdot u = \alpha \boxdot v \Rightarrow u = v$
4. $\forall \alpha, \beta \in A \quad \forall u \in A \setminus \{\underline{0}\} \quad \alpha \boxdot u = \beta \boxdot u \Rightarrow \alpha = \beta$

Dimostrazione

1. - " $\Leftarrow$ "
     - Sia $\alpha = 0$ ed osserviamo che $0 \boxdot u = (0 + 0) \boxdot u = (0 \boxdot u) \boxplus (0 \boxdot u)$ quindi so che $\exists -(0 \boxdot u)$
       $$\underline{0} = \quad (0 \boxdot u) - (0 \boxdot u) = ((0 \boxdot u) \boxplus (0 \boxdot u)) - (0 \boxplus u) \quad = 0 \boxdot u$$
     - Sia $u = \underline{0}$ ed osserviamo che $\alpha \boxdot \underline{0} = \alpha \boxdot (\underline{0} + \underline{0}) = (\alpha \boxdot \underline{0}) \boxplus (\alpha \boxdot 0)$ quindi so che $\exists -(\alpha \boxdot \underline{0})$
       $$\underline{0} = \quad (\alpha \boxdot \underline{0}) - (\alpha \boxdot \underline{0}) = ((\alpha \boxdot \underline{0}) \boxplus (\alpha \boxdot \underline{0})) - (\alpha \boxdot \underline{0}) \quad = \alpha \boxdot 0$$
   - " $\Rightarrow$ "
     - Se $\alpha \neq 0 \Rightarrow \exists \alpha^{-1}$ allora
       $$u = 1 \boxdot u = \quad (\alpha^{-1}\alpha) \boxdot u = \alpha^{-1} \boxdot (\alpha \boxdot u) \quad = \alpha^{-1} \boxdot \underline{0} = \underline{0}$$

2. $\forall \alpha \in A \quad \forall u \in V \quad -(\alpha \boxdot u) = -(\alpha) \boxdot u = \alpha \boxdot -(u)$

$$(-(\alpha) \boxdot u) \boxplus (\alpha \boxdot u) = (-\alpha + \alpha) \boxdot u = 0 \boxdot u = \underline{0}$$

$$(\alpha \boxdot -(u)) \boxplus (\alpha \boxdot u) = \alpha \boxdot (-(u) \boxplus u) = \alpha \boxdot \underline{0} = \underline{0}$$

3. $\forall \alpha \neq 0 \quad \forall u, v \in V \quad \alpha \boxdot u = \alpha \boxdot v \Rightarrow u = v$

$$u = 1 \boxdot u = (\alpha^{-1} \cdot \alpha) \boxdot u = \quad \alpha^{-1} \boxdot (\alpha \boxdot u) = \alpha^{-1} \boxdot (\alpha \boxdot v) \quad = (\alpha^{-1} \cdot \alpha) \boxdot v = 1 \boxdot v = v$$

4. $\forall \alpha, \beta \in A \quad \forall u \in A \setminus \{\underline{0}\} \quad \alpha \boxdot u = \beta \boxdot u \Rightarrow \alpha = \beta$

$$\alpha \boxdot u = \beta \boxdot u \Rightarrow \alpha \boxdot u \boxplus -(\beta) \boxdot u = \underline{0} \Rightarrow (\alpha - \beta) \boxdot u = \underline{0} \Rightarrow \alpha - \beta = \underline{0} \Rightarrow \alpha = \beta$$

Sotto-spazio Vettoriale / Linearmente Chiuso

Definizione - Linearmente Chiuso

Sia $(A, V, \boxplus, \boxdot)$ uno spazio vettoriale e $X \subseteq V$ questo si dice Linearmente chiuso se

1. $X \neq \emptyset$
2. $\forall u, v \in X \quad u \boxplus v \in X$
3. $\forall \alpha \in A \quad \forall u \in X \quad \alpha \boxdot u \in X$

Domanda - Ma $\underline{0}$ e l'opposto di u appartengono a X?

- Se $X \neq \emptyset$ allora sappiamo che $\exists u \in X$ con la proprietà che $\underline{0} = 0 \boxdot u \in X$
- Se $u \in X$ e $-u \in V$ allora sappiamo che $-u = (-1) \boxdot u \in X$

Definizione - Sotto-Spazio Vettoriale

Un sottoinsieme $X \subseteq V$ linearmente chiuso si dice sotto-spazio vettoriale di V se $(A, X, \boxplus_{|X}, \boxdot_{|X})$ è uno spazio vettoriale su A

Combinazione lineare

Definizione - Combinazione lineare

Sia $(A, V, \boxplus, \boxdot)$ uno spazio vettoriale e preso una n-upla di vettori $(u_1, \ldots, u_n)$ definiamo una sua combinazione lineare

$$\text{un vettore } u = \alpha_1 \boxdot u_1 \boxplus \ldots \boxplus \alpha_n \boxdot u_n \text{ dove } (\alpha_1, \ldots, \alpha_n) \in V$$

Chiusura lineare

Definizione - Chiusura lineare

Sia $(A, V, \boxplus, \boxdot)$ uno spazio vettoriale e $X \subseteq V$ allora chiamiamo chiusura lineare di X l'insieme di tutte le combinazioni lineari

$$\mathscr{L}(X) = \left\{ \begin{array}{l} \{\underline{0}\}, \text{ se } X = \emptyset \\ \{\alpha_1 \boxdot u_1 \boxplus \dots \boxplus \alpha_n \boxdot u_n \mid n \in \mathbb{N}^* \quad u_1, \dots, u_n \in X \quad \alpha_1, \dots, \alpha_n \in K\} \end{array} \right\}$$

NOTA! Si dice $\mathscr{L}(X)$ è il sotto-spazio vettoriale generato da X

Sistema di Generatori

Definizione - Sistema di Generatori

Sia $S \subseteq V$ allora si dice sistema di generatori di V se $V = \mathscr{L}(S)$, ossia ogni vettore di V è combinazione lineare dei vettori di S

$$S \text{ è sistema di generatori di } V \Leftrightarrow \forall u \in V \quad u \in \mathscr{L}(S)$$

NOTA! V si dice finitamente generato se ha un sistema di generatori finito

Nota - Allegeriamo la notazione!

Da ora in poi useremo i simboli usuali anche per l'addizione e la motiplicazione dello spazio vettoriale, quindi per distinguerli da quelli del campo basterà confrontare gli operandi, se le operazioni hanno come operando un vettore stiamo usando l'operazione dello spazio vettoriale

Teorema - Sulla Chiusura Lineare

1. $X \subseteq \mathscr{L}(X)$
2. $\mathscr{L}(X)$ è linearmente chiuso
3. Comunque prendo un sottospazio vettoriale $W \subseteq V$ con la proprietà che $X \subseteq W$ allora $\mathscr{L}(X) \subseteq W$

Dimostrazione

1. $u \in X \Rightarrow u = 1 \cdot u \in \mathscr{L}(X)$
2. Osserviamo la chiusura lineare di entrambe le operazioni
   - **Addizione** siano $v, w \in \mathscr{L}(X) \Rightarrow \begin{cases} \exists u_1, \dots, u_n \in X \quad \exists \alpha_1, \dots, \alpha_n \in V \quad v = \alpha_1 \cdot u_1 + \dots + \alpha_n \cdot u_n \\ \exists k_1, \dots, k_m \in X \quad \exists \beta_1, \dots, \beta_m \in V \quad w = \beta_1 \cdot k_1 + \dots + \beta_m \cdot k_m \end{cases}$

     Quindi $v + w = \alpha_1 \cdot u_1 + \dots + \alpha_n \cdot u_n + \beta_1 \cdot k_1 + \dots + \beta_m \cdot k_m \in \mathscr{L}(X)$
   - **Moltiplicazione** Sia $\gamma \in \mathscr{L}(X)$ e $v \in \mathscr{L}(X)$ allora $\gamma \cdot v = \gamma(\alpha_1 \cdot u_1 + \dots + \alpha_n \cdot u_n) = \gamma(\alpha_1 \cdot u_1) + \dots + \gamma(\alpha_1 \cdot u_n)$

     Quindi $\gamma \cdot v = (\gamma \cdot \alpha_1) \cdot u_1 + \dots + (\gamma \cdot \alpha_n) \cdot u_n \in \mathscr{L}(X)$
3. Sia $v \in \mathscr{L}(X)$ allora $\exists u_1, \dots, u_n \in X \quad \exists \alpha_1, \dots, \alpha_n \in A \quad v = \alpha_1 \cdot u_1 + \dots + \alpha_n \cdot u_n$

   Ma per la linearità di W sappiamo che $\left. \begin{array}{ccc} u_1 \in X & \Rightarrow & \alpha_1 \cdot u_1 \in W \\ \vdots & \vdots & \vdots \\ u_1 \in X & \Rightarrow & \alpha_1 \cdot u_1 \in W \end{array} \right\} \Rightarrow v = \alpha_1 \cdot u_1 + \dots + \alpha_n \cdot u_n \in W$

Matrici

Definizione - Matrici

Sia A un'insieme non vuoto e prensi $n, m \in \mathbb{N}^*$ chiamiamo matrice su A di tipo $n \times m$ l'applicazione

$$f: \begin{array}{ccc} \{1, ..., n\} \times \{1, ..., m\} & \to & A \\ (i, j) & \rightsquigarrow & f((i, j)) \end{array}$$

Lezione del 18/03/2024

Linearmente Dipendente

Definizione - Linearmente Dipendente

Sia $(A, V, +, \cdot)$ uno spazio vettoriale, presa una n-upla $(u_1, ..., u_n)$ di vettori di V si dice lienearmente dipendente se il vettore nullo si può scrivere come una combinazione lineare di vettori della n-upla anche con scalari non tutti nulli

$$\exists(\alpha_1, ..., \alpha_n) \in A^n \setminus \{\underline{0}\} \quad \underline{0} = \alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n$$

Linearmente Indipendente

Definizione - lienearmente Indipendente

Sia $(A, V, +, \cdot)$ uno spazio vettoriale, presa una n-upla $(u_1, ..., u_n)$ di vettori di V si dice linearmente indipendente se il vettore nullo si può scrivere come combinazione lineare di vettori della n-upla solo con scalari tutti nulli

$$(\alpha_1, ..., \alpha) \in A^n \quad \underline{0} = \alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n \Rightarrow \alpha_1 = ... = \alpha_n = 0$$

NOTA! L'insieme vuoto è linearmente indipendente

Domanda - Come posso capire velocemente se un'insieme è linearmente dipendente?

Sia $X \subseteq V$ allora X si dice linearmente dipendente se esiste un sotto-insieme finito di X linearmente dipendente

Sia $S = \{u_1, ..., u_n\}$ linearmente dipendente allora vediamo che se $T = S \cup \{u_{n+1}, ..., u_m\}$ allora T è linearmente dipendente, siccome S è linearmente dipendente allora

$$\exists(\alpha_1, ..., \alpha_n) \in A^n \setminus \{\underline{0}\} \quad \alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n = \underline{0} \Rightarrow \alpha_1 \cdot u_1 + ... + \alpha_{n+1} \cdot u_{n+1} + ... + \alpha_m \cdot u_m = \underline{0}$$

Teorema - Sulla Dipendenza Lineare

Sia $(A, V, +, \cdot)$ con $X \subseteq V$ sappiamo che X è linearmente dipendente $\Leftrightarrow \exists u \in X \quad \mathscr{L}(X) = \mathscr{L}(X \setminus \{u\})$

Dimostrazione

- Se $X = \{\underline{0}\}$ sappiamo che $X \setminus \{\underline{0}\} = \emptyset$ ed abbiamo che $\mathscr{L}(X) = \{\underline{0}\} = \mathscr{L}(\emptyset)$
- Se $|X| \geq 2$ osserviamo entrambi i lati della dell'implicazione
  - "$\Rightarrow$" per ipotesi X è linearmente dipendente, ovvero $\exists(\alpha_1, ..., \alpha_n) \in A^n \setminus \{\underline{0}\} \quad \underline{0} = \alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n$

    Sia allora $\alpha_1 \neq 0$ e questo ci dice che $\exists \alpha_1^{-1} \quad \alpha_1^{-1}(\alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n) = \alpha_1^{-1} \cdot \underline{0} = \underline{0}$ sfruttando la distributività e l'associatività abbiamo $(\alpha_1^{-1} \cdot \alpha_1)u_1 + ... + (\alpha_1^{-1} \cdot \alpha_n)u_n = u_1 + ... + (\alpha_1^{-1} \cdot \alpha_n)$

Sfruttando l'uguaglianza precedente abbiamo che $u_1 = -(\alpha_1^{-1} \cdot \alpha_2) - .... - (\alpha_1^{-1} \cdot \alpha_n)u_2 \in \mathscr{L}(X \setminus \{u_1\})$

- "$\Leftarrow$" per ipotesi $\exists u \in X \quad \mathscr{L}(X) = \mathscr{L}(X \setminus \{u\})$

  Allora sappiamo che $\exists v_1, ..., v_n \in X \setminus \{u\} \quad \exists \beta_1, ..., \beta_n \in A \quad u = \beta_1 \cdot v_1 + ... + \beta_n \cdot v_n$

  Ma questo ci porta a dire che $1 \cdot u - (\beta_1) \cdot u_1 - .... - (\beta_n) \cdot u_n = \underline{0}$ e quindi X è linearmente dipendente

Lezione del 20/03/2024

Domanda - Quando due chiusure lineari coincidono?

Sia $(A, V, +, \cdot)$ uno spazio vettoriale e $S, T \subseteq V$ allora sappiamo che $\mathscr{L}(S) = \mathscr{L}(T) \Leftrightarrow S \subseteq \mathscr{L}(T)$ e $T \subseteq \mathscr{L}(T)$

- "$\Rightarrow$" $S \subseteq \mathscr{L}(S) = \mathscr{L}(T)$ e $T \subseteq \mathscr{L}(T) = \mathscr{L}(S)$
- "$\Leftarrow$" $\left.\begin{matrix} S \subseteq \mathscr{L}(T) \Rightarrow \mathscr{L}(S) \subseteq \mathscr{L}(T) \\ T \subseteq \mathscr{L}(S) \Rightarrow \mathscr{L}(T) \subseteq \mathscr{L}(S) \end{matrix}\right\} \Rightarrow \mathscr{L}(S) = \mathscr{L}(T)$

Base di uno Spazio-Vettoriale

Definizione - Base di uno Spazio-Vettoriale

Una base di uno spazio vettoriale V è un sistmea di generatori di V linearmente indipendente

NOTA! è chiamata base canonica la base composta da $\{(1, 0, ...), (0, 1, ...)\}$

Teorema - Di estrazione di una Base

Sia V uno spazio vettoriale finitamente generato su un campo A e sia $S = \{u_1, ..., u_n\}$ un suo sistema di generatori finito, allora sappiamo che esiste una base B di V tale che $B \subseteq S$

Dimostrazione Per ipotesi sappiamo che $\mathscr{L}(S) = V$

1. Se S è linearmente indipendente allora $B = S$ ed è base di V
2. Altrimenti $\exists u \in S \quad \mathscr{L}(S) = \mathscr{L}(S \setminus \{u\})$ e sia $u = u_1$ allora $S' = S \setminus \{u\}$ è un sistema di generatori di V

Ripetiamo il processo finché non si trova un base di V

Nota - Cosa succede nel caso di un'insieme linearmente dipendente con due vettori?

Sia $(A, V, +, \cdot)$ uno spazio vettoriale con $S \subseteq V$ dove $S = \{u, v\}$ allora

$$S \text{ è linearmente dipendente} \Leftrightarrow \exists \gamma \in A \quad u = \gamma \cdot v \text{ oppure } v = \gamma \cdot u$$

Infatti per ipotesi $\exists(\alpha, \beta) \in A^2 \setminus \{(0, 0)\} \quad \alpha u + \beta c = \underline{0}$ ma questo ci dice che $\alpha \neq 0$ oppure $\beta \neq 0$

- Se $\alpha \neq 0$ allora $\exists \alpha^{-1}$ ottenendo $\left.\begin{matrix} \alpha^{-1}(\alpha \cdot u + \beta \cdot v) = \alpha^{-1} \cdot \underline{0} = \underline{0} \\ (\alpha^{-1} \cdot \alpha)u + (\alpha^{-1} \cdot \beta)v = 1 \cdot u + (\alpha^{-1} \cdot \beta)v \end{matrix}\right\} \Rightarrow u = -(\alpha^{-1} \cdot \beta)v$
- Se $\beta \neq 0$ allora $\exists \beta^{-1}$ ottenendo $\left.\begin{matrix} \beta^{-1}(\alpha \cdot u + \beta \cdot v) = \beta^{-1} \cdot \underline{0} = \underline{0} \\ (\beta^{-1} \cdot \alpha)u + (\beta^{-1} \cdot \beta)v = (\beta^{-1} \cdot \alpha)u + 1 \cdot v \end{matrix}\right\} \Rightarrow v = -(\beta^{-1} \cdot \alpha)u$

Nota - Se poniamo lo stesso caso sui vettori?

Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{R}$ allora sappiamo che

- $u, v \in \mathbb{V} \quad \{u, v\}$ è linearmente dipendente $\Leftrightarrow u \parallel v$
- $u, v, w \in \mathbb{V} \quad \{u, v, w\}$ è linearmente dipendente $\Leftrightarrow u, v, w$ sono complanari

Teorema - Sull'Indipendenza Lineare

Sia $(A, V, +, \cdot)$ uno spazio vettoriale, presa $S \subseteq V$, sia S linearmente indipendente allora $u \in V \quad u \notin \mathscr{L}(S) \Rightarrow S \cup \{u\}$ è linearmente indipendente

Dimostrazione Sia $S \cup \{u\} = \{u, v_1, \dots, v_n\}$ allora $\alpha, \alpha_1, \dots, \alpha_n \in A \quad \alpha \cdot u + \dots + \alpha_n \cdot v_n = \underline{0}$ con la proprietà che $\alpha = \dots = \alpha_n = \underline{0}$

Supponiamo per assurdo che $\alpha \neq 0$ allora $\exists \alpha^{-1} \in A$ allora abbiamo la seguente uguaglianza

$$1 \cdot u + (\alpha^{-1} \cdot \alpha_1)v_1 + \dots + (\alpha^{-1} \cdot \alpha^n)v_n = \quad \alpha^{-1}(\alpha \cdot u + \dots + \alpha_n \cdot v_n) \quad = \alpha^{-1} \cdot \underline{0} = \underline{0}$$

Quindi $u = -(\alpha^{-1} \cdot \alpha_1)v_1 + \dots + -(\alpha^{-1} \cdot \alpha_n)v_n \in \mathscr{L}(\{v_1, \dots, v_n\}) = \mathscr{L}(S)$ ma questo è impossibile

Teorema - di Steinitz

Sia $(A, V, +, \cdot)$ uno spazio vettoriale finitamente generato su un campo A allora sappiamo che

- $S = \{u_1, \dots, u_n\} \subseteq V$ con la proprietà che $V = \mathscr{L}(S)$
- $X = \{v_1, \dots, u_m\} \subseteq V$

Allora sappiamo che se $|X| = m > n = |S| \Rightarrow X$ è linearmente dipendente

Domanda - Cosa succede nel caso opposto?

Dal teorema di Steinitz ricaviamo che se $Y \subseteq V$ con la proprietà che Y è linearmente indipendente $\Rightarrow |Y| \leq |S|$

Teorema - Di Equipotenza delle Basi

Sia $(A, V, +, \cdot)$ uno spazio vettoriale finitamente generato su un campo A allora ogni base di V è finita ed ha lo stesso numero di vettori (sono equipontenti)

Dimostrazione Sia S un sistema di generatori finito di V allora

1. Presa B una base estratta da S allora $|B| = n < +\infty$
2. Sia B' un'altra base di V
3. B' è linearmente indipendente e sistema di generatori di V, ovvero $\mathscr{L}(B') = V = \mathscr{L}(B)$

Quindi per il teorema di Steinitz abbiamo che

$$\left.\begin{array}{l} |B'| \leq |B| \text{ altrimenti } B' = \{v_1, \dots, v_{n+1}\} \text{ sarebbe linearmente indipendente} \\ B \text{ è linearmente indipendente} \\ \mathscr{L}(B') = V \end{array}\right\} \Rightarrow |B| = |B'|$$

Dimensione

Definizione - Dimensione

Sia $(A, V, +, \cdot)$ uno spazio vettoriale, sia V finitamente generato su A allora la cardinalità comune alle sue basi si dice dimensione di V e si indica con $dim(V)$

Teorema - sulla Dimensione

Sia $(A, V, +, \cdot)$ uno spazio vettoriale, sia V finitamente generato su A con $dim(V) = n$

Allora preso $S = \{u_1, \ldots, u_n\} \subseteq V$ ottengo che S è linearmente indipendente $\Leftrightarrow$ S è un sistema di generatori di V

Dimostrazione

- "$\Rightarrow$" Per assurdo supponiamo che $\mathscr{L}(S) \subset V$, ovvero $\exists u \in V \quad u \notin \mathscr{L}(S)$ quindi otteniamo che

$$\left.\begin{array}{l} S \text{ è linearmente indipendete} \\ u \notin \mathscr{L}(S) \\ u \in V \end{array}\right\} \Rightarrow S \cup \{u\} \text{ è linearmente indipendente}$$

  ma questo è assurdo perché $|S \cup \{u\}| = n + 1 > n = dim(V)$

- "$\Leftarrow$" Per assurdo S è linearmente dipendente, quindi $\exists u \in S \quad \mathscr{L}(S \setminus \{u\}) = \mathscr{L}(S) = V$ allora per il teorema di estrazione di una base sappiamo che

$$\exists B \subseteq S \setminus \{u\} \text{ tale che } B \text{ è una base di } V \text{ con la proprietà che } |B| \leq |S \setminus \{u\}| = n - 1$$

  Ma questo è assurdo proprio per il teorema di estrazione di una base