

Appunti di Algebra

A.A. 2022/2023

1 Introduzione

1.1 Relazioni

Una **relazione** é un sottoinsieme del prodotto cartesiano di due o piú insiemi.
Una relazione su A é un sottoinsieme di $A \times A$.

a_1 é in relazione con a_2 e si scrive $a_1 Ra_2$.

Def. Una relazione é di **equivalenza** se rispetta le seguenti propriet :

Riflessiva: $aRa \ \forall a \in A$ (ogni elemento é in relazione con se stesso)

Simmetrica: $a_1 Ra_2 \implies a_2 Ra_1 \ \forall a_1, a_2 \in A$

Transitiva: $a_1 Ra_2 \wedge a_2 Ra_3 \implies a_1 Ra_3$

1.2 Funzioni/Applicazioni

$f : X \rightarrow Y$

f iniettiva: $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$

f suriettiva: $\forall y \in Y, \exists x \in A : y = f(x)$

f biettiva: $\forall y \in Y, \exists! x \in A : y = f(x)$

1.3 Insiemi numerici

L'insieme dei numeri razionali \mathbb{Q} introduce gli inversi del prodotto (es. $3 \rightarrow \frac{1}{3}$).

L'insieme dei numeri reali \mathbb{R} introduce limiti, radici e altri valori.

L'insieme dei numeri complessi \mathbb{C} introduce le radici di indice pari di numeri negativi tramite l'unit  immaginaria i e i suoi multipli. Un numero complesso é esprimibile in forma polare come $a + ib$, con $a, b \in \mathbb{R}$.

1.4 Campi

$(K, +, \cdot)$ é un campo se:

$+, \cdot$ sono associative ($a + (b + c) = (a + b) + c$), commutative ($a + b = b + a$)
e distributive ($a(b + c) = ab + ac$)

esistono elementi **neutri** (0 per la somma ($a + 0 = a$), 1 per il prodotto ($a \cdot 1 = a$)) e **opposti** ($-a$ per la somma ($a - a = 0$), x^{-1} per il prodotto ($x \cdot x^{-1} = 1$)), che restituiscono il valore neutro

Alcuni insiemi campi sono $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

1.4.1 Campi finiti

Dato un numero intero $n \geq 0$, definiamo su \mathbb{Z} la relazione di equivalenza

$$a \equiv b(n) \iff \exists k \in \mathbb{Z} : a - b = k \cdot n$$

essa rispetta tutte e 3 le proprietà elencate sopra.

Definiamo $[b] = \{a \in \mathbb{Z} : a \equiv b(n)\}$ e $Z_n = \{[0], [1], \dots, [n-1]\}$.

Es. in $Z_2 = \{[0], [1]\}$, $[0]$ sono i numeri pari, $[1]$ quelli dispari.

Definiamo su Z_n le operazioni:

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

Es. Possiamo scrivere, con la notazione dei campi finiti, il prodotto tra numeri interi:

Dato Z_2 : $[0] \cdot [0] = [0], [0] \cdot [1] = [0 \cdot 1] = [0], [1] \cdot [1] = [1 \cdot 1] = [1]$.

Z_n é un campo $\iff n$ é **primo**. Se n non é primo, non esisterá l'inverso di un fattore di n , ovvero non esisterá nessuna classe di elementi che se moltiplicata con la classe del fattore restituisca classe 1.

2 Spazi vettoriali

Uno **spazio vettoriale** definito su un campo K é un insieme V con due operazioni:

$$+ : V \times V \rightarrow V \quad (v_1, v_2) \rightarrow v_1 + v_2$$

$$\cdot : K \times V \rightarrow V \quad (a, v) \rightarrow av$$

che verificano le seguenti proprietà: $+$ é commutativa, associativa, con elem. neutri (vettore nullo) e opposti ($-v$), \cdot é associativa, distribuitiva rispetto alla somma e con elemento neutro.

Per ogni campo K , K^n é uno spazio vettoriale su K .

$$K^n = \{(x_1, x_2, \dots, x_n), x_i \in K, \forall i = 1, \dots, n\}$$

$$v = (x_1, x_2, \dots, x_n), u = (y_1, y_2, \dots, y_n)$$

$$v + u = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

$$av = (ax_1, ax_2, \dots, ax_n), a \in K$$

2.1 Sottospazi vettoriali

Un sottoinsieme non vuoto (contenente almeno il vettore nullo) $U \subseteq V$ (spazio vettoriale su K) é un **sottospazio vettoriale** (SSV) di V se é **chiuso** rispetto alle sue operazioni, cioè:

- $\forall v_1, v_2 \in U \rightarrow v_1 + v_2 \in U$
- $\forall v_1 \in U, a \in K, a \cdot v_1 \in U$

Esempio: $V = R^2$ spazio vettoriale su R , $U = \{(x, y) \in R^2 : y = 2x\}$. É un SSV?

Se $v_1, v_2 \in U : v_1 = (x_1, y_1) \rightarrow y_1 = 2x_1, v_2 = (x_2, y_2) \rightarrow y_2 = 2x_2$
 $v_1 + v_2 = (x_1 + x_2, 2x_1 + 2x_2) \rightarrow (x_1 + x_2, 2(x_1 + x_2)) \implies v_1 + v_2 \in U$. Inoltre,
 $\forall a \in R, a \cdot v_1 = a(x_1, 2x_1) \implies a \cdot v_1 \in U$. Quindi, U é un SSV di V .

Graficamente, significa che la somma di qualsiasi coppia di vettori presenti sulla retta $y = 2x$ é un vettore sempre giacente su questa retta, cosí come il prodotto di qualsiasi vettore giacente sulla retta per un qualsiasi scalare é un vettore sempre giacente su questa retta.

U é un SSV di $V \iff \forall u_1, u_2 \in U, \forall a_1, a_2 \in K$.

Dimostrazione:

\Rightarrow : se U é un SSV di V e $u_1, u_2 \in U \implies a_1 u_1, a_2 u_2 \in U \implies a_1 u_1 + a_2 u_2$

\Leftarrow : se $a_1 u_1 + a_2 u_2 \in U \forall a_1, a_2 \in K$, in particolare: prendendo $a_1 = 1, a_2 = 1, u_1 + u_2 \in U$, prendendo a_1 qualsiasi e $a_2 = 0, a_1 u_1 \in U$

2.2 Combinazione lineare

Dati $v_1, v_2, \dots, v_n \in V$, diciamo che $v \in V$ é una **combinazione lineare** di v_1, v_2, \dots, v_n se $\exists a_1, a_2, \dots, a_n \in K : v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$, quindi se v é esprimibile come la somma di tutti i vettori di V moltiplicati per un corrispettivo scalare.

Per quanto osservato sopra, U é un SSV \iff contiene *tutte le combinazioni lineari* di *tutti i suoi elementi*. Non esiste una combinazione lineare u degli elementi di U che non sia $\in U$.

Esempio: $V = R^2, v_1 = (1, 0), v_2 = (0, 1), v_3 = (3, -2)$. $v_3 = 3v_1 - 2v_2$ quindi v_3 é combinazione lineare di v_1, v_2 . Altro esempio: $u_1 = (2, 0), u_2 = (-1, 0), u_3 = (3, -2)$. u in questo caso non é combinazione lineare di u_1, u_2 perché non é possibile ottenere la seconda coordinata -2 essendo 0 in entrambi.

2.3 Span

Un SSV U di V é **generato** da $\{v_1, \dots, v_n\}$ se ogni elemento $u \in U$ é combinazione lineare di v_1, \dots, v_n , cioè se $\forall u \in U, \exists a_1, \dots, a_n \in K : u = a_1 v_1 + \dots + a_n v_n$. U é lo **span** di $\{v_1, \dots, v_n\}$ ed é scritto $U = \langle v_1, \dots, v_n \rangle$. Si noti che

l'insieme contiene infiniti elementi, siccome infinite sono le combinazioni lineari ottenibili $(a_1, \dots, a_n \in R)$.

Esempio: $V = R^4 = \{(x, y, z, w), x, y, z, w \in R\}$,
 $v_1 = (2, 0, 0, 0), v_2 = (0, 1, -1, 0)$. Il sottospazio generato da v_1, v_2 é $\langle v_1, v_2 \rangle = \{a_1 v_1 + a_2 v_2, a_1, a_2 \in R\} = (2a_1, 0, 0, 0) + (0, a_2, -a_2, 0) = (2a_1, a_2, -a_2, 0) = \{(x, y, z, w) \in R^4 : y + z = 0, w = 0\}$.
 Altro esempio: $V = R[x], \langle x^2, x, 1 \rangle = \{ax^2 + bx + c, a, b, c \in R\} = \{ \text{tutti i polinomi di grado } \leq 2 \}$ (con $a = 0$ il grado é < 2).

2.4 Indipendenza lineare

Un insieme di vettori $\{v_1, \dots, v_n\}$ é **linearmente indipendente** se *nessun vettore* é la combinazione lineare degli altri vettori dell'insieme, ovvero se l'*unica combinazione lineare* di v_1, \dots, v_n che restituisce il vettore nullo é quella con tutti i coefficienti $a_1, \dots, a_n \in K = \vec{0}$. Questo perché se un vettore é combinazione lineare di un insieme di vettori (es. $v_3 = 2v_1 + 4v_2$), basta dare i giusti coefficienti ($a_1 = 2, a_2 = 4, a_3 = -1$) per fare in modo che si annullino e mettere i coefficienti degli altri vettori a 0.

Un insieme di vettori é **linearmente dipendente** se non é linearmente indipendente. Non é però detto che ogni vettore appartenente a un insieme linearmente dipendente sia combinazione lineare di altri (es. $v_1 = (1, 0), v_2 = (2, 0), v_3 = (0, 1) \rightarrow v_2 = 2v_1$ ma v_3 non é combinazione lineare di v_1, v_2), é sufficiente che una coppia di vettori sia ricavabile l'una dall'altra per rendere tutto l'insieme linearmente dipendente.

2.4.1 Equivalenza delle definizioni di indipendenza lineare

1. Nessun vettore tra v_1, \dots, v_n é combinazione lineare degli altri
2. Se $a_1 v_1 + \dots + a_n v_n = 0 \implies a_1 = 0, \dots, a_n = 0$

Se la 1 é falsa, $\exists v_i$ (supponiamo per semplicitá sia v_1) che é combinazione lineare degli altri, quindi $v_1 = a_2 v_2 + \dots + a_n v_n \iff v_1 - a_2 v_2 - \dots - a_n v_n = 0 \implies$ la 2 é anch'essa falsa perché i coefficienti non sono per forza tutti 0 (sicuramente $a_1 = 1$).

Se la 2 é falsa significa che $\exists a_1, \dots, a_n$ con almeno un $a_i \neq 0 : a_1 v_1 + \dots + a_n v_n = 0$, allora $v_i = \frac{a_1}{a_i} v_1 + \dots + \frac{a_n}{a_i} v_n \implies$ la 1 é anch'essa falsa siccome v_i é combinazione lineare degli altri.

3 Base

Sia V uno spazio vettoriale su K , $\{v_1, \dots, v_n\}$ é una **base** di V se $\{v_1, \dots, v_n\}$ é **indipendente** e **genera** V .

Ad esempio, per $V = R^2, \{(1, 0), (0, 1)\}$ é indipendente e genera R^2 , quindi é

una base, mentre $\{(1, 0), (0, 1), (1, 1)\}$ genera R^2 ma é linearmente dipendente, quindi non é una base.

3.1 Teorema. Ogni vettore dello spazio vettoriale si scrive in modo univoco come combinazione lineare dei vettori di una base

Teorema. B é una base di uno spazio vettoriale V su un campo $K \iff \forall v \in V, \exists! a_1, \dots, a_n \in K : v = a_1 v_1 + \dots + a_n v_n$ (ogni vettore dello spazio si scrive in modo univoco come combinazione lineare degli altri).

In questo caso, a_1, \dots, a_n sono detti le **coordinate** di v nella base B .

Dimostrazione.

- 1. \implies 2

Sia B una base, $v \in V$. Poiché B genera V (per ipotesi é una base), $\exists a_1, \dots, a_n : v = a_1 v_1 + \dots + a_n v_n$. Per mostrare l'unicità dei coefficienti, supponiamo $\exists b_1, \dots, b_n : v = b_1 v_1 + \dots + b_n v_n$.

$$\begin{cases} v = a_1 v_1 + \dots + a_n v_n \\ v = b_1 v_1 + \dots + b_n v_n \end{cases} \quad \begin{cases} v - v = (a_1 v_1 + \dots + a_n v_n) - (b_1 v_1 + \dots + b_n v_n) \\ 0 = v_1(a_1 - b_1) + \dots + v_n(a_n - b_n) \end{cases} \quad (1)$$

Poiché B é linearmente indipendente $\implies a_1 - b_1 = \dots = a_n - b_n = 0$, cioè $a_1 = b_1, \dots, a_n = b_n$

- 2 \implies 1

Per ipotesi, $\forall v \in V, \exists! a_1, \dots, a_n \in K : v = a_1 v_1 + \dots + a_n v_n$. Da questo, possiamo dedurre che B genera V . Inoltre, sapendo che il vettore nullo é sempre ottenibile come combinazione lineare in cui tutti i coefficienti $a_1, \dots, a_n \in K$ sono uguali a 0, sfruttando la loro unicità, ciò implica che $0v_1 + \dots + 0v_n = \vec{0}$, ovvero che B é linearmente indipendente. B genera V ed é linearmente indipendente $\implies B$ é una base.

3.2 Base canonica

Sia K^n spazio vettoriale di dimensione n del campo K . Si definisce l'insieme di vettori $e_1 = (1, 0, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, 0, 0, \dots, 1)$ **base canonica** di K^n . In generale, é un insieme di vettori e_1, \dots, e_n dove l' i -esimo vettore ha la i -esima componente a 1 e tutte le altre a 0.

Ad esempio, la base canonica di R^3 é $\{e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)\}$. La base canonica per l'insieme dei polinomi di grado $\leq k$ é $\{1, x, x^2, \dots, x^k\}$.

3.3 Estrazione e completamento a una base

Sia X un insieme di vettori che genera V : **estrarre** una base da X significa trovare $B \subseteq X$ che sia una base di V .

Ad esempio, $X = \{v_1 = (1, 0), v_2 = (1, 1), v_3 = (0, 1)\}$, $B = \{v_1, v_3\}$ é una base estratta da X .

Sia X un insieme linearmente indipendente in V : **completare** X ad una base di V significa trovare un insieme di vettori da aggiungere ad X in modo da ottenere una base.

Ad esempio, $X = \{v_1 = (1, 0, 0), v_2 = (2, 0, 0)\}$. X non genera R^3 perché $\langle X \rangle = \{(x, y, z) \in R^3 : z = 0\}$. Per completare X a una base di R^3 basta aggiungere un vettore linearmente indipendente dagli altri due e che abbia $z \neq 0$, ad esempio aggiungendo $v_3 = (0, 0, 1)$ si ottiene la base canonica.

In generale: sia V spazio vettoriale di dimensione d su un campo K :

- ogni insieme linearmente indipendente in V contiene k elementi, $k \leq d$; può essere completato a una base di V aggiungendo $d - k$ elementi in modo opportuno (senza rendere l'insieme linearmente dipendente)
- ogni insieme che genera V contiene g elementi, $g \geq d$; possiamo estrarre una base rimuovendo opportunamente $g - d$ elementi

3.4 Teorema. Numero di elementi di una base

Teorema. Tutte le basi di uno spazio vettoriale V su un campo K hanno lo **stesso numero di elementi** e tale numero é detto la **dimensione** di V . La dimensione può anche essere pensata come il numero di direzioni linearmente indipendenti sufficienti per potersi muovere in tutto lo spazio vettoriale.

Ad esempio, $V = K^n$ ha base canonica $\{e_1, \dots, e_n\}$ composta da n elementi, quindi qualunque base di K^n ha n elementi ($\dim(K^n) = n$).

Ad esempio, $V = R[x] = \{\text{polinomi}\}$ ha una base $\{1, x, x^2, \dots\} \implies \dim(R[x]) = \infty$, mentre $U_n = \{p(x) \in R[x] : p(x) \text{ ha grado } \leq n\}$ é un sottospazio di V che ha base $\{1, x, x^2, \dots, x^n\}$ con $n + 1$ elementi, quindi $\dim(U_n) = n + 1$.

3.5 Forma cartesiana e parametrica

Sia U sottospazio vettoriale di dimensione d in uno spazio vettoriale di dimensione n ($d \leq n$). Posso esprimere U in 2 forme:

- forma **cartesiana**: U é identificato in K^n da $n - d$ equazioni tra loro linearmente indipendenti
- forma **parametrica**: U é espresso in funzione di d parametri

Ad esempio, $V = R^4$, $U = \{(x, y, z, w) \in R^4 : x = 2y, y = 3z, w = 0\}$ (forma cartesiana), oppure $U = \{(6t, 3t, t, 0), t \in R\}$ (forma parametrica). In questo caso, U ha dimensione 1, siccome posso scegliere solamente 1 parametro: una volta scelto, gli altri ne derivano di conseguenza. Ogni equazione (linearmente indipendente), nella forma cartesiana, toglie 1 grado di libertà.

3.5.1 Cambio di forma

- da **cartesiana** a **parametrica**: si usano le equazioni per esplicitare $n - d$ coordinate in funzione delle altre.

Ad esempio, dato $\{(x, y, z) \in R^3 : x + 2y - z = 0\}$, risolvo $z = x + 2y$, quindi se $x = t, y = s \implies z = t + 2s$, che in forma cartesiana diventa $\{(t, s, t + 2s), t, s \in R\}$

- da **parametrica** a **cartesiana**: si risolve il sistema.

Ad esempio, $\{(t, -2t, s, t + 2s), t, s \in R\}$:

$$\begin{cases} x = t \\ y = -2t \\ z = s \\ w = t + 2s \end{cases} \quad \begin{cases} x = t \\ 2x + y = 0 \\ z = s \\ x + 2z - w = 0 \end{cases} \quad \begin{matrix} (2I + II) \\ (I + 2III - IV) \end{matrix} \quad (2)$$

$$= \{(x, y, z, w) \in R^4 : 2x + y = 0 \wedge x + 2z - w = 0\}$$

3.6 Intersezione e unione di sottospazi vettoriali

Osservazione. La forma cartesiana facilita l'intersezione dei sottospazi vettoriali, mentre la forma parametrica risulta più comoda per trovare le basi di uno spazio.

Ad esempio, $U = \{(t, -2t, s, t + 2s), t, s \in R\} = \{(t, -2t, 0, t) + (0, 0, s, 2s), t, s \in R\} = \{t(1, -2, 0, 1) + s(0, 0, 1, 2), t, s \in R\}$. $v_t = (1, -2, 0, 1), v_s = (0, 0, 1, 2)$.

$\{tv_t + sv_s, t, s \in R\} = \langle v_t, v_s \rangle \implies v_t, v_s$ generano U e sono linearmente indipendenti $\implies v_t, v_s$ sono una base di U .

Proposizione. L'intersezione di sottospazi vettoriali é anch'esso un sottospazio vettoriale.

Dimostrazione. Sia V uno spazio vettoriale su un campo K e siano U, W sottospazi vettoriali di V . $U \cap W = \{v \in V : v \in U, v \in W\}$.

Vogliamo mostrare che se $\forall v_1, v_2 \in U \cap W, v_1 + v_2 \in U \cap W$: in effetti, sapendo che $v_1, v_2 \in U, v_1, v_2 \in W$ e che U e W sono dei sottospazi, $v_1 + v_2 \in U, v_1 + v_2 \in W \implies v_1 + v_2 \in U \cap W$.

Al contrario, l'unione di sottospazi non sempre é un sottospazio. Ad esempio, in $V = R^2$, $U = \{(x, y) \in R^2 : x = 0\} = \{(0, t), t \in R\}$, $W = \{(x, y) \in R^2 : y = 0\} = \{(x, 0), x \in R\}$.

$e_1 = (1, 0) \in W, e_2 = (0, 1) \in U \implies e_1, e_2 \in U \cup W$ ma $e_1 + e_2 = (1, 1) \notin U, \notin W \implies e_1 + e_2 \notin U \cup W$.

4 Somma di sottospazi

Dato uno spazio vettoriale V su un campo K , dati due sottospazi vettoriali U, W , la **somma** dei sottospazi U e W é il sottospazio

$$U + W = \{u + w, u \in U, w \in W\}$$

$U + W$ é un sottospazio di V perché $(u + w) + (u' + w') = \underbrace{u + u'}_{\in U} + \underbrace{w + w'}_{\in W}$
 $(\in U + W)$. Analogamente, $\forall a \in K, a(u + w) = \underbrace{au}_{\in U} + \underbrace{aw}_{\in W} (\in U + W)$.

4.1 Formula di Grassman

Siano U, W sottospazi vettoriali di V :

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$$

Intuitivamente, questa formula ricorda il modo di contare gli elementi appartenenti a due insiemi A e B : elementi in A + elementi in B - elementi in $A \cap B$ siccome li ho già contati negli elementi di A .

Idea alla base della dimostrazione:

Scelgo una base v_1, \dots, v_k di $U \cap W$ ($\dim(U \cap W) = k$) e la completo a una base $v_1, \dots, v_k, u_1, \dots, u_m$ di U ($\dim(U) = k + m$) e a una base $v_1, \dots, v_k, w_1, \dots, w_l$ di W ($\dim(W) = k + l$).

Si può dimostrare che $v_1, \dots, v_k, u_1, \dots, u_m, w_1, \dots, w_l$ é una base di $U + W$, quindi $\dim(U + W) = k + l + m = \dim(U) + \dim(W) - \dim(U \cap W) = (k + l) + (k + m) - k$.

4.2 Somma diretta

Sia U, W sottospazi vettoriali di V , allora U e W formano **somma diretta** se $U \cap W = \{\vec{0}\}$. Scriviamo $U \oplus W$ al posto di $U + W$.

4.2.1 Implicazioni

Sia V spazio vettoriale, siano U, W sottospazi vettoriali di V tali che $V = U \oplus W$, allora

$$\forall v \in V, \exists! u \in U, w \in W : v = u + w$$

ovvero ogni vettore v di V si scrive in modo unico come somma di un vettore $u \in U$ e $w \in W$.

Dimostrazione. Sappiamo che:

1. $V = U + W$
2. $U \cap W = \{\vec{0}\}$

Per la 1, ogni vettore v di V si scrive come somma di un vettore $u \in U$ e $w \in W$ ($\forall v \in V, \exists u \in U, w \in W : v = u + w$).

Per mostrarne l'unicità, supponiamo si possa scrivere anche come somma di altri due vettori $u' + w', u' \in U, w' \in W$.

Quindi, $v = u + w = u' + w' \iff \underbrace{u - u'}_{\in U} = \underbrace{w' - w}_{\in W} \implies \in U \cap W$. Per la 2,

$U \cap W = \{\vec{0}\}$, quindi $u - u' = \vec{0} \iff u = u', w' - w = \vec{0} \iff w = w'$.

4.2.2 Esempio

$R^2 = U \oplus W$, $U = \{(x, y) \in R^2 : y = 0\}$, $W = \{(x, y) \in R^2 : x = 0\}$ (assi cartesiani): ogni vettore in R^2 si scrive in modo unico come somma di $u \in U, w \in W$.

5 Applicazioni lineari

Siano U, V spazi vettoriali su K . Un'applicazione lineare $f : V \rightarrow U$ é **lineare** se é compatibile con le operazioni di V e U , ovvero se:

- $\forall v_1, v_2 \in V, f(v_1 + v_2) = f(v_1) + f(v_2)$
- $\forall v \in V, \forall a \in K, f(av) = af(v)$

equivalentemente, $\forall v_1, v_2 \in V, \forall a_1, a_2 \in K, f(a_1v_1 + a_2v_2) = a_1f(v_1) + a_2f(v_2)$ (coimplica 1 e 2).

5.1 Nucleo e immagine

Sia $f : V \rightarrow U$ applicazione lineare:

nucleo di f : $\text{Ker } f = \{v \in V : f(v) = \vec{0}\}$

immagine di f : $\text{Im } f = \{u \in U : \exists v \in V : u = f(v)\}$

5.1.1 Nucleo e immagine sottospazi vettoriali

1. $\text{Ker } f$ é un sottospazio vettoriale di V
2. $\text{Im } f$ é un sottospazio vettoriale di U

Dimostrazione:

1. siano $v_1, v_2 \in \text{Ker } f$ ($f(v_1) = f(v_2) = \vec{0}$), dobbiamo mostrare che anche $v_1 + v_2 \in \text{Ker } f$:
 $f(v_1 + v_2) = f(v_1) + f(v_2) = \vec{0} + \vec{0} = \vec{0}$ (ragionamento analogo per lo scalare)
2. siano $u_1, u_2 \in \text{Im } f$ ($\exists v_1, v_2 \in V : u_1 = f(v_1), u_2 = f(v_2)$), devo mostrare che anche $u_1 + u_2 \in \text{Im } f$:
 $f(v_1 + v_2) = f(v_1) + f(v_2) = u_1 + u_2 \in \text{Im } f$, ovvero $\exists v_1 + v_2 \in V : u_1 + u_2 = f(v_1 + v_2)$ (ragionamento analogo per lo scalare)

5.2 Iniettività e suriettività

Sia $f : V \rightarrow U$ applicazione lineare:

- f é **suriettiva** $\iff \text{Im } f = U$ ($\forall u \in U, \exists v \in V : u = f(v)$)
- f é **iniettiva** $\iff \text{Ker } f = \{\vec{0}\}$ ($\forall v_1, v_2, v_1 \neq v_2, f(v_1) \neq f(v_2)$)

5.2.1 Dimostrazione dell'iniettività

- 1 \implies 2 Poiché f é lineare, $f(\vec{0}) = f(v - v) = f(v) - f(v) = \vec{0}$ (il vettore nullo viene mandato nel vettore nullo). Siccome f é iniettiva, se $v \neq \vec{0}, f(v) \neq f(\vec{0})$ (solamente il vettore nullo viene mandato nel vettore nullo), quindi $\text{Ker } f = \{\vec{0}\}$
- 2 \implies 1 Siano $v_1, v_2 \in V : f(v_1) = f(v_2)$, devo mostrare che $v_1 = v_2$. Dalla 2, $f(v_1 - v_2) = f(v_1) - f(v_2) = \vec{0}$, ovvero $v_1 - v_2 \in \text{Ker } f$, ma $\text{Ker } f = \{\vec{0}\}$, quindi $v_1 - v_2 = \vec{0} \iff v_1 = v_2$, ovvero f é iniettiva

5.3 Teorema del rango

Sia $f : V \rightarrow U$ applicazione lineare:

$$\dim(V) = \dim(\text{Ker } f) + \dim(\text{Im } f)$$

5.3.1 Dimostrazione

Sia v_1, \dots, v_k base di $\text{Ker } f$ ($\dim(\text{Ker } f) = k$), la completo a una base $v_1, \dots, v_k, v_{k+1}, \dots, v_n$ di V ($\dim(V) = n$).

Avendo una base di V , so che $\forall v \in V, \exists! a_1, \dots, a_n \in K : v = a_1 v_1 + \dots + a_n v_n$.

Poiché f é lineare, $f(a_1 v_1 + \dots + a_n v_n) = \underbrace{a_1 v_1 + \dots + a_k v_k}_{\in \text{Ker } f} + a_{k+1} v_{k+1} + \dots + a_n v_n$.

Questo significa che ogni vettore v di V si scrive come combinazione lineare di v_{k+1}, \dots, v_n , ovvero $\{v_{k+1}, \dots, v_n\}$ é una base di $\text{Im } f$ ($\dim(\text{Im } f) = n - k$).

Infine, unendo i pezzi, ottengo $\dim(V) = n = \dim(\text{Ker } f) + \dim(\text{Im } f) = k + n - k$.

5.4 Rapporto tra dimensione e iniettività/suriettività

1. se $\dim(V) > \dim(U)$, allora f **non può essere iniettiva**
2. se $\dim(V) < \dim(U)$, allora f **non può essere suriettiva**
3. se $\dim(V) = \dim(U)$, allora f é **biunivoca**

5.4.1 Dimostrazione

1. $\dim(\text{Im } f) \leq \dim(U) < \dim(V) \quad \underbrace{=}_{\text{teorema del rango}} \quad \dim(\text{Im } f) + \dim(\text{Ker } f) \iff$
 $\dim(\text{Im } f) < \dim(\text{Im } f) + \dim(\text{Ker } f) \iff \dim(\text{Ker } f) > 0 \implies \text{Ker } f \neq \{\vec{0}\} \text{ (} f \text{ non é iniettiva)}$
2. $\dim(\text{Im } f) + \dim(\text{Ker } f) < \dim(U) \implies \dim(\text{Im } f) \neq \dim(U) \text{ (} \dim(\text{Ker } f) \geq 0 \text{), quindi } f \text{ non é suriettiva perché non é } = U$
3. $\dim(\text{Ker } f) + \dim(\text{Im } f) = \dim(V) = \dim(U) \text{ ma } \dim(\text{Im } f) \leq \dim(U) \implies \dim(\text{Im } f) = \dim(U) \wedge \dim(\text{Ker } f) = 0$