

# Geometria

22 giugno 2015

<b>1</b>	<b>Spazi vettoriali</b>	<b>3</b>
1.1	Proprietà principali . . . . .	3
1.2	Sottospazi vettoriali . . . . .	4
1.3	Sistemi di generatori . . . . .	6
1.4	Basi e dimensioni . . . . .	8
1.5	Spazi quoziente . . . . .	12
1.6	Algebre . . . . .	13



## Capitolo 1

# Spazi vettoriali

### 1.1 Proprietà principali

**Definizione 1.1.1.** Dato un campo  $K$ , un insieme  $V$  non vuoto e due operazioni interne  $+: V \times V \rightarrow V$  e  $\cdot: K \times V \rightarrow V$ , la terna  $(V, +, \cdot)$  si definisce spazio vettoriale sul campo  $K$  se sono soddisfatte le seguenti proprietà:

- $(V, +)$  è un gruppo abeliano;
- $1_K x = x$  per ogni  $x \in V$ ;
- la proprietà associativa, ossia se  $\forall \lambda, \mu \in K$  e  $\forall x \in V$ , si ha  $\lambda(\mu x) = (\lambda\mu)x$ ;
- la proprietà distributiva, ossia se  $\forall \lambda, \mu \in K$  e  $\forall x, y \in V$ , si ha  $(\lambda + \mu)x = \lambda x + \mu x$  e  $\lambda(x + y) = \lambda x + \lambda y$ .

Gli elementi di  $V$  si chiamano *vettori* mentre quelli di  $K$  *scalari*. L'elemento neutro della somma, che per le proprietà note dei gruppi esiste ed è unico, sarà indicato con  $0$ , oppure  $0_V$  in caso di ambiguità. Lo zero e l'unità del campo  $K$  seguono la convenzione già usata per la quale saranno indicati con  $0$  e  $1$ , o anche  $0_K$  e  $1_K$ ; il fatto che  $0$  indichi sia lo zero di  $K$  che quello di  $V$  sarà spesso chiaro dal contesto.

#### Esempi

- $(\mathbb{R}^n, +, \cdot)$ , l'insieme delle  $n$ -uple ordinate di numeri reali, è uno spazio vettoriale su  $\mathbb{R}$ , infatti  $\forall \lambda \in \mathbb{R}$  si ha, rappresentando i vettori come colonne,

$$\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

eccetera definendo somma e prodotto per scalare componente per componente.

- L'anello dei polinomi  $\mathbb{R}[x]$  è uno spazio vettoriale su  $\mathbb{R}$  con l'addizione e il prodotto per un numero reale, dove moltiplicare un polinomio per  $\lambda \in \mathbb{R}$  equivale a moltiplicare per tale scalare tutti i suoi termini.
- L'insieme delle funzioni (qualunque) definite da un insieme  $X \neq \emptyset$  e a valori reali forma uno spazio vettoriale, con le operazioni di addizione e prodotto per numero reale "puntuali", ossia  $(f + g)(x) = f(x) + g(x)$  e  $(\lambda f)(x) = \lambda f(x)$ .
- Ogni campo può essere visto come spazio vettoriale su se stesso: ad esempio  $(\mathbb{R}, +, \cdot)$  è uno spazio vettoriale su  $\mathbb{R}$ , e  $(\mathbb{C}, +, \cdot)$  è uno spazio vettoriale su  $\mathbb{C}$  ma anche su  $\mathbb{R}$  se lo consideriamo come l'insieme delle coppie  $(a, b) = a + ib$  con  $a, b \in \mathbb{R}$ .

Elenchiamo ora una serie di proprietà di base sugli spazi vettoriali, in cui assumiamo  $V$  come spazio vettoriale su un campo  $K$ .

**Proprietà 1.1.2.** Per ogni vettore  $x \in V$ ,  $0_K x = 0_V$ .

*Dimostrazione.* Lo  $0_K$  si può sempre scrivere come somma di  $0_K$  con se stesso, quindi  $0_K x = (0_K + 0_K)x = 0_K x + 0_K x$ . Poiché  $V$  è abeliano, sommando l'inverso di  $0_K x$  ai due membri si ottiene  $0_K x = 0_V$ .  $\square$

**Proprietà 1.1.3.** Per ogni scalare  $a \in K$  e  $\forall x \in V$ ,  $-(ax) = (-a)x$ .

*Dimostrazione.* Per la proprietà precedente si ha  $0_V = 0_K x$ , e lo zero scalare si scrive come somma degli inversi  $a + (-a)$ , quindi  $0_V = [a + (-a)]x = ax + (-a)x$ , che significa che  $(-a)x$  è il vettore inverso di  $ax$  rispetto alla somma, ossia  $(-a)x = -(ax)$ .  $\square$

**Proprietà 1.1.4.** Per ogni  $a \in K$ ,  $a0_V = 0_V$ .

*Dimostrazione.* Si ha che  $a0_V = a(0_V + 0_V) = a0_V + a0_V$ , e come per la proprietà 1.1.2 poiché  $V$  è abeliano si somma ai due membri dell'uguaglianza l'inverso di  $a0_V$ , ottenendo  $a0_V = 0_V$ .  $\square$

**Proprietà 1.1.5.** Se  $ax = 0_V$  per  $a \in K$  e  $x \in V$ , allora  $a = 0_K$  o  $x = 0_V$ .

*Dimostrazione.* Se  $a = 0_K$  è ovvia, se invece  $a \neq 0_K$  allora esiste il suo inverso,  $a^{-1} \in K$ , rispetto al prodotto in  $K$  (cioè tale che  $aa^{-1} = 1_K$ ). Quindi  $0_V = a^{-1}0_V$ , e poiché per ipotesi  $ax = 0_V$  segue che  $0_V = a^{-1}(ax) = (aa^{-1})x = 1_K x = x$ , perciò  $x = 0_V$ .  $\square$

**Proprietà 1.1.6.** Per ogni  $a, b \in K$  e per ogni  $x \in V$ , se  $ax = bx$  allora  $a = b$  oppure  $x = 0_V$ .

*Dimostrazione.* Se vale che  $ax = bx$ , allora aggiungendo l'inverso di  $bx$  per la somma si ottiene  $ax - (bx) = 0_V$ . Inoltre per la proprietà distributiva questo è uguale ad  $ax + (-b)x = (a - b)x = 0_V$ . Per la proprietà 1.1.5, infine,  $a + (-b) = 0_K$  oppure  $x = 0_V$ . Sommando  $b$  alla prima delle due risulta  $a = b$  o  $x = 0_V$ .  $\square$

**Proprietà 1.1.7.** Per ogni scalare  $\lambda \in K$  e  $\forall x, y \in V$ , se  $\lambda x = \lambda y$  allora  $\lambda = 0_K$  o  $x = y$ .

*Dimostrazione.* Da  $\lambda x = \lambda y$  risulta  $\lambda x + (-\lambda y) = \lambda x + \lambda(-y) = 0_V$ . Per la proprietà distributiva equivale a  $\lambda(x + (-y)) = 0_V$ , da cui sempre per la 1.1.5  $\lambda = 0_K$  oppure  $x + (-y) = 0_V$ , da cui sommando  $y$  ai due membri risulta  $\lambda = 0_K$  oppure  $x = y$ .  $\square$

## 1.2 Sottospazi vettoriali

**Definizione 1.2.1.** Sia  $V$  uno spazio vettoriale sul campo  $K$ . Un suo sottoinsieme  $W \subseteq V$  non vuoto si dice sottospazio vettoriale se  $(W, +, \cdot)$ , con le operazioni indotte da  $V$ , è a sua volta uno spazio vettoriale.

In altre parole un sottospazio (ommetteremo spesso l'attributo “vettoriale” per brevità) è un sottoinsieme che risulta chiuso rispetto alle due operazioni dello spazio vettoriale che lo contiene. Per verificare che un insieme  $W$  sia un sottospazio bisogna dunque provare che le combinazioni lineari di elementi di  $W$  siano ancora in  $W$ : una condizione necessaria facile da verificare è che  $W$  deve contenere lo  $0_V$ .

Ogni spazio vettoriale  $V$  contiene sempre due spazi vettoriali, che sono banalmente  $\{0_V\}$  e  $V$  stesso. Vediamone altri esempi.

- Preso lo spazio vettoriale  $\mathbb{R}^n$ , l'insieme

$$N = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ 0 \end{pmatrix} : x_1, \dots, x_{n-1} \in \mathbb{R} \right\}$$

è un sottospazio vettoriale, perché ognuna delle due operazioni dà sempre come risultato un vettore con l' $n$ -esima componente nulla.

- Dato  $\mathbb{R}[x]$ , l'insieme dei polinomi di grado non maggiore di  $n$ , indicato con  $\mathbb{R}_n[x] = \{p(x) = a_0 + a_1x + \dots + a_nx^n : a_0, a_1, \dots, a_n \in \mathbb{R}\}$ , formano un sottospazio vettoriale di  $\mathbb{R}[x]$ . Infatti la somma di due polinomi di grado massimo  $n$  è ancora un polinomio di grado massimo  $n$ , mentre moltiplicando un polinomio per uno scalare non nullo si moltiplicano i coefficienti di ogni termine per tale scalare, quindi il grado rimane immutato. Moltiplicando per zero si ottiene invece un polinomio nullo, che ha ancora ovviamente grado minore di  $n$ . Lo stesso vale per  $\mathbb{C}_n[x] \leq \mathbb{C}[x]$ .
- L'insieme  $\mathcal{C}(\mathbb{R})$  delle funzioni definite da  $\mathbb{R}$  a  $\mathbb{R}$  e continue è un sottospazio vettoriale dello spazio delle funzioni  $f: \mathbb{R} \rightarrow \mathbb{R}$ . Infatti sommando due funzioni continue si ottiene una funzione continua, e ovviamente anche moltiplicando una funzione continua per uno scalare.

**Teorema 1.2.2.** Sia  $V$  uno spazio vettoriale su un campo  $K$  e sia  $\{W_i\}_{i \in I}$  un insieme di sottospazi vettoriali di  $V$ . Allora la loro intersezione  $\bigcap_{i \in I} W_i$  è ancora un sottospazio vettoriale di  $V$ .

*Dimostrazione.* Siano  $w_1, w_2 \in \bigcap_{i \in I} W_i$ . Allora  $\forall i \in I$ ,  $w_1$  e  $w_2$  appartengono a  $W_i$  (appartengono a tutti i sottospazi). Poiché i  $W_i$  sono sottospazi vettoriali, allora accade sempre che  $\forall i \in I$ ,  $w_1 + w_2 \in W_i$ , quindi appartengono anche a  $\bigcap_{i \in I} W_i$ . Un ragionamento analogo si effettua per il prodotto per scalare. Quindi  $\bigcap_{i \in I} W_i$  è un sottospazio vettoriale di  $V$ .  $\square$

Il teorema non vale se al posto dell'intersezione si effettua l'unione dei  $W_i$ : ad esempio le due rette  $x = 0$  e  $y = x$ , rappresentate in forma vettoriale come  $\left\{\begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R}\right\}$  e  $\left\{\begin{pmatrix} x \\ x \end{pmatrix} : x \in \mathbb{R}\right\}$ , sono banalmente due sottospazi vettoriali di  $\mathbb{R}^2$ . Prendendo però un elemento del primo e uno del secondo,  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  e  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ , sommandoli si ottiene  $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$  che non appartiene all'unione dei due sottospazi.

**Definizione 1.2.3.** Siano  $V$  uno spazio vettoriale su  $K$  e  $S \subseteq V$  un insieme non vuoto. Si dice sottospazio generato di  $V$ , e si indica con  $\langle S \rangle$ , un sottospazio vettoriale che soddisfa le seguenti due proprietà:

- $S \subseteq \langle S \rangle$ ;
- se  $W \leq V$  tale che  $S \subseteq W$ , allora  $\langle S \rangle \leq W$ .

**Teorema 1.2.4.** Siano  $V$  uno spazio vettoriale su  $K$  e  $S \subseteq V$  un insieme non vuoto, esiste sempre  $\langle S \rangle$  ed è unico.

*Dimostrazione.* Mostriamo l'esistenza: costruiamo l'insieme  $\langle S \rangle = \bigcap_{i \in I} Z_i$  dove  $\{Z_i\}_{i \in I}$  sono tutti sottospazi vettoriali di  $V$  che includono  $S$ ; ogni  $Z_i$  non è vuoto perché include  $S$ . Sicuramente  $\langle S \rangle$  è, a sua volta, un sottospazio di  $V$  per il teorema 1.2.2.  $S$  è contenuto in ogni  $Z_i$ , quindi è incluso anche in  $\langle S \rangle = \bigcap_{i \in I} Z_i$ . Inoltre, sia  $W$  un sottospazio di  $V$  tale che  $S \subseteq W$ : allora  $S \subseteq \langle S \rangle \subseteq W$ . Poiché  $\langle S \rangle$  è un sottospazio vettoriale, per ogni  $x, y \in S$  e  $\lambda, \mu \in K$  ( $x$  e  $y$  appartengono a  $\langle S \rangle$  e a  $W$ ), mentre  $\lambda x + \mu y \in \langle S \rangle$ , quindi  $\langle S \rangle \leq W$ . Tale  $\langle S \rangle$  rispetta dunque la definizione 1.2.3.

Vediamo ora l'unicità. Se  $Z_1, Z_2$  sono due sottospazi vettoriali di  $V$  che soddisfano la definizione 1.2.3, allora  $S \subseteq Z_1$  e  $S \subseteq Z_2$ . Se poi per un altro sottospazio vettoriale  $W$  si ha  $S \subseteq W$ , allora sempre dalla definizione si deve avere  $Z_1 \leq W$  e analogamente  $Z_2 \leq W$ . Ma anche  $Z_2$  è un sottospazio di  $V$  e  $S \subseteq Z_2$ , dunque  $Z_1 \leq Z_2$ , e allo stesso modo  $Z_2 \leq Z_1$ , quindi  $Z_1 = Z_2$ .  $\square$

Definiamo ora la somma di sottospazi come l'insieme  $U + W = \{u + w : u \in U, w \in W\}$ : esso è un sottospazio vettoriale, infatti

$$\begin{aligned}(u_1 + w_1) + (u_2 + w_2) &= (u_1 + u_2) + (w_1 + w_2) \in U + W \\ \lambda(u + w) &= \lambda u + \lambda w \in U + W.\end{aligned}$$

Dimostriamo inoltre che  $U + W$  è lo spazio generato dall'unione dei due sottospazi, seguendo la definizione 1.2.3.

**Teorema 1.2.5.** Siano  $U, W$  sottospazi vettoriali di  $V$  su un campo  $K$ . Allora  $\langle U \cup W \rangle \equiv U + W$ .

*Dimostrazione.* Ogni  $u \in U$  si può scrivere come  $u + 0_W = u + 0_V$  che quindi appartiene a  $U + W$ , quindi  $U \subseteq U + W$  e analogamente  $W \subseteq U + W$ , quindi  $U \cup W \subseteq U + W$ . Consideriamo un sottospazio vettoriale  $T$  di  $V$  che includa  $U \cup W$ : ogni elemento  $u + w$  appartiene anche a  $T$  per qualunque  $u$  e  $w$ , ma allora  $U + W$  è un sottoinsieme di  $T$  oltre che uno spazio vettoriale, e ciò lo rende un sottospazio vettoriale di  $T$ . Abbiamo allora dimostrato che  $U + W$  soddisfa la definizione 1.2.1, perciò  $U + W = \langle U \cup W \rangle$ .  $\square$

### 1.3 Sistemi di generatori

Sia  $V$  uno spazio vettoriale su  $K$ , e  $S \subseteq V$  un insieme non vuoto. Le combinazioni lineari (sempre finite!) di elementi di  $S$  sono definite come

$$\sum_{i=1}^n \lambda_i s_i = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n,$$

con  $\lambda_i \in K$ ,  $s_i \in S$  e  $n \in \mathbb{N}$ .

**Teorema 1.3.1.** Sia  $V$  uno spazio vettoriale su  $K$ , e  $S \subseteq V$  non vuoto. Allora

$$\langle S \rangle = \left\{ \sum_{i=1}^n \lambda_i s_i : \lambda_i \in K, s_i \in S, i = 1, 2, \dots, n, n \in \mathbb{N} \right\}.$$

*Dimostrazione.* Questo particolare  $\langle S \rangle$  deve soddisfare la definizione 1.2.3:

- gli elementi  $s_i$  appartengono a  $S$ , e possiamo esprimerli come  $s_i = 1_K s_i$  quindi  $S \subseteq \langle S \rangle$ ;
- se  $W \leq V$  e  $S \subseteq W$ , allora dato che  $\langle S \rangle \supseteq S$  se prendiamo una combinazione lineare di due elementi di  $S$ , lo è anche di elementi di  $W$ , e poiché il risultato è sempre un elemento di  $\langle S \rangle$  quest'ultimo è un sottospazio vettoriale di  $W$ .  $\square$

Per l'unicità del sottospazio generato, questa è anche l'unica forma che  $\langle S \rangle$  assume.

**Definizione 1.3.2.** Sia  $V$  uno spazio vettoriale sul campo  $K$  e sia  $S \subseteq V$  un insieme non vuoto.  $S$  è detto sistema di generatori per  $V$  se  $\langle S \rangle = V$ .

Il fatto che con alcuni elementi di uno spazio  $V = \langle S \rangle$  possiamo ricostruire tramite delle combinazioni lineari tutti i restanti è molto utile, in quanto possiamo dedurre molte proprietà di  $V$  studiando soltanto  $S$ . La situazione però si può ancora migliorare, come vedremo in seguito: il problema principale è che, senza ulteriori ipotesi, potrebbero esistere molti modi di esprimere  $v \in V$  in termini di combinazioni lineari di elementi di  $S$ .

#### Esempi

- Come già detto, i vettori di  $\mathbb{R}^n$  sono definiti dalle loro coordinate, quindi possono essere scritti come combinazioni lineari di questi elementi: allora

$$\mathbb{R}^n = \left\langle \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\} \right\rangle$$

I vettori dello spazio generatore sono a tutti gli effetti dei versori di  $\mathbb{R}^n$ ; in questo esempio sono i versori allineati con gli assi cartesiani.

- $\mathbb{R}[x]$  è generato da  $\{1, x, x^2, \dots, x^n, \dots\}$ ; questo insieme è infinito, perché non esiste un polinomio “di grado massimo”. Ogni  $x \in \mathbb{R}[x]$  è determinato da una combinazione lineare di questi componenti, in modo univoco.
- In  $\mathbb{R}^2$  si può individuare il sistema di generatori  $\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}$ . Con questo insieme però si può scrivere l'elemento  $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$  in due modi diversi, ossia come  $2\begin{pmatrix} 0 \\ 1 \end{pmatrix} + 2\begin{pmatrix} 1 \\ 0 \end{pmatrix} + 0\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  ma anche come  $0\begin{pmatrix} 0 \\ 1 \end{pmatrix} + 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ .

**Definizione 1.3.3.** Sia  $V$  uno spazio vettoriale su  $K$ , e  $\{v_i\}_{i \in I} \subseteq V$ . Si dice che l'insieme  $\{v_i\}_{i \in I}$  è linearmente dipendente se esiste  $I_0 \subseteq I$ , di cardinalità  $n$  finita, e un insieme di scalari  $\{\lambda_i\}_{i \in I}$  non tutti nulli tali per cui

$$\sum_{i \in I} \lambda_i v_i = 0_V.$$

Nell'ultimo degli esempi precedenti l'insieme  $\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}$  è linearmente dipendente.

Ovviamente, un sistema che non è linearmente dipendente si dice *linearmente indipendente*.

**Definizione 1.3.4.** Un insieme finito di vettori  $\{v_1, v_2, \dots, v_k\}$  si dice linearmente indipendente, se in ogni combinazione lineare dei  $k$  vettori che produce  $0_V$  i coefficienti sono tutti nulli:

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_k v_k = 0_V \quad \Rightarrow \quad \lambda_1 = \lambda_2 = \dots = \lambda_k = 0_K.$$

Un insieme infinito di vettori  $\{v_i\}_{i \in I}$  è linearmente indipendente se  $\forall J \subseteq I$  di cardinalità finita  $\{v_j\}_{j \in J}$  è linearmente indipendente.

Alcuni esempi di insiemi linearmente indipendenti:

- il sistema che genera  $K_n[x]$ , ossia  $\{1, x, x^2, \dots, x^n\}$ , è linearmente indipendente perché un polinomio è identicamente nullo se e solo se tutti i coefficienti dei vari termini sono nulli. Lo stesso vale per i polinomi di grado non limitato di  $K[x]$ , poiché la definizione è verificata da “blocchi” di termini.
- l'insieme  $\{v, w, 0_V, z\} \subset V$  spazio vettoriale su  $K$  non lo è, poiché  $0_K v + 0_K w + 1_K 0_V + 0_K z = 0_V$  anche se uno dei coefficienti,  $1_K$ , non è nullo. In generale ogni insieme che contenga l'elemento nullo dello spazio è sempre linearmente dipendente.

Il seguente teorema indica un modo più semplice di verificare questa definizione.

**Teorema 1.3.5.** Un insieme di vettori  $\{v_i\}_{i \in I} \subset V$  è linearmente dipendente se e solo se almeno uno di essi è una combinazione lineare di un numero finito dei rimanenti.

*Dimostrazione.* Sia dato un insieme  $\{v_i\}_{i=1}^k$  linearmente dipendente: esiste allora una combinazione lineare  $\sum_{n=1}^k \lambda_n v_n = 0_V$  senza che tutti i  $\lambda_n$  siano nulli. Trascurando nella serie gli eventuali termini nulli, possiamo allora scrivere  $\lambda_1 v_1 = -\lambda_2 v_2 - \dots - \lambda_n v_n$ . Poiché  $\lambda_1$  non è nullo, esiste il suo inverso rispetto al rapporto,  $(\lambda_1)^{-1}$ , e moltiplicando la precedente equazione per questo risulta che il primo termine è  $(\lambda_1)^{-1}(\lambda_1 v_1) = (\lambda_1^{-1} \lambda_1) v_1 = v_1$  da cui

$$v_1 = (\lambda_1^{-1})(-\lambda_2 v_2 - \dots - \lambda_n v_n),$$

cioè  $v_1$  è combinazione lineare degli altri vettori dell'insieme.

Viceversa, sia  $v^* \neq 0_V$  un vettore dell'insieme dato, combinazione lineare (in cui quindi i coefficienti non possono essere tutti nulli) di alcuni dei vettori rimanenti, quindi

$$v^* = \mu_1 v_1 + \mu_2 v_2 + \dots + \mu_r v_r.$$

Portando tutto al primo termine risulta  $v^* - \mu_1 v_1 - \mu_2 v_2 - \dots - \mu_r v_r = 0_V$  sebbene non siano tutti nulli, ossia l'insieme dei  $v_i$  è linearmente dipendente.  $\square$

## 1.4 Basi e dimensioni

**Definizione 1.4.1.** Si chiama base di uno spazio vettoriale  $V$  ogni sistema  $S$  linearmente indipendente che genera  $S$ .

La base in un certo senso “codifica” tutto ciò che è necessario sapere dello spazio vettoriale: tramite delle combinazioni lineari possiamo ricostruire tutto lo spazio a partire da un numero limitato di elementi. Il vantaggio delle basi è che esiste sempre un unico modo di esprimere ogni vettore dello spazio in termini dei suoi elementi, come dimostriamo nel teorema seguente.

**Teorema 1.4.2.** Sia  $\{e_i\}_{i \in I}$  un insieme di  $V$ . Esso è una base di  $V$  se e solo se ogni elemento  $v \in V$  non nullo si può scrivere in modo univoco come combinazione lineare finita, a coefficienti non nulli, di elementi di  $\{e_i\}_{i \in I}$ .

Gli elementi  $v$  non devono essere nulli, perché  $0_V$  si può scrivere come combinazione lineare di qualunque sistema di vettori; inoltre i coefficienti della combinazione non devono essere nulli poiché altrimenti si potrebbe affermare che  $v = ae_1 + be_2$  ma anche  $v = ae_1 + be_2 + 0_K e_3 + \dots + 0_K e_n + \dots$  a piacere.

*Dimostrazione.* Dimostriamo che la condizione è necessaria. Sia  $\{e_i\}_{i \in I}$  una base di  $V$ : essa per definizione genera tutto  $V$ . Preso un elemento  $v \in V$  non nullo, possiamo scriverlo come una combinazione lineare finita

$$v = \sum_{i \in I_0} \lambda_i e_i, \quad (1.4.1)$$

con  $I_0 \subset I$  di cardinalità finita. Dimostriamo che questa scrittura è unica: supponiamo che  $\forall i \in I_0$   $\lambda_i \neq 0_K$  (eventuali termini nulli nella combinazione lineare si trascurano), e supponiamo che esista anche

$$v = \sum_{j \in J_0} \mu_j e_j \quad (1.4.2)$$

con  $\mu_j \neq 0_K \forall j \in J_0 \subset I$  e tale  $J_0$  di cardinalità finita. Sommando gli opposti della (1.4.2) alla (1.4.1) si ha

$$\sum_{i \in I_0} \lambda_i e_i + \sum_{j \in J_0} -\mu_j e_j = 0_V.$$

Sia  $I_0 \neq J_0$ , e prendiamo  $j_0 \in J_0$  ma  $\notin I_0$ . L'elemento  $e_{j_0}$ , nella combinazione, è associato a un coefficiente  $-\mu_{j_0} \neq 0_K$  (quindi esiste il suo reciproco). Portando  $-\mu_{j_0} e_{j_0}$  al secondo membro dell'uguaglianza e moltiplicando per il reciproco di  $\mu_{j_0}$  risulta

$$\sum_{i \in I_0} (\lambda_i \mu_{j_0}^{-1}) e_i + \sum_{j \in J_0} (\mu_j \mu_{j_0}^{-1}) e_j = e_{j_0},$$

cioè uno degli  $e_i$  è espresso come combinazione lineare degli altri, vale a dire la base è linearmente dipendente, il che è assurdo: quindi non può esistere un  $j_0$  che appartiene a  $J_0$  ma non a  $I_0$ . Ponendo  $j_0 \in I_0$  e  $\notin J_0$  si ottiene allo stesso modo un'altra contraddizione. Allora non può che essere  $I_0 = J_0$ , ma ciò significa che

$$\sum_{i \in I_0} (\lambda_i - \mu_i) e_i = 0_V,$$

cui segue che  $\lambda_i = \mu_i \forall i \in I_0$ , cioè le (1.4.1) e (1.4.2) sono identiche: dunque la scrittura di  $v$  in termini della base è unica.

Mostriamo ora che la condizione è anche sufficiente: innanzitutto,  $\langle \{e_i\}_{i \in I} \rangle = V$  perché per ipotesi possiamo scrivere ogni vettore di  $V$  come combinazione lineare di elementi di questo insieme. Supponiamo per assurdo che  $\{e_i\}_{i \in I}$  sia linearmente dipendente, ossia che esista  $I_0 \subset I$  di cardinalità finita per cui

$$\sum_{i \in I_0} \lambda_i e_i = 0_V, \quad (1.4.3)$$



e come prima che  $\lambda_i \neq 0_K \forall i \in I_0$ . Considerando un  $i^* \in I_0$ ,  $\lambda_{i^*}$  non è nullo, quindi moltiplicando la (1.4.3) per il suo inverso si trova

$$\sum_{i \in I_0} (\lambda_{i^*}^{-1} \lambda_i) e_i = 0_V.$$

Isolando il termine in  $i^*$  si ottiene poi che

$$\sum_{i^* \neq i \in I_0} (\lambda_{i^*}^{-1} \lambda_i) e_i = -e_{i^*} \quad (1.4.4)$$

vale a dire che  $e_{i^*}$  si esprime come combinazione lineare di altri elementi dell'insieme. Ma allora ogni volta che scriviamo un vettore come combinazione lineare che contenga  $e_{i^*}$  possiamo scegliere di usare, indifferentemente, il primo o il secondo membro della (1.4.4), e ciò viola l'ipotesi che la scrittura di ogni vettore di  $V$  in termini degli  $e_i$  sia unica. Dunque un tale  $I_0$  non può esistere: dunque l'insieme è linearmente indipendente, e dato che genera  $V$  è una sua base.  $\square$

**Definizione 1.4.3.** Sia  $V$  uno spazio vettoriale su  $K$ : esso si dice di *dimensione finita* se ammette un sistema finito di generatori, altrimenti si dice di *dimensione infinita*.

**Teorema 1.4.4.** Sia  $G \subset V$  un sistema di generatori di  $V$  finito. Se  $S \subseteq G$  è linearmente indipendente, allora esiste una base  $B$  di  $V$  tale che  $S \subseteq B \subseteq G$ .

*Dimostrazione.* Si supponga che  $V$  abbia dimensione finita: allora esiste un sistema di generatori  $G$ .<sup>1</sup> Escludiamo il caso in cui  $V \equiv \{0_V\}$  perché non esisterebbe nemmeno una base.

Indichiamo con  $S_n$  il fatto che nell'insieme linearmente indipendente  $S$  ci siano  $n$  vettori. Potrebbe essere che  $\langle S_n \rangle \equiv V$ , ma allora possiamo scegliere subito  $S_n$  come base per  $V$ , e poiché  $B = S_n \subseteq G$  il teorema è dimostrato. Sia allora  $\langle S_n \rangle \neq V$ : deve esistere  $x_{n+1} \in G$ , ma  $\notin \langle S_n \rangle$  (perché altrimenti dato che  $\langle S \rangle \supseteq G$  si avrebbe che  $\langle S_n \rangle \equiv V$ ). Definiamo  $S_{n+1} = S_n \cup \{x_{n+1}\}$ , per cui sicuramente vale  $S_n \subseteq S_{n+1} \subseteq G$ . Questo  $S_{n+1}$  è un insieme linearmente indipendente, altrimenti avremmo che  $x_{n+1} \in \langle S_n \rangle$ . Se  $\langle S_{n+1} \rangle = V$  il teorema è dimostrato, altrimenti procediamo aggiungendo un altro elemento di  $G \setminus \langle S_{n+1} \rangle$ . Iteriamo il processo per  $n+2$ ,  $n+3$  e così via: il processo deve necessariamente terminare poiché

$$S_n \subseteq S_{n+1} \subseteq S_{n+2} \subseteq \cdots \subseteq G$$

e  $G$  è finito. Esisterà dunque  $k \in \mathbb{N}$  per cui  $\langle S_{n+k} \rangle = \langle G \rangle$ , e anche in questo caso abbiamo trovato che  $S_{n+k}$  (che è ancora linearmente indipendente per costruzione) è base di  $V$ .  $\square$

Sempre in  $\mathbb{R}^3$ , per esempio, una delle possibili basi è quella composta dai tre versori  $\{e_1, e_2, e_3\} = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ , ma anche  $\{e_1, e_2, e_2 + e_3\}$  è un'altra base. In effetti ruotando  $e_1$ ,  $e_2$  e  $e_3$  di un angolo qualsiasi si ottiene un'altra base, e se ne ottengono ancora delle altre moltiplicando per degli scalari (anche differenti) i tre versori. Quindi le basi di uno spazio vettoriale sono infinite; quello che non cambia è il numero di elementi di queste basi, che è sempre costante (in questo esempio, la base è sempre composta da tre vettori).

**Corollario 1.4.5.** Ogni spazio vettoriale  $V \neq \{0_V\}$  di dimensione finita ammette almeno una base.

*Dimostrazione.* L'esistenza di un sistema di generatori  $G$  per  $V$  è garantita (semmai prendiamo  $G = V$ ). In tale insieme, un elemento singolo  $v \neq 0_V$  forma da solo un insieme linearmente indipendente  $\{v\}$ . Il teorema precedente assicura dunque l'esistenza di una base  $\mathcal{B}$  di  $V$  tale che  $\{v\} \subseteq \mathcal{B} \subseteq G$ .  $\square$

**Teorema 1.4.6.** Sia  $V$  uno spazio vettoriale di dimensione finita, contenente una base di  $n$  vettori. Allora:

<sup>1</sup>Esiste sempre un sistema di generatori per qualsiasi spazio: nel peggiore dei casi,  $V$  genera se stesso, ossia  $\langle V \rangle = V$ , dunque possiamo prendere  $G = V$ .

1. ogni sistema linearmente indipendente  $S$  di  $n$  vettori è una base di  $V$ ;
2. ogni sistema  $U$  di  $m > n$  vettori è linearmente dipendente;
3. ogni sistema  $W$  di  $m < n$  vettori non può generare  $V$ , cioè  $\langle W \rangle \neq V$ ;
4. ogni sistema  $T$  di  $n$  vettori per cui  $\langle T \rangle = V$  è una base.

*Dimostrazione.*

1. Siano  $\{e_i\}_{i=1}^n$  una base di  $V$ , e  $S = \{f_i\}_{i=1}^n$  un insieme finito linearmente indipendente. Allora

$$f_1 = \sum_{i=1}^n \lambda_i e_i.$$

Poiché  $S$  è linearmente indipendente, almeno un  $\lambda_i$  non è nullo, quindi  $f_1 \neq 0_V$ , e riordinando i vettori nella combinazione possiamo supporre che sia  $\lambda_1 \neq 0_K$ : in questo modo  $\lambda_1 e_1 \neq 0_V$ . Portando quest'ultimo termine al secondo membro e moltiplicando per  $\mu_1 = \lambda_1^{-1}$  risulta con opportuni  $\mu_i \in K$  che

$$e_1 = \mu_1 f_1 + \sum_{i=2}^n \mu_i e_i.$$

Ogni vettore di  $V$  è una combinazione lineare di elementi di  $\{e_i\}_{i=1}^n$ , ma sostituendo  $e_1$  con l'espressione trovata sopra abbiamo  $\forall v \in V$

$$v = \sum_{i=1}^n \lambda_i e_i = \lambda_1 \left( \mu_1 f_1 + \sum_{i=2}^n \mu_i e_i \right) + \sum_{i=2}^n \lambda_i e_i$$

che quindi può essere espresso anche come combinazione lineare di  $\{f_1, e_2, \dots, e_n\}$  anziché degli  $\{e_i\}_{i=1}^n$ , quindi anche l'insieme  $\{f_1, e_2, \dots, e_n\}$  è un sistema di generatori di  $V$ . Dunque troviamo anche che

$$f_2 = \sigma_1 f_1 + \sum_{i=1}^n \sigma_i e_i.$$

Almeno uno dei  $\sigma_i$  non è nullo, altrimenti sarebbe che  $f_2 = \sigma_1 f_1$  che contraddice l'indipendenza lineare degli  $f_i$ . Supponendo  $\sigma_2 \neq 0_K$ , si esplicita  $e_2$  moltiplicando per  $\sigma_2^{-1}$ , ottenendo

$$e_2 = \rho_1 f_1 + \rho_2 f_2 + \sum_{i=3}^n \rho_i e_i.$$

L'insieme  $\{f_1, f_2, e_3, \dots, e_n\}$  è ancora un sistema di generatori di  $V$ . Si itera il procedimento ottenendo alla fine che  $\{f_1, f_2, \dots, f_n\}$  è ancora un sistema di generatori per  $V$ , e dunque ne è una base dato che è linearmente indipendente.

2. Sia  $U$  con  $m > n$  elementi linearmente indipendente, e si prenda  $U' \subset U$  tale che abbia  $n$  elementi (dunque  $U \setminus U' \neq \emptyset$ ). Per il punto 1  $U'$  è una base di  $V$ , quindi i vettori di  $U'$  generano anche quelli di  $U \setminus U'$ . Ciò contraddice l'indipendenza lineare di  $U$ , che deve essere quindi linearmente dipendente.
3. Sia  $W$  con  $m < n$  elementi un sistema di generatori di  $V$ : allora deve esistere una base con al più  $m$  vettori, tanti quanti ce ne sono in  $W$ . Per il punto precedente, la base  $\{e_i\}_{i \in I}$  (considerata nel punto 1) ha più vettori della base estratta da  $W$ , quindi sarebbe linearmente dipendente, che è assurdo. Allora  $W$  non può essere un sistema di generatori di  $V$ .
4. Se  $\langle T \rangle = V$ ,  $T$  deve avere almeno  $n$  elementi per il punto 3; allora esiste  $T' \subseteq T$  che è una base di  $V$ . Se  $T'$  avesse meno di  $n$  elementi, contraddirebbe il punto 3 prima citato, quindi deve averne esattamente  $n$ , perciò  $T \equiv T'$ , e  $T$  è linearmente indipendente. Poiché genera  $V$ ,  $T$  ne è anche una base.

□

**Corollario 1.4.7.** Sia  $V$  uno spazio vettoriale di dimensione finita, contenente una base di  $n$  vettori. Ogni altra base  $V$  ha a sua volta esattamente  $n$  vettori.

**Definizione 1.4.8.** Dato uno spazio vettoriale  $V \neq \{0_V\}$  su  $K$  di dimensione finita, si dice *dimensione di  $V$  su  $K$*  il numero di vettori di una sua base qualunque.

La dimensione di  $V$  (su  $K$ ) si indica con  $\dim_K V$  o anche solo, se non ci sono ambiguità, con  $\dim V$ . Convenzionalmente, allo spazio contenente soltanto  $\{0_V\}$  si assegna la dimensione 0.

**Teorema 1.4.9.** Sia  $V$  uno spazio vettoriale, e  $W$  un suo sottospazio. Se  $\dim V$  è finita, allora  $\dim W \leq \dim V$ .

*Dimostrazione.* Nel caso banale in cui  $W = \{0_V\}$ , la sua dimensione è 0 quindi è ovviamente minore o uguale della dimensione di  $V$ , qualunque essa sia. Se invece  $W$  non contiene soltanto il vettore nullo, una base qualunque di  $W$  è un sistema linearmente indipendente anche in  $V$ . Siccome  $W \neq \{0_V\}$ , esiste un vettore  $w_1 \in W$  non nullo. Se  $\langle w_1 \rangle = W$  allora  $\{w_1\}$  è una base di  $W$  da cui si ottiene subito la tesi: infatti  $w_1$  appartiene anche a  $V$  che dunque ha almeno dimensione 1. Altrimenti  $\langle w_1 \rangle \neq W$  ma comunque esiste un altro vettore di  $W$ ,  $w_2 \notin \langle w_1 \rangle$  (quindi appartenente a  $W \setminus \langle w_1 \rangle$ ). Sia  $S = \{w_1, w_2\}$ : esso è un sistema linearmente indipendente per come abbiamo scelto  $w_2$ . Se  $\langle S \rangle = W$ , come nel caso precedente abbiamo dimostrato il teorema: per teorema precedente (1.4.6)  $V$  ha due vettori linearmente indipendenti dunque deve essere  $\dim V \geq 2 = \dim W$ . Se invece  $\langle S \rangle \neq W$ , si consideri un altro  $w_3 \in W \setminus \langle w_1, w_2 \rangle$  e si ripete il ragionamento compiuto in precedenza. Ogni volta si trova un nuovo insieme  $S = \{w_1, w_2, \dots, w_n\}$ , ancora linearmente indipendente in  $V$ . Per il punto 3, sempre del teorema 1.4.6,  $\dim V \geq |S|$ , quindi  $W$  ha dimensione finita, inoltre  $n = \dim W = |S| \leq \dim V$ . □

**Teorema 1.4.10.** Sia  $V$  uno spazio vettoriale di dimensione finita,  $W$  un suo sottospazio e  $B_W$  una base di  $W$ . Allora tale base si può estendere per formare una base di  $V$ , cioè  $\exists B_V: B_W \subseteq B_V$ .

*Dimostrazione.*  $B_W$  è linearmente indipendente in  $W$  in quanto è una base, e lo è quindi anche in  $V$  (quindi  $\dim V \geq |B_W|$ ), che deve avere un sistema finito  $G$  di generatori. Allora  $B_W \cup G$  è ancora un sistema di generatori per  $V$ , ed è anche finito. Da questo insieme, che per generare  $V$  deve essere tale che  $\dim V \leq |B_W \cup G|$ , possiamo estrarre  $\dim V$  elementi linearmente indipendenti. Poiché  $B_W \subseteq B_W \cup G$  è già linearmente indipendente, esiste una base  $B_V$  di  $V$  contenente  $B_W$  (e contenuta in  $B_W \cup G$ ). □

Ad esempio,  $\mathbb{R}$  è un sottospazio di  $\mathbb{R}^3$ : prendendo una base  $\{v\}$  del primo, si ottiene una base del secondo semplicemente aggiungendo due vettori (distinti) perpendicolari a  $v$ .

**Definizione 1.4.11.** Un insieme  $\{V_i\}_{i \in I}$  di sottospazi vettoriali di  $V$  si dice *linearmente indipendente* se comunque si scelga un vettore  $x_i \neq 0$  per ciascun  $V_i$ , l'insieme  $\{x_i\}_{i \in I}$  è linearmente indipendente.

**Teorema 1.4.12.** Un insieme  $\{V_i\}_{i \in I}$  di sottospazi vettoriali di  $V$  è linearmente indipendente se e solo se  $\forall k \in I$  si ha che l'intersezione tra  $V_k$  e lo spazio generato dai restanti  $V_i$  contiene soltanto lo zero, cioè<sup>2</sup>

$$V_k \cap \sum_{j \in I \setminus \{k\}} V_j = \{0\}.$$

*Dimostrazione.* Se i sottospazi  $V_i$  sono linearmente indipendenti, e per assurdo  $V_k \cap \sum_{j \in I \setminus \{k\}} V_j \neq \{0\}$  per qualche  $k \in I$ , allora esisterebbe un elemento  $v_k \in V_k$  non nullo che è combinazione lineare di elementi dei restanti sottospazi, cioè  $v_k = x_{i_1} + \dots + x_{i_r}$  con  $\{i_1, \dots, i_r\} \subseteq I \setminus \{k\}$ . Ma allora l'insieme  $\{V_i\}_{i \in I}$  dei sottospazi non sarebbe linearmente indipendente, contraddicendo l'ipotesi, quindi l'uguaglianza deve essere vera.

<sup>2</sup>Ricordiamo che la somma di più spazi vettoriali è lo spazio generato dalla loro unione, ossia  $\sum_i V_i = \langle \bigcup_i V_i \rangle$ .

Viceversa, se prendessimo una combinazione lineare nulla di elementi uno da ciascun sottospazio

$$a_{i_1} v_{i_1} + \cdots + a_{i_k} v_{i_k} = 0 \quad (1.4.5)$$

con  $v_{i_j} \in V_{i_j}$  appartenenti tutti a sottospazi distinti, e ci fosse  $a_{i^*} \neq 0$ , allora potremmo scrivere

$$v_{i^*} = \sum_{j \in I \setminus \{i^*\}} c_j v_j \quad (1.4.6)$$

ma allora  $v_{i^*} \in V_{i^*}$  e anche  $v_{i^*} \in \sum_{j \in I \setminus \{i^*\}} V_j$ , ossia esiste un  $i^* \in I$  tale per cui

$$V_{i^*} \cap \sum_{j \in I \setminus \{i^*\}} V_j \neq \{0\}$$

che contraddice l'ipotesi. Dunque nella (1.4.5) si ha  $a_j = 0$  per ogni  $j \in I$ , cioè i sottospazi sono linearmente indipendenti.  $\square$

**Teorema 1.4.13.** Sia  $\{V_i\}_{i \in I}$  un insieme linearmente indipendente di sottospazi vettoriali di  $V$ . Se  $\forall i \in I$  il sistema di vettori  $S_i \subset V_i$  è linearmente indipendente, allora  $\bigcup_{i \in I} S_i$  è linearmente indipendente in  $V$ .

*Dimostrazione.* Consideriamo un sistema linearmente indipendente di vettori  $S_i \subset V_i$  e ipotizziamo per assurdo che l'unione non sia linearmente indipendente. Questo implica che, considerando gli elementi  $y_i^k \in S_i$  con  $i, k \in I_0$  in cui  $I_0 \in I$  ha cardinalità finita,

$$\sum_{1 \leq k \leq n_i} \lambda_i^k y_i^k = 0,$$

per ogni  $\lambda_i^k$  meno un  $\tilde{\lambda}_i^k$ , corrispondente a un  $\tilde{k}$ . Posto  $x_i = \sum_{1 \leq k \leq n_i} \lambda_i^k x_k^i$  sappiamo che  $\sum_{i \in I_0} x_i = 0$  e che un elemento di questa sommatoria non è nullo, ma per ipotesi  $x_i \in S_i$  che è una combinazione di vettori linearmente indipendente, allora deve essere  $x_i = 0$ . L'unione  $S$  dei vari  $S_i$  è allora linearmente indipendente.  $\square$

**Definizione 1.4.14.** Uno spazio vettoriale  $V$  si dice somma diretta di un insieme di sottospazi vettoriali  $\{V_i\}_{i \in I}$  se  $\{V_i\}_{i \in I}$  è linearmente indipendente e se  $\sum_{i \in I} V_i \equiv V$ .

Per indicare che  $V$  è composto dalla somma diretta degli spazi  $V_i$  si usa la scrittura  $V = \bigoplus_{i \in I} V_i$ .

### Esempi

- Lo spazio  $\mathbb{R}[x]$  è generato dall'insieme  $\{1, x, x^2, \dots\}$ . Posto  $V_j = \langle x^j \rangle$ , con  $j \in \mathbb{N}_0$ , si ha che

$$\mathbb{R}[x] = \bigoplus_{j \in \mathbb{N}_0} V_j = \bigoplus_{j \in \mathbb{N}_0} \langle x^j \rangle.$$

- In  $\mathbb{R}^3$ , siano  $V_1 = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$  e  $V_2 = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ . Certamente  $V_1 + V_2 = \mathbb{R}^3$ , ma la somma non è diretta poiché la loro intersezione è l'asse  $y$ .

## 1.5 Spazi quoziente

Sia  $W$  un sottospazio vettoriale di  $V$ . Definiamo la relazione  $x \sim y$ , con  $x, y \in V$ , se  $x - y \in W$ : essa è di equivalenza, perché soddisfa le tre proprietà della definizione ???. Infatti  $x - x = 0_V$  che certamente appartiene a  $W$ ; se  $x - y = w \in W$  esiste, allora deve esistere il suo opposto in  $W$  (ed esiste, dato che  $W$  è uno spazio vettoriale) che è  $-w = y - x \in W$ ; infine se  $x - y = w_1$  e  $y - z = w_2$  sono vettori di  $W$ , allora sommandoli si ottiene  $w_1 - w_2 = x - y + y - z = x - z$  che

poiché  $W$  è uno spazio vettoriale, vi appartiene. Prendiamo un elemento  $a \in V$ : la sua classe di equivalenza è formata da tutti quegli elementi di  $V$  tali che  $a - v \in W$ , cioè

$$[a] = \{x \in V : x - a = w \in W\} = \{w + a : w \in W\}.$$

Questa classe si indica anche come  $W + a$ , che si può leggere come l'insieme degli elementi che sono somma di un elemento di  $W$  e di  $a$  (e che danno un elemento di  $V$ ): essa si chiama anche *laterale destro*<sup>3</sup> di  $W$  in  $V$ , con rappresentante  $a$ . L'insieme di queste classi di equivalenza distinte, come appena descritte, di  $W$  in  $V$  si indica con  $V / W$  e si chiama *spazio quoziente*.

Nello spazio quoziente possiamo definire la somma, che indicheremo con il simbolo  $\oplus$ , di due laterali come

$$(W + a) \oplus (W + b) = W + (a + b).$$

Se anche fosse  $[a] \equiv [a']$  e  $[b] \equiv [b']$ , non è detto a priori che si abbia  $a + b = a' + b'$  come conseguenza della proprietà transitiva<sup>4</sup>. Perché ciò accada serve un'ulteriore condizione, che la relazione sia una *relazione di congruenza*, ossia che sia compatibile con le operazioni in  $V$ . Se da  $x \sim x'$  e  $y \sim y'$  seguono le relazioni  $x + y \sim x' + y'$  e  $\lambda x \sim \lambda x'$ , allora la relazione  $\sim$  è una relazione di congruenza nello spazio vettoriale: mostriamo che la relazione da noi usata per definire lo spazio quoziente lo è.

*Dimostrazione.* Se  $x \sim x'$ , allora  $x - x' = w_1 \in W$ , e analogamente  $y - y' = w_2 \in W$ . Sommandoli, si ottiene  $w_1 + w_2 = x - x' + y - y' = (x + y) - (x' + y')$  che essendo  $W$  un sottospazio vettoriale vi appartengono: allora  $x + y \sim x' + y'$ . Anche per il prodotto con uno scalare  $\lambda$ , si ottiene analogamente che se  $x - x' = w \in W$ , allora sempre poiché  $W$  è un sottospazio vettoriale si ha che  $\lambda x - \lambda x' = \lambda w$  che appartiene a  $W$ .  $\square$

Come per  $\oplus$ , definiamo anche l'operazione analoga al prodotto scalare, che indichiamo con  $\odot$ :

$$\lambda \odot (W + a) = W + \lambda a.$$

La terna  $(V / W, \oplus, \odot)$  è uno spazio vettoriale su  $K$ , dove  $V$  è a sua volta uno spazio vettoriale sul medesimo campo. Infatti, oltre alle proprietà appena dimostrate, esiste l'elemento neutro rispetto a  $\oplus$ , che è  $W + 0_V$  (si indica anche solamente con  $W$ ), e l'opposto, che è  $-(W + a) = W + (-a)$ .

## 1.6 Algebre

**Definizione 1.6.1.** Si definisce algebra sul campo  $K$  uno spazio vettoriale  $A$  sul campo  $K$  munito di un'ulteriore operazione interna di prodotto, che sia associativo e distributivo rispetto alla somma, ossia tale per cui

- $\forall v, w, z \in A$  si ha:  $(vw)z = v(wz)$ ,
- $\forall v, w, z \in A$  e  $\forall \lambda \in K$  si ha  $(\lambda v + w)z = \lambda vz + wz$ .

Un'algebra  $A$  si dice *commutativa* se il prodotto è commutativo, si dice *con unità* se  $\exists I_a : \forall a \in A$  si ha  $aI_a = I_a a = a$ .

<sup>3</sup>In questo caso il laterale è detto *destro* perché il rappresentante  $a$  si trova alla destra dell'operazione. Ovviamente esistono anche laterali sinistri, che in questo caso sarebbero della forma  $a + W$ . Trovandoci in spazi vettoriali, però, la somma è commutativa quindi non ha senso distinguere i due casi.

<sup>4</sup>Ovviamente con  $a \neq a'$  e  $b \neq b'$ , altrimenti sarebbe ovvia: è sufficiente a questo scopo che  $a \sim a'$ , e lo stesso per  $b$ .