Cap. 1

SPAZI VETTORIALI

1.1 Gruppi, anelli e campi.

Sono note allo studente alcune *operazioni* elementari sugli insiemi numerici; ad esempio l'addizione e la moltiplicazione su $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Ciò che tali operazioni hanno in comune è il seguente fatto: ad ogni coppia di numeri viene associato un altro numero (il risultato dell'operazione). Questa semplice osservazione è alla base della seguente definizione di *operazione su un insieme*.

DEFINIZIONE **1**. *Sia A un insieme non vuoto. Sia*

$$A \times A = \big\{(a,b),\ \forall\, a \in A,\ \forall\, b \in A\big\}$$

il prodotto cartesiano di A per se stesso. Ogni applicazione

$$* : A \times A \to A$$

è detta ***operazione su*** *A. L'operazione $*$ associa quindi ad ogni coppia $(a,b) \in A \times A$ la sua immagine $*(a,b)$, che, per semplificare le notazioni, denoteremo con $a * b$. L'operazione $*$ è detta:*

(i) ***associativa****, se risulta:*

$$a * (b * c) = (a * b) * c, \quad \forall\, a,b,c \in A;$$

(ii) ***commutativa****, se risulta:*

$$a * b = b * a, \quad \forall\, a,b \in A.$$

Inoltre:

(iii) l'operazione $*$ ***ammette elemento neutro*** *$e \in A$, se risulta:*

$$a * e = e * a = a, \quad \forall\, a \in A;$$

(iv) l'operazione $*$ ***ammette reciproco*** *(o* ***opposto*** *o* ***inverso****)* ***di ogni elemento*** *se verifica (iii) e se per ogni $a \in A$ esiste $a' \in A$ [dipendente da a] tale che*

$$a * a' = a' * a = e.$$

ESEMPIO **1.** È evidente che l'addizione e la moltiplicazione sono operazioni su $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ verificanti le proprietà $(i), (ii), (iii)$ [con 0 elemento neutro dell'addizione e 1 elemento neutro della moltiplicazione]. Relativamente alla proprietà (iv) si osserva subito che:

(a) l'addizione verifica la proprietà (iv) su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ [il reciproco (o, più propriamente, l'opposto) di a è $-a$] ma non su $\mathbb{N}$ [infatti 1 non ha opposto in $\mathbb{N}$].

(b) la moltiplicazione non verifica la proprietà (iv): infatti 0 non ha reciproco. Ci chiediamo ora cosa avviene se eliminiamo 0. Per $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, denotiamo $A - \{0\}$ con A^*. È evidente che la moltiplicazione verifica la proprietà (iv) come operazione su $\mathbb{Q}^*$, su $\mathbb{R}^*$ e su $\mathbb{C}^*$ [il reciproco (o, meglio, l'inverso) di a è $a^{-1} = \frac{1}{a}$] ma non su $\mathbb{N}^*$ e su $\mathbb{Z}^*$ [infatti ad esempio 2 non ha inverso in $\mathbb{N}^*$ o $\mathbb{Z}^*$].

Veniamo ora alle altre due operazioni elementari: sottrazione e divisione. È evidente che la sottrazione è un'operazione su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (ma non lo è su $\mathbb{N}$) e che la divisione è un'operazione soltanto su $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$. Entrambe le operazioni non verificano alcuna delle proprietà $(i), .., (iv)$.

ESEMPIO **2.** Sia A un insieme non vuoto. Denotiamo con $\mathcal{F}(A)$ l'insieme di tutte le applicazioni di A in sè. Ricordiamo che, $\forall\, f, g \in \mathcal{F}(A)$, si chiama *composizione* (o *prodotto operatorio*) di f e g l'applicazione $g \circ f \in \mathcal{F}(A)$ così definita:

$$(g \circ f)(a) = g(f(a)), \quad \forall\, a \in A.$$

Resta pertanto definita l'operazione di *composizione di applicazioni*:

$$\circ : \mathcal{F}(A) \times \mathcal{F}(A) \to \mathcal{F}(A)$$

tale che:

$$(f, g) \to g \circ f.$$

Tale operazione verifica le proprietà (i) e (iii), cioè è associativa [semplice verifica] ed ammette elemento neutro [che è l'*applicazione identica* (o *identità di* A):

$$\mathbf{1}_A : A \to A \text{ tale che } \mathbf{1}_A(a) = a,\ \forall\, a \in A].$$

Limitiamoci ora a considerare le *applicazioni biunivoche* (o *biiezioni*) su un insieme A e denotiamo con $\mathcal{S}(A)$ l'insieme di tali applicazioni. Poiché la composizione di due biiezioni è ancora una biiezione [semplice verifica], l'operazione $\circ$ si può *restringere* ad $\mathcal{S}(A)$ e dunque è definita l'operazione:

$$\circ : \mathcal{S}(A) \times \mathcal{S}(A) \to \mathcal{S}(A)$$

(*composizione di applicazioni biunivoche*). Tale operazione verifica, oltre alle proprietà (i) e (iii), anche la proprietà (iv). Infatti, assegnata $f \in \mathcal{S}(A)$ e definita l'applicazione $g : A \to A$ tale che:

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

si verifica subito che $g \in \mathcal{S}(A)$ e che $g \circ f = f \circ g = \mathbf{1}_A$ [cioè g è l'elemento reciproco di f]. L'applicazione g è usualmente denotata con f^{-1} ed è detta *applicazione inversa di* f.

Con facili esempi si verifica che in generale la composizione di applicazioni (anche biunivoche) non è un'operazione commutativa (cfr. Eserc. **3**).

Gli esempi precedenti ci introducono al concetto di *gruppo*, cioè un insieme dotato di un'operazione verificante le proprietà $(i), (iii)$ e (iv). Riformuliamo questa definizione.

DEFINIZIONE **2.** *Sia A un insieme non vuoto. Sia $*$ un'operazione su A. La coppia $(A, *)$ è un* ***gruppo*** *se valgono i tre seguenti assiomi:*

$(\mathbf{G}_1)$ $a * (b * c) = (a * b) * c, \quad \forall\, a, b, c \in A$ *[proprietà associativa].*

$(\mathbf{G}_2)$ $\exists\, e \in A$ *[****elemento neutro*** *di A] tale che* $a * e = e * a = a, \quad \forall\, a \in A.$

$(\mathbf{G}_3)$ $\forall\, a \in A,\ \exists\, a' \in A$ *[****reciproco*** *di a] tale che* $a * a' = a' * a = e.$

Il gruppo $(A, *)$ è detto ***gruppo commutativo*** *se vale l'ulteriore assioma:*

$(\mathbf{G}_4)$ $a * b = b * a, \quad \forall\, a, b \in A$ *[proprietà commutativa].*

OSSERVAZIONE **1.** (i) È immediato verificare che in un gruppo $(A, *)$ l'elemento neutro e ed il reciproco a' di ogni elemento $a \in A$ sono unici. Infatti, se e, e' sono due elementi neutri di A, risulta:

$$e' = e * e' = e' * e, \quad e = e' * e = e * e'.$$

Ne segue che $e = e'$. Se poi a', a'' sono due reciproci di a, risulta:

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

Una conseguenza immediata di tale unicità è la seguente formula (la cui verifica è lasciata al lettore):

$$(a * b)' = b' * a', \quad \forall\, a, b \in A.$$

(ii) In $(A, *)$ valgono le seguenti *regole di cancellazione* (o di *semplificazione*) *a sinistra* e *a destra*:

$$a * b = a * c \implies b = c, \quad a * b = c * b \implies a = c,$$

$\forall\, a, b, c \in A$. Proviamo la prima [e per la seconda si proceda in modo analogo]. Denotato, al solito, con a' il reciproco di a, si ha:

$$b = e * b = (a' * a) * b = a' * (a * b) = a' * (a * c) = (a' * a) * c = e * c = c.$$

(iii) Spesso i gruppi vengono presentati con *notazione additiva* [l'operazione viene indicata con $+$, l'elemento neutro con 0 ed il reciproco di a con $-a$ (ed è chiamato *opposto*)] ovvero con *notazione moltiplicativa* [l'operazione viene indicata con $\cdot$, l'elemento neutro con 1 ed il reciproco di a con a^{-1} oppure $\frac{1}{a}$ (ed è chiamato *inverso*)]. Tradizionalmente i gruppi presentati con notazione additiva vengono supposti commutativi.

ESEMPIO **3.** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ sono esempi di gruppi commutativi.

Per ogni insieme A non vuoto, $(\mathcal{S}(A), \circ)$ è un gruppo. Se A ha almeno tre elementi, tale gruppo non è commutativo [cfr. Eserc. **3**(i)]. Se l'insieme A è finito ed è formato da n elementi, il gruppo $\mathcal{S}(A)$ è denotato usualmente con $\mathbf{S}_n$ ed è chiamato *gruppo delle permutazioni su n elementi* [cfr. Eserc. **3**(ii)].

DEFINIZIONE **3.** *Siano $(A, *)$ e $(B, \bullet)$ due gruppi. Sia $f : A \to B$ un'applicazione. f è detta* ***omomorfismo*** *(di gruppi) se risulta:*

$$f(a) \bullet f(b) = f(a * b), \quad \forall\, a, b \in A.$$

Un omomorfismo biiettivo è detto ***isomorfismo****. Inoltre, posto $(B, \bullet) = (A, *)$, un omomorfismo di $(A, *)$ in sè è detto* ***endomorfismo*** *ed un endomorfismo biiettivo è detto* ***automorfismo****.*

OSSERVAZIONE **2.** Dato un omomorfismo $f : (A, *) \to (B, \bullet)$, verifichiamo che:

(i) $f(e) = e'$, [cioè f *conserva gli elementi neutri* e di A ed e' di B].

(ii) $f(a') = f(a)'$, $\forall\, a \in A$ [cioè *l'immagine del reciproco di un elemento è il reciproco della sua immagine*].

Infatti: $f(e) = f(e*e) = f(e) \bullet f(e)$ e quindi $e' \bullet f(e) = f(e) \bullet f(e)$. Cancellando (a destra) segue che $e' = f(e)$. Inoltre, $\forall\, a \in A$:

$$e' = f(e) = f(a * a') = f(a) \bullet f(a') \quad \text{e} \quad e' = f(e) = f(a' * a) = f(a') \bullet f(a).$$

Ne segue che $f(a') = f(a)'$.

DEFINIZIONE **4.** *Sia $(A, *)$ un gruppo e sia B un sottoinsieme non vuoto di A. B [o $(B, *)$] è detto* ***sottogruppo*** *di $(A, *)$ se $(B, *)$ è un gruppo [rispetto alla stessa operazione di $(A, *)$].*

OSSERVAZIONE **3.** Si verifica facilmente che un sottoinsieme non vuoto B di A è un sottogruppo di $(A, *) \iff$ verifica le tre seguenti condizioni:

$$a * b \in B,\ \forall\, a, b \in B; \qquad e \in B; \qquad a' \in B,\ \forall\, a \in B.$$

In particolare $\{e\}$ e A sono sempre sottogruppi di $(A, *)$ [detti *sottogruppi banali di* $(A, *)$]. Lasciamo infine al lettore la verifica del seguente criterio per riconoscere se un sottoinsieme di un gruppo è un sottogruppo.

Sia $(A, *)$ un gruppo e sia B un sottoinsieme non vuoto di A. Risulta:

$$(B, *) \text{ è un sottogruppo di } (A, *) \iff a * b' \in B,\ \forall\, a, b \in B.$$

Riformuliamo tale criterio con le notazioni additiva e moltiplicativa:

$$(B, +) \text{ è un sottogruppo di } (A, +) \iff a - b \in B,\ \forall\, a, b \in B;$$
$$(B, \cdot) \text{ è un sottogruppo di } (A, \cdot) \iff a\, b^{-1} \in B,\ \forall\, a, b \in B.$$

ESEMPIO **4.** (i) $(\mathbb{Z},+)$ è un sottogruppo di $(\mathbb{Q},+)$ ed anche di $(\mathbb{R},+)$ e di $(\mathbb{C},+)$. $(\mathbb{Q},+)$ è un sottogruppo di $(\mathbb{R},+)$ e di $(\mathbb{C},+)$. Analogamente, $(\mathbb{Q}^*,\cdot)$ è un sottogruppo di $(\mathbb{R}^*,\cdot)$ ed anche di $(\mathbb{C}^*,\cdot)$. Inoltre, posto

$$\mathbb{Q}^+ = \{a \in \mathbb{Q} :\ a > 0\} \quad \text{e} \quad \mathbb{R}^+ = \{a \in \mathbb{R} :\ a > 0\},$$

si verifica facilmente che $(\mathbb{Q}^+,\cdot)$ e $(\mathbb{R}^+,\cdot)$ sono rispettivamente sottogruppi di $(\mathbb{Q}^*,\cdot)$ e $(\mathbb{R}^*,\cdot)$.

(ii) Fissato in un insieme non vuoto A un elemento a_0, l'insieme

$$\mathcal{S}(A)_0 = \{f \in \mathcal{S}(A) :\ f(a_0) = a_0\}$$

(biiezioni che fissano a_0) è un sottogruppo di $(\mathcal{S}(A),\circ)$.

(iii) Ogni sottogruppo $(B,*)$ di un gruppo $(A,*)$ definisce un omomorfismo iniettivo (detto *inclusione canonica*):

$$i : (B,*) \to (A,*) \ \text{ tale che } \ i(b) = b, \quad \forall\, b \in B.$$

In particolare, se $B = A$, l'inclusione canonica coincide con l'identità $\mathbf{1}_A$ ed è un automorfismo di $(A,*)$.

Si può facilmente verificare che l'insieme degli automorfismi di $(A,*)$ forma un sottogruppo di $(\mathcal{S}(A),\circ)$, usualmente denotato $Aut(A)$ [cfr. Eserc. **1**(iii)].

DEFINIZIONE **5.** *Sia $f : (A,*) \to (B,\bullet)$ un omomorfismo tra gruppi. Tramite f restano individuati i due seguenti insiemi*

$$Ker(f) = \{a \in A :\ f(a) = e'\} \quad e$$
$$Im(f) = \{f(a),\ \forall\, a \in A\} = \{b \in B :\ b = f(a),\ \exists\, a \in A\}.$$

*$Ker(f)$ è detto **nucleo** (o **kernel**) di f. Si tratta (come verificheremo nell'osservazione che segue) di un sottogruppo di $(A,*)$. $Im(f)$ è detto **immagine** di f. Si tratta (come vedremo) di un sottogruppo di $(B,\bullet)$.*

OSSERVAZIONE **4.** (i) Per verificare che $Ker(f)$ è un sottogruppo di $(A,*)$ possiamo utilizzare il criterio di Oss. **3**. Risulta: $Ker(f) \neq \Phi$ [infatti (in base a Oss. **2**) $e \in Ker(f)$]. Inoltre, $\forall\, a,b \in Ker(f)$:

$$f(a * b') = f(a) \bullet f(b') = f(a) \bullet f(b)' = e' \bullet e' = e'$$

e dunque $a * b' \in Ker(f)$.

Analogamente, per verificare che $Im(f)$ è un sottogruppo di $(B,\bullet)$, osserviamo che $Im(f) \neq \Phi$ [infatti $e' = f(e) \in Im(f)$]. Inoltre, $\forall\, f(a),\ f(b) \in Im(f)$:

$$f(a) \bullet f(b)' = f(a) \bullet f(b') = f(a * b') \in Im(f).$$

(ii) Sia $f : (A,*) \to (B,\bullet)$ un omomorfismo tra gruppi. Ovviamente:

$$f \text{ è suriettivo } \iff Im(f) = (B,\bullet).$$

Lasciamo al lettore la seguente verifica:

$$f \text{ è iniettivo } \iff Ker(f) = \{e\}.$$

Sino ad ora abbiamo considerato insiemi dotati di un'unica operazione (i gruppi). Osserviamo però che gli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono dotati di due operazioni (addizione e moltiplicazione), tra le quali sussiste un'importante relazione (la proprietà distributiva). Questo fatto ci suggerisce la seguente definizione.

DEFINIZIONE **6.** *Un* ***anello*** *è una terna* $(A, +, \cdot)$ *verificante i tre assiomi:*

($\mathbf{A}_1$*)* $(A, +)$ *è un gruppo commutativo [con elemento neutro* $0 = 0_A$*].*

($\mathbf{A}_2$*)* $\cdot : A \times A \to A$ *è un'operazione associativa, cioè:*

$$a(bc) = (ab)c, \quad \forall\, a, b, c \in A.$$

($\mathbf{A}_3$*) Valgono le proprietà distibutive (destra e sinistra)*

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc, \quad \forall\, a, b, c \in A.$$

Un anello $(A, +, \cdot)$ *è detto* ***anello commutativo unitario*** *se valgono i due ulteriori assiomi:*

($\mathbf{A}_4$*)* $\cdot$ *è un'operazione commutativa, cioè:*

$$ab = ba, \quad \forall\, a, b \in A;$$

($\mathbf{A}_5$*)* $\cdot$ *ammette un elemento neutro [denotato* $1 = 1_A$*], cioè:*

$$a1 = 1a = a, \quad \forall\, a \in A.$$

Infine, un anello commutativo unitario $(A, +, \cdot)$ *è detto* ***campo*** *se l'operazione* $\cdot$ *ristretta ad* $A^* = A - \{0\}$ *ammette inverso, cioè vale l'ulteriore assioma:*

($\mathbf{A}_6$*)* $\forall\, a \in A^*$, $\exists\, a' \in A$ *tale che* $aa' = a'a = 1$.

[Ovviamente risulta: $(A, +, \cdot)$ *è un campo* $\iff$ $(A, +, \cdot)$ *è un anello e* $(A^*, \cdot)$ *è un gruppo commutativo].*

Ad esempio $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario (e non è un campo), mentre gli anelli $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono campi. Altri esempi di anelli commutativi unitari saranno esaminati nei successivi Esempi **5, 6**. Per esempi di anelli non commutativi rinviamo al capitolo successivo (anelli di matrici quadrate).

OSSERVAZIONE **5.** (i) Valgono per gli anelli definizioni analoghe a quelle già introdotte per i gruppi. Un *sottoanello* $(B, +, \cdot)$ di un anello $(A, +, \cdot)$ è un sottoinsieme non vuoto $B \subseteq A$ tale che $(B, +, \cdot)$ è un anello (con le stesse operazioni di A). Un *omomorfismo di anelli* $f : (A, +, \cdot) \to (A', +, \cdot)$ è un omomorfismo di gruppi additivi, verificante l'ulteriore condizione

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

[per semplificare le notazioni abbiamo indicato con lo stesso simbolo la moltiplicazione nei due anelli]. Infine *nucleo* e *immagine* di un omomorfismo di anelli sono definiti come per gli omomorfismi tra gruppi.

(*ii*) Sia $(A, +, \cdot)$ un anello arbitrario. Risulta:

$$a0 = 0, \quad \forall\, a \in A.$$

Infatti: $a0 = a(0+0) = a0 + a0$. Dunque $a0 + 0 = a0 + a0$ e pertanto [in base alla regola di cancellazione in $(A, +)$] risulta: $0 = a0$.

(*iii*) Sia $(A, +, \cdot)$ un campo. Risulta:

($\bullet$) *se* $ab = 0$, *allora* $a = 0$ *oppure* $b = 0$.

Infatti, se ad esempio assumiamo $a \neq 0$, allora

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

È lecito chiedersi se la proprietà ($\bullet$) vale, più generalmente, se $(A, +, \cdot)$ è un anello arbitrario. La risposta è negativa: infatti nell'esempio che segue costruiremo anelli che non verificano la condizione ($\bullet$) [detti *anelli non integri*].

Esempio **5.** (*Anelli delle classi resto modulo un intero*). Fissiamo un intero $n > 0$. Per ogni $a \in \mathbb{Z}$ consideriamo il seguente sottoinsieme di $\mathbb{Z}$:

$$\overline{a} = a + n\mathbb{Z} = \{a + kn,\ \forall\, k \in \mathbb{Z}\},$$

detto *classe resto di* a *modulo* n. Si osserva subito che risulta:

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ \ldots\ \cup \overline{n-1}$$

e che le classi resto $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sono a due a due disgiunte. Risulta inoltre, $\forall\, a, b \in \mathbb{Z}$:

$$\overline{a} = \overline{b} \iff a - b \text{ è multiplo di } n.$$

[Ad esempio: $\overline{0} = \overline{n} = \overline{-n} = \overline{2n} = \ldots$; $\overline{1} = \overline{n+1} = \overline{1-n} = \overline{2n+1} = \ldots$].

Poniamo ora:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

e su tale insieme introduciamo le due operazioni $+$ e $\cdot$ così definite:

$$+ : (\overline{a}, \overline{b}) \to \overline{a} + \overline{b} = \overline{a+b}, \quad \forall\, (\overline{a}, \overline{b}) \in \mathbb{Z}_n \times \mathbb{Z}_n;$$
$$\cdot : (\overline{a}, \overline{b}) \to \overline{a} \cdot \overline{b} = \overline{ab}, \quad \forall\, (\overline{a}, \overline{b}) \in \mathbb{Z}_n \times \mathbb{Z}_n.$$

Perché tali definizioni siano accettabili è necessario verificare preliminarmente che sono *ben definite* (cioè non dipendono dagli interi scelti per rappresentare le classi resto). Dunque sono necessarie le seguenti verifiche (che lasciamo al lettore):

$$\text{se } \overline{a} = \overline{a_1} \text{ e } \overline{b} = \overline{b_1}, \text{ allora } \overline{a+b} = \overline{a_1 + b_1} \text{ e } \overline{ab} = \overline{a_1 b_1}.$$

Risulta:

$$(\mathbb{Z}_n, +, \cdot) \text{ è un anello commutativo unitario.}$$

Per dimostrare tale affermazione invitiamo il lettore a verificare con pazienza tutti gli assiomi $(\mathbf{A}_1), \ldots, (\mathbf{A}_5)$. Ovviamente $\overline{0}$ ed $\overline{1}$ sono gli elementi neutri del-

la somma e del prodotto. A titolo di esempio verifichiamo una delle due proprietà distributive. Per ogni $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, si ha:

$$(\overline{a}+\overline{b})\overline{c} = \overline{a+b}\;\overline{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac}+\overline{bc} = \overline{a}\,\overline{c}+\overline{b}\,\overline{c}.$$

Illustriamo ora alcune semplici proprietà degli anelli $(\mathbb{Z}_n, +, \cdot)$. Posto ad esempio $n = 6$, risulta:

$$\overline{0} = \overline{6} = \overline{2}\cdot\overline{3}.$$

Dunque l'anello $(\mathbb{Z}_6, +, \cdot)$ possiede due elementi non nulli il cui prodotto è nullo e pertanto è un anello non integro [cfr. Oss. **5**(*iii*)]. È evidente che la stessa conclusione è vera per ogni anello $(\mathbb{Z}_n, +, \cdot)$, con n intero *non primo*. Cosa avviene invece se n è un numero primo ? In ogni testo di Algebra è dimostrato il seguente risultato:

$$(\mathbb{Z}_n, +, \cdot) \text{ } \textit{è un campo} \iff n \text{ } \textit{è un numero primo.}$$

Ne segue che (oltre ai campi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) esistono anche *campi finiti*, ad esempio $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \ldots$ (aventi rispett. $2, 3, 5, 7, \ldots$ elementi). Rileviamo inoltre esplicitamente che nel campo $\mathbb{Z}_2$ risulta: $\overline{2} = \overline{1}+\overline{1} = \overline{0}$.

Lasciamo infine al lettore il compito di scrivere le tavole [analoghe alla *'tavola pitagorica'*] delle due operazioni dell'anello $(\mathbb{Z}_n, +, \cdot)$ [per i primi valori di n, cfr. Eserc. **8**].

ESEMPIO **6.** (*Anelli di polinomi*). Denotiamo con $K = (K, +, \cdot)$ un campo. Sia x un'*indeterminata* (o *incognita*) su K. Un *polinomio* p *a coefficienti in* K *nell'indeterminata* x è, come ben noto, un'espressione della forma:

$$p = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

con $n \in \mathbb{N}$ e $a_0, a_1, \ldots, a_n \in K$. Si noti che p è somma di un numero finito di addendi del tipo $a_i x^i$, detti *monomi*; inoltre l'indeterminata x verifica le seguenti relazioni:

$$x^0 = 1, \quad 0x = 0, \quad x^n = x\,x^{n-1}, \ \forall\, n \geq 2.$$

L'insieme dei polinomi a coefficienti in K nell'indeterminata x verrà denotato con $K[x]$. Vogliamo assegnare a tale insieme una struttura algebrica.

Osserviamo che in $K[x]$ si ritrovano gli elementi di K (*polinomi costanti*) ed in particolare il *polinomio nullo* $p = 0$. Se $p = \sum_{i=0}^{n} a_i x^i$ è un polinomio non nullo, il più grande intero d tale che $a_d \neq 0$ è detto *grado* di p, denotato $deg(p)$; inoltre il coefficiente a_d è detto *coefficiente direttore* di p. I polinomi costanti non nulli hanno grado 0, mentre al polinomio nullo si attribuisce usualmente grado $-\infty$.

Introduciamo ora in $K[x]$ le operazioni di *somma* e *prodotto*. Siano:

$$p = \sum_{i=0}^{n} a_i x^i, \ q = \sum_{j=0}^{m} a_j x^j \in K[x].$$

Assumiamo, ad esempio, $n \leq m$. Poiché p può essere riscritto nella forma:

$$p = \sum_{i=0}^{n} a_i x^i + 0x^{n+1} + \ldots + 0x^m$$

[e dunque si può porre $a_{n+1} = \ldots = a_m = 0$], è lecito definire *polinomio somma* di p e q il polinomio

$$p + q = \sum_{j=0}^{m} \big(a_j + b_j\big) x^j \,.$$

Definiamo inoltre *polinomio prodotto* di p e q il polinomio

$$p\,q = \sum_{k=0}^{n+m} c_k x^k, \quad \text{con} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

[si tratta dell'usuale prodotto di polinomi, ben noto al lettore]. Lasciamo per esercizio la verifica del fatto che

$$(K[x], +, \cdot) \ \textit{è un anello commutativo unitario.}$$

[Ovviamente i polinomi 0, 1 sono gli elementi neutri di somma e prodotto].

Si noti che in $K[x]$ non esistono polinomi p, q non nulli il cui prodotto $p\,q$ è nullo [infatti, se $p, q \neq 0$, risulta: $deg(p\,q) = deg(p) + deg(q) \geq 0$ e quindi $p\,q \neq 0$]. Inoltre $(K[x], +, \cdot)$ non è un campo [infatti l'inverso di x non è un polinomio].

Concludiamo osservando che è possibile considerare anche polinomi a coefficienti in un anello A [non necessariamente un campo]. In tal caso $(A[x], +, \cdot)$ è ancora un anello. Ad esempio $K[x][y]$ è l'anello dei polinomi a coefficienti in $K[x]$ nell'indeterminata y. Tale anello è costituito dai polinomi in due indeterminate x, y a coefficienti in K, che possono essere scritti nella forma:

$$a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \ldots + a_{n0}x^n + \ldots + a_{0n}y^n \,.$$

Ovviamente $K[y][x] = K[x][y]$. Tale anello è usualmente denotato $K[x, y]$.

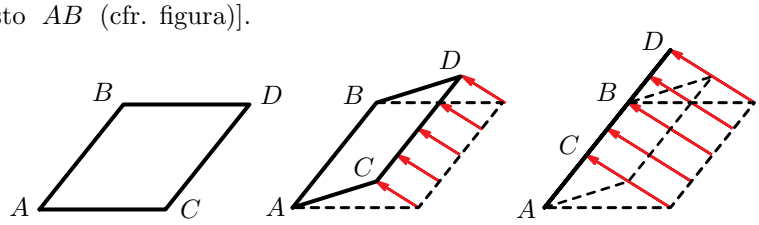
1.2 Spazi vettoriali: generalità.

Per introdurre e motivare la definizione di spazio vettoriale, descriviamo brevemente lo *spazio dei vettori liberi*.

Assumiamo intuitivamente noto il concetto di *spazio euclideo* (o *spazio fisico*) $\mathcal{E}$ *tridimensionale*. Fissati in $\mathcal{E}$ due punti A, B, la coppia $(A, B) \in \mathcal{E}\times\mathcal{E}$ è detta ***segmento orientato***. Tra i segmenti orientati introduciamo la seguente relazione $\sim$, detta ***relazione di equipollenza***:

$$(A, B) \sim (C, D) \iff A, B, D, C \ \textit{sono vertici consecutivi di un parallelogramma (eventualmente degenere).}$$

[*Nota*. Un parallelogramma è detto *degenere* se i suoi lati opposti sono allineati; un siffatto 'parallelogramma' può essere interpretato come posizione limite di un parallelogramma di vertici A, B, C, D, il cui lato CD venga traslato sulla retta del suo lato opposto AB (cfr. figura)].

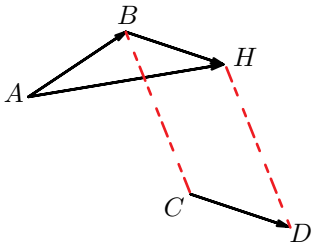


Lasciamo al lettore la verifica del fatto che la relazione di equipollenza è riflessiva, simmetrica e transitiva (cioè è una relazione di equivalenza sull'insieme $\mathcal{E}\times\mathcal{E}$ dei segmenti orientati). La classe di equivalenza del segmento orientato (A, B) è detta ***vettore*** (o ***vettore libero*** o ***vettore geometrico***) di $\mathcal{E}$ ed è denotata con $\overrightarrow{AB}$. Il vettore $\overrightarrow{AB}$ è rappresentato quindi dal segmento orientato (A, B) e da ogni altro segmento orientato (C, D) ad esso equipollente.

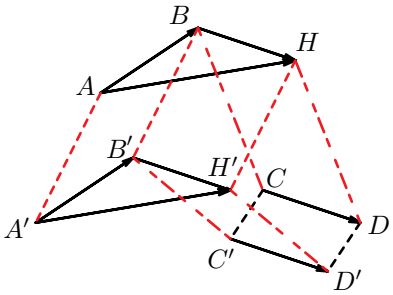
L'insieme $\mathcal{V}$ dei vettori di $\mathcal{E}$ è detto ***spazio dei vettori liberi***. Si noti che $\mathcal{V}$ è l'insieme quoziente [cfr. [**MZ**] pag. 39] di $\mathcal{E}\times\mathcal{E}$ modulo la relazione di equipollenza $\sim$, cioè:

$$\mathcal{V} = \mathcal{E}\times\mathcal{E}/_{\sim}.$$

Vogliamo ora definire su $\mathcal{V}$ una struttura di gruppo commutativo.



(fig. 1)



(fig. 2)

Definiamo la ***somma*** di due vettori $\overrightarrow{AB}$ e $\overrightarrow{CD}$, ponendo

$$\overrightarrow{AB} + \overrightarrow{CD} = \overrightarrow{AH}, \quad \text{se } \overrightarrow{CD} = \overrightarrow{BH}.$$

[si tratta della ben nota *regola del parallelogramma* (cfr. fig. 1)]. Affinché tale definizione sia accettabile, occorre dimostrare che non dipende dai rappresentanti dei vettori considerati. Dunque è necessario verificare che, se

$$\overrightarrow{AB} = \overrightarrow{A'B'}, \quad \overrightarrow{CD} = \overrightarrow{C'D'}, \quad \overrightarrow{CD} = \overrightarrow{BH} \quad \text{e} \quad \overrightarrow{C'D'} = \overrightarrow{B'H'},$$

allora $\overrightarrow{AH} = \overrightarrow{A'H'}$. Lasciamo al lettore la verifica di questo fatto (cfr. fig. 2).

Si può facilmente verificare che $(\mathcal{V}, +)$ è un gruppo commutativo. L'elemento neutro è il *vettore nullo* $\underline{0} = \overrightarrow{AA}$ $(\forall\, A \in \mathcal{E})$ e l'opposto del vettore $\underline{v} = \overrightarrow{AB}$ è il vettore $\overrightarrow{BA}$ (denotato $-\underline{v}$).

È certamente noto al lettore che è possibile anche *moltiplicare un vettore per un numero reale.* Se $\underline{v} = \overrightarrow{AB} \in \mathcal{V}$ e $c \in \mathbb{R}$, definiamo il vettore $c\underline{v}$ nel seguente modo:

(i) se $c > 0$, sulla semiretta $\mathbf{r}$ di origine A e contenente B esiste un unico punto Q tale che $\overline{AQ} = c\,\overline{AB}$ [$\overline{AB}$ e $\overline{AQ}$ denotano la lunghezza dei segmenti AB e AQ]. Poniamo quindi $c\underline{v} = c\,\overrightarrow{AB} = \overrightarrow{AQ}$.

(ii) se $c < 0$, sia Q' l'unico punto della semiretta $\mathbf{r}'$ opposta ad $\mathbf{r}$ tale che $|c|\,\overline{AB} = \overline{AQ'}$. Poniamo quindi $c\underline{v} = c\,\overrightarrow{AB} = \overrightarrow{AQ'}$.

(iii) se infine $c = 0$, poniamo $0\,\overrightarrow{AB} = \underline{0}$.

La moltiplicazione sopra definita, detta ***moltiplicazione per uno scalare***, associa ad un vettore $\underline{v}$ e ad un numero reale c (detto *scalare*) un nuovo vettore $c\underline{v}$. Dunque è un'applicazione del tipo:

$$\mathbb{R} \times \mathcal{V} \to \mathcal{V}.$$

[una siffatta applicazione è detta *operazione esterna su* $\mathcal{V}$]. Si può verificare [e la verifica, al solito, è lasciata al lettore] che la moltiplicazione per uno scalare verifica le seguenti quattro proprietà:

(a) $(c+d)\underline{v} = c\underline{v} + d\underline{v}, \quad \forall\, c, d \in \mathbb{R},\ \forall\, \underline{v} \in \mathcal{V}$;
(b) $c(\underline{v}_1 + \underline{v}_2) = c\underline{v}_1 + c\underline{v}_2, \quad \forall\, c \in \mathbb{R},\ \forall\, \underline{v}_1, \underline{v}_2 \in \mathcal{V}$;
(c) $(cd)\underline{v} = c(d\underline{v}), \quad \forall\, c, d \in \mathbb{R},\ \forall\, \underline{v} \in \mathcal{V}$;
(d) $1\underline{v} = \underline{v}, \quad \forall\, \underline{v} \in \mathcal{V}$.

Riassumendo quanto esposto sopra, lo spazio $\mathcal{V}$ dei vettori liberi è un gruppo commutativo, dotato di un'operazione esterna verificante le quattro proprietà sopra enunciate.

Poiché, come presto vedremo, molti altri insiemi hanno una simile struttura algebrica, è conveniente introdurre la definizione (astratta) di *spazio vettoriale* avendo come riferimento questo esempio.

DEFINIZIONE **7.** *Sia $K = (K, +, \cdot)$ un campo. Un insieme non vuoto V è detto* ***K-spazio vettoriale*** *se è dotato di un'operazione $+$ rispetto a cui $(V, +)$ è un gruppo commutativo e se è definita su V un'operazione esterna (detta moltiplicazione per uno scalare) $K \times V \to V$ tale che:*

(i) $(c+d)\underline{v} = c\underline{v} + d\underline{v}, \quad \forall\, c, d \in K,\ \forall\, \underline{v} \in V$;
(ii) $c(\underline{v}_1 + \underline{v}_2) = c\underline{v}_1 + c\underline{v}_2, \quad \forall\, c \in K,\ \forall\, \underline{v}_1, \underline{v}_2 \in V$;

(iii) $(cd)\underline{v} = c(d\underline{v}), \quad \forall\, c, d \in K,\ \forall\, \underline{v} \in V;$

(iv) $1\underline{v} = \underline{v}, \quad \forall\, \underline{v} \in V.$

*Gli elementi di V sono detti **vettori** e gli elementi di K **scalari**.*

ESEMPIO **7.** Descriviamo alcuni esempi di spazi vettoriali.

(i) L'insieme $\mathcal{V}$ dei vettori liberi è un $\mathbb{R}$-spazio vettoriale [è l'esempio da cui è stata desunta la definizione di spazio vettoriale!].

(ii) Sia K un campo. Nell'insieme $K[x]$ (cfr. Esempio **6**) consideriamo, oltre alla somma $+$, anche l'operazione esterna $K \times K[x] \to K[x]$ così definita:

$$(c, p) \to cp = \sum_{i=0}^{n} ca_i x^i, \quad \forall\, c \in K,\ \forall\, p = \sum_{i=0}^{n} a_i x^i \in K[x].$$

Si verifica facilmente che $K[x]$ è un K-spazio vettoriale.

(iii) Ogni campo $K = (K, +, \cdot)$ è anche un K-spazio vettoriale [basta interpretare la moltiplicazione come operazione esterna].

(iv) Sia K un campo e sia n un intero positivo. Sia K^n il prodotto cartesiano di n copie del campo K. Gli elementi di K^n (detti *n-ple*) sono insiemi ordinati costituiti da n elementi di K, del tipo:

$$\underline{a} = (a_1, a_2, \ldots, a_n).$$

Per ogni $\underline{a} = (a_1, a_2, \ldots, a_n)$, $\underline{b} = (b_1, b_2, \ldots, b_n) \in K^n$ e per ogni $c \in K$, definiamo le seguenti operazioni di somma e moltiplicazione per uno scalare:

$$\underline{a} + \underline{b} = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n), \quad c\underline{a} = (ca_1, ca_2, \ldots, ca_n).$$

Si verifica facilmente che, dotato di tali operazioni, K^n è un K-spazio vettoriale [in particolare l'elemento neutro della somma è la n-pla nulla $\underline{0} = (0, 0, \ldots, 0)$ e l'opposto della n-pla $\underline{a} = (a_1, a_2, \ldots, a_n)$ è la n-pla $-\underline{a} = (-a_1, -a_2, \ldots, -a_n)$].

Più generalmente, si noti che, se V è un K–spazio vettoriale, il prodotto cartesiano $(V)^n$ di n copie di V è ancora un K–spazio vettoriale, rispetto alle due seguenti operazioni:

$$(\underline{u}_1, \ldots, \underline{u}_n) + (\underline{v}_1, \ldots, \underline{v}_n) = (\underline{u}_1 + \underline{v}_1, \ldots, \underline{u}_n + \underline{v}_n); \quad c(\underline{v}_1, \ldots, \underline{v}_n) = (c\underline{v}_1, \ldots, c\underline{v}_n).$$

(v) Sia $\mathcal{F}_I$ l'insieme di tutte le funzioni reali definite su un sottoinsieme I della retta $\mathbb{R}$. Introduciamo in $\mathcal{F}_I$ le operazioni di somma e moltiplicazione per uno scalare, ponendo, $\forall\, f, g \in \mathcal{F}_I$, e $\forall\, c \in \mathbb{R}$:

$$(f + g)(x) = f(x) + g(x), \quad (cf)(x) = cf(x), \quad \forall\, x \in I.$$

Lasciamo al lettore la verifica che $\mathcal{F}_I$ è un $\mathbb{R}$-spazio vettoriale.

Analogamente, se denotiamo con Σ l'insieme di tutte le successioni di numeri reali, e poniamo, $\forall\, \{a_n\}, \{b_n\} \in \Sigma$, $\forall\, c \in \mathbb{R}$:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}, \quad c\{a_n\} = \{ca_n\},$$

si verifica facilmente che anche Σ è un $\mathbb{R}$-spazio vettoriale.

PROPOSIZIONE **1**. *Sia K un campo e sia V un K-spazio vettoriale. Risulta:*

(i) $0\underline{v} = \underline{0}, \quad \forall\, \underline{v} \in V$;
(ii) $(-c)\underline{v} = -(c\underline{v}), \quad \forall\, c \in K,\ \forall\, \underline{v} \in V$;
(iii) $c\underline{0} = \underline{0}, \quad \forall\, c \in K$;
(iv) se $c\underline{v} = \underline{0}$, *allora* $c = 0$ *oppure* $\underline{v} = \underline{0}$.

DIM. (*i*) Risulta: $\underline{v} + 0\underline{v} = 1\underline{v} + 0\underline{v} = (1+0)\underline{v} = 1\underline{v} = \underline{v} = \underline{v} + \underline{0}$. Dunque, applicando a $(V,+)$ la legge di cancellazione, $0\underline{v} = \underline{0}$.

(*ii*) Risulta: $c\underline{v} + (-c)\underline{v} = (c-c)\underline{v} = 0\underline{v} = \underline{0}$ e, analogamente, $(-c)\underline{v} + c\underline{v} = \underline{0}$. Ne segue che $(-c)\underline{v}$ è l'opposto di $c\underline{v}$, come richiesto.

(*iii*) Infatti, $\forall\, \underline{v} \in V$:

$$c\,\underline{0} = c(\underline{v} - \underline{v}) = c\underline{v} + c(-\underline{v}) = c\underline{v} + c[(-1)\underline{v}] = c\underline{v} + (-c)\underline{v} = c\underline{v} - c\underline{v} = \underline{0}.$$

(*iv*) Se $c \neq 0$, allora $c^{-1} \in K$ e quindi

$$\underline{v} = 1\underline{v} = (c^{-1}c)\underline{v} = c^{-1}(c\underline{v}) = c^{-1}\underline{0} = \underline{0}. \qquad \square$$

DEFINIZIONE **8.** *Sia V un K-spazio vettoriale e sia W un sottoinsieme non vuoto di V. W è detto* ***K-sottospazio vettoriale*** *di V se W è un K-spazio vettoriale [rispetto alle stesse operazioni di V].*

PROPOSIZIONE **2.** *Sia W un sottoinsieme non vuoto di un K-spazio vettoriale V. W è un K-sottospazio vettoriale di V $\iff$ sono verificate le due condizioni:*

(i) $\underline{w}_1 + \underline{w}_2 \in W, \quad \forall\, \underline{w}_1, \underline{w}_2 \in W$; *(ii)* $c\underline{w} \in W, \quad \forall\, c \in K,\ \forall\, \underline{w} \in W$.

DIM. ($\Longrightarrow$) è ovvio. ($\Longleftarrow$). Da (*ii*) segue, per ogni $\underline{w} \in W$:

$$\underline{0} = 0\underline{w} \in W \quad \text{e} \quad -\underline{w} = (-1)\underline{w} \in W.$$

Da (*i*) e da tali osservazioni segue che $(W,+)$ è un gruppo. Gli assiomi $(i), ..., (iv)$ di Def. **7** valgono in V e dunque anche in W. Pertanto W è un K-spazio vettoriale.

Nota. Si osserva subito che (*i*) e (*ii*) equivalgono all'unica condizione:

(*i'*) $c_1\underline{w}_1 + c_2\underline{w}_2 \in W, \quad \forall\, \underline{w}_1, \underline{w}_2 \in W,\ \forall\, c_1, c_2 \in K$. $\square$

ESEMPIO **8.** Descriviamo alcuni esempi di sottospazi vettoriali.

(*i*) Sia V un K-spazio vettoriale. $\{\underline{0}\}$ e V sono K-sottospazi vettoriali di V [detti sottospazi vettoriali ***banali***].

(*ii*) Sia V un K-spazio vettoriale. Fissato in V un vettore $\underline{v}_0$, l'insieme

$$\langle \underline{v}_0 \rangle = \{ c\underline{v}_0,\ \forall\, c \in K \}$$

è un K-sottospazio vettoriale di V [infatti, $\forall\, c\underline{v}_0,\, d\underline{v}_0 \in \langle \underline{v}_0 \rangle$ e $\forall\, a, b \in K$ si ha: $a(c\underline{v}_0) + b(d\underline{v}_0) = (ac + bd)\underline{v}_0 \in \langle \underline{v}_0 \rangle$]. Tale sottospazio vettoriale è detto ***sottospazio vettoriale generato da*** $\underline{v}_0$. Si noti che $\langle \underline{0} \rangle = \{\underline{0}\}$.

Più generalmente, fissati in V t vettori $\underline{v}_1, \ldots, \underline{v}_t$, l'insieme

$$\langle \underline{v}_1, \ldots, \underline{v}_t \rangle = \big\{ c_1\underline{v}_1 + \ldots + c_t\underline{v}_t,\ \forall\, c_1, \ldots, c_t \in K \big\}$$

è ancora un sottospazio vettoriale di V, detto ***sottospazio vettoriale generato da*** $\underline{v}_1, \ldots, \underline{v}_t$.

Ad esempio, sia $\mathcal{V}$ l' $\mathbb{R}$-spazio vettoriale dei vettori liberi. Se $\underline{v}_0 = \overrightarrow{AB}$ è un vettore non nullo di $\mathcal{V}$, indicata con $\mathbf{r}$ la retta per A, B, si verifica facilmente [cfr. Eserc. **12**(i)] che:

$$\langle \underline{v}_0 \rangle = \big\{ \overrightarrow{AP},\ \forall\, P \in \mathbf{r} \big\}.$$

Se si sceglie un altro rappresentante di $\underline{v}_0$, ad esempio $\underline{v}_0 = \overrightarrow{CD}$, la retta per C, D è parallela ad $\mathbf{r}$. Dunque il sottospazio vettoriale $\langle \underline{v}_0 \rangle$ [detto ***retta vettoriale***] non ha una 'posizione geometrica' ben individuata, ma può essere visualizzato in $\mathcal{E}$ come la totalità delle rette parallele ad una retta assegnata.

Siano ora $\underline{v}_1 = \overrightarrow{AB_1}$, $\underline{v}_2 = \overrightarrow{AB_2}$ due vettori di $\mathcal{V}$ tali che i tre punti A, B_1, B_2 non siano allineati. In tal caso esiste un unico piano $\mathbf{p}$ per i tre punti e si verifica [cfr. Eserc. **12**(i)] che:

$$\langle \underline{v}_1, \underline{v}_2 \rangle = \big\{ \overrightarrow{AQ},\ \forall\, Q \in \mathbf{p} \big\}.$$

Se $\underline{v}_1 = \overrightarrow{CD_1}$ e $\underline{v}_2 = \overrightarrow{CD_2}$, il piano per C, D_1, D_2 è parallelo a $\mathbf{p}$. Dunque il sottospazio vettoriale $\langle \underline{v}_1, \underline{v}_2 \rangle$ [detto ***piano vettoriale***] può essere visualizzato in $\mathcal{E}$ come la totalità dei piani paralleli ad un piano assegnato.

(iii) Se W_1, W_2 sono sottospazi vettoriali di V, si verifica subito che l'insieme intersezione $W_1 \cap W_2$ è un sottospazio vettoriale di V [detto ***sottospazio intersezione*** di W_1, W_2]. Infatti $\underline{0} \in W_1 \cap W_2$ [e dunque $W_1 \cap W_2$ è non vuoto]; inoltre, $\forall\, \underline{w}_1, \underline{w}_2 \in W_1 \cap W_2$, $\forall\, c_1, c_2 \in K$, risulta: $c_1\underline{w}_1 + c_2\underline{w}_2 \in W_1 \cap W_2$. [Più generalmente, anche l'intersezione di un numero arbitrario di sottospazi vettoriali di V è un sottospazio vettoriale di V].

Invece l'insieme unione $W_1 \cup W_2$ non è in generale un sottospazio vettoriale di V. Ad esempio, se in $\mathcal{V}$ scegliamo due vettori $\underline{v}_1 = \overrightarrow{AB_1}$, $\underline{v}_2 = \overrightarrow{AB_2}$ tali che i tre punti A, B_1, B_2 non siano allineati, allora $\underline{v}_1 + \underline{v}_2 \notin \langle \underline{v}_1 \rangle \cup \langle \underline{v}_2 \rangle$.

(iv) Se W_1, W_2 sono sottospazi vettoriali di V, l'insieme:

$$W_1 + W_2 = \big\{ \underline{w}_1 + \underline{w}_2,\ \forall\, \underline{w}_1 \in W_1, \forall\, \underline{w}_2 \in W_2 \big\}$$

è ancora un sottospazio vettoriale di V, detto ***sottospazio somma*** di W_1, W_2. Infatti $\underline{0} = \underline{0} + \underline{0} \in W_1 + W_2$ [e dunque $W_1 + W_2$ è non vuoto]; inoltre, $\forall\, c \in K$ e $\forall\, \underline{u}_1 + \underline{u}_2,\ \underline{v}_1 + \underline{v}_2 \in W_1 + W_2$, risulta:

$$(\underline{u}_1 + \underline{u}_2) + (\underline{v}_1 + \underline{v}_2) = (\underline{u}_1 + \underline{v}_1) + (\underline{u}_2 + \underline{v}_2) \in W_1 + W_2 \quad \text{e}$$

$$c(\underline{u}_1 + \underline{u}_2) = c\underline{u}_1 + c\underline{u}_2 \in W_1 + W_2.$$

Si noti che $W_1 + W_2 \supseteq W_1 \cup W_2$.

PROPOSIZIONE **3.** *Sia V un K-spazio vettoriale e siano W_1, W_2 due suoi sottospazi vettoriali. Le due seguenti condizioni sono equivalenti:*

(i) $W_1 \cap W_2 = \langle \underline{0} \rangle$;

(ii) $\forall\, \underline{w} \in W_1 + W_2,\ \exists!\, (\underline{w}_1, \underline{w}_2) \in W_1 \times W_2$ *tale che* $\underline{w} = \underline{w}_1 + \underline{w}_2$ *[cioè ogni vettore di $W_1 + W_2$ si scrive* **in modo unico** *come somma di un vettore di W_1 e di uno di W_2.]*

DIM. $(i) \Longrightarrow (ii)$. Supponiamo che un vettore $\underline{w} \in W_1 + W_2$ si scriva in due modi:

$$\underline{w} = \underline{u}_1 + \underline{u}_2 = \underline{v}_1 + \underline{v}_2, \quad \text{con } \underline{u}_1, \underline{v}_1 \in W_1 \text{ e } \underline{u}_2, \underline{v}_2 \in W_2.$$

Allora $\underline{u}_1 - \underline{v}_1 = \underline{v}_2 - \underline{u}_2 \in W_1 \cap W_2 = \langle \underline{0} \rangle$ e dunque $\underline{u}_1 = \underline{v}_1,\ \underline{u}_2 = \underline{v}_2$.

$(i) \Longleftarrow (ii)$. Per assurdo, sia $\underline{w}$ un vettore non nullo in $W_1 \cap W_2$. Si ha:

$$\underline{w} = \underline{0} + \underline{w} = \underline{w} + \underline{0} \in W_1 + W_2$$

e quindi $\underline{w}$ si scrive in due modi diversi come vettore di $W_1 + W_2$: assurdo. □

DEFINIZIONE **9.** *Siano W_1, W_2 due sottospazi vettoriali di un K-spazio vettoriale V. W_1 e W_2 sono detti* ***sottospazi supplementari*** *se risulta*

$$W_1 + W_2 = V \quad e \quad W_1 \cap W_2 = \langle \underline{0} \rangle.$$

Dalla Prop. **3** *segue subito che W_1, W_2 sono supplementari $\Longleftrightarrow$ ogni vettore di V si scrive in modo unico come somma di un vettore di W_1 e di uno di W_2.*

Se, più generalmente, W_1, W_2 sono sottospazi vettoriali tali che $W_1 \cap W_2 = \langle \underline{0} \rangle$, il sottospazio somma $W_1 + W_2$ è detto ***somma diretta*** *di W_1 e W_2 ed è denotato con $W_1 \oplus W_2$.*

1.3 Basi di uno spazio vettoriale.

DEFINIZIONE **10.** *Sia V un K-spazio vettoriale. Siano $\underline{v}_1, \ldots, \underline{v}_t \in V$ e siano $c_1, \ldots, c_t \in K$. Il vettore*

$$c_1\underline{v}_1 + c_2\underline{v}_2 + \ldots + c_t\underline{v}_t = \sum_{i=1}^{t} c_i\underline{v}_i$$

è detto ***combinazione lineare di*** $\underline{v}_1, \ldots, \underline{v}_t$ ***con coefficienti*** $c_1, \ldots, c_t$.

OSSERVAZIONE **6.** Presi comunque $\underline{v}_1, \ldots, \underline{v}_t \in V$, ovviamente risulta:

$$0\underline{v}_1 + 0\underline{v}_2 + \ ... \ + 0\underline{v}_t = \underline{0},$$

cioè il vettore nullo $\underline{0}$ è combinazione lineare dei vettori $\underline{v}_1, \ ..., \underline{v}_t$ (con coefficienti tutti nulli). La combinazione lineare $0\underline{v}_1 + \ ... \ + 0\underline{v}_t$ è detta *combinazione lineare banale* di $\underline{v}_1, \ ..., \underline{v}_t$.

Ci chiediamo se, dati t vettori $\underline{v}_1, \ ..., \underline{v}_t \in V$, il vettore nullo possa essere scritto anche come combinazione lineare *non banale* di $\underline{v}_1, \ ..., \underline{v}_t$ [o, più brevemente, se $\underline{v}_1, \ ..., \underline{v}_t$ *ammettono una combinazione lineare non banale di* $\underline{0}$]. Illustriamo tale questione con due esempi.

(a) Sia $\underline{v} \in V$ e sia $c \in K$. Considerati i due vettori $\underline{v}$, $c\underline{v}$, risulta:

$$\underline{0} = c\underline{v} + (-1)c\underline{v}$$

e dunque i vettori $\underline{v}$, $c\underline{v}$ ammettono una combinazione lineare non banale di $\underline{0}$ (con coefficienti c, -1).

(b) In $\mathbb{R}^2$ consideriamo i due vettori $\underline{v}_1 = (1,2)$, $\underline{v}_2 = (0,1)$. Poniamo

$$\underline{0} = c_1\underline{v}_1 + c_2\underline{v}_2$$

[cioè $(0,0) = c_1(1,2) + c_2(0,1) = (c_1, 2c_1 + c_2)$]. Ne segue:

$$c_1 = 0, \ 2c_1 + c_2 = 0 \ \text{ e pertanto } \ c_1 = c_2 = 0.$$

Dunque $\underline{v}_1$, $\underline{v}_2$ non ammettono alcuna combinazione lineare non banale di $\underline{0}$.

Gli esempi dell'osservazione precedente introducono la definizione che segue.

DEFINIZIONE **11.** *Sia V un K-spazio vettoriale e siano $\underline{v}_1, \ ..., \underline{v}_t \in V$. I vettori $\underline{v}_1, \ ..., \underline{v}_t$ sono detti* ***linearmente dipendenti*** *se ammettono una combinazione lineare non banale di $\underline{0}$, cioè se*

$$\exists\, c_1, \ ..., c_t \in K \ \text{ non tutti nulli, tali che } \ c_1\underline{v}_1 + \ ... \ + c_t\underline{v}_t = \underline{0}.$$

In caso contrario, $\underline{v}_1, \ ..., \underline{v}_t$ sono detti ***linearmente indipendenti****. In altri termini, $\underline{v}_1, \ ..., \underline{v}_t$ sono linearmente indipendenti se l'unica loro combinazione lineare di $\underline{0}$ è quella banale, cioè:*

$$c_1\underline{v}_1 + \ ... \ + c_t\underline{v}_t = \underline{0} \implies c_1 = \ ... \ = c_t = 0.$$

OSSERVAZIONE **7.** (i) Riesaminando gli esempi (a) e (b) di Oss. **6**, si verifica subito che i vettori $\underline{v}$, $c\underline{v}$ dell'esempio (a) sono linearmente dipendenti, mentre i vettori $\underline{v}_1$, $\underline{v}_2$ dell'esempio (b) sono linearmente indipendenti.

(ii) Se consideriamo un singolo vettore $\underline{v} \in V$, risulta:

$$\underline{v} \ \text{ è } \textit{linearmente dipendente} \iff \underline{v} = \underline{0}.$$

Infatti se $\underline{v}$ è linearmente dipendente, $\exists\, c \in K^* = K - \{0\}$ tale che $c\underline{v} = \underline{0}$. Ne segue che $\underline{v} = \underline{0}$ [cfr. Prop. **1**(iv)]. Viceversa, se $\underline{v} = \underline{0}$ si ha: $1\underline{v} = 1\,\underline{0} = \underline{0}$ e dunque $\underline{0}$ è linearmente dipendente.

(*iii*) Assegnati t vettori linearmente indipendenti, ogni loro sottoinsieme è formato da vettori ancora linearmente indipendenti.

Dimostriamo tale affermazione limitandoci (per semplificare le notazioni) a verificare che, per ogni intero s (con $0 < s < t$) risulta:

$\underline{v}_1, \ldots, \underline{v}_t$ *linearmente indipendenti* $\Longrightarrow$ $\underline{v}_1, \ldots, \underline{v}_s$ *linearmente indipendenti,*

ovvero, equivalentemente:

$\underline{v}_1, \ldots, \underline{v}_s$ *linearmente dipendenti* $\Longrightarrow$ $\underline{v}_1, \ldots, \underline{v}_t$ *linearmente dipendenti.*

Infatti, se $c_1\underline{v}_1 + \ldots + c_s\underline{v}_s = \underline{0}$, con $c_1, \ldots, c_s$ non tutti nulli, allora

$$c_1\underline{v}_1 + \ldots + c_s\underline{v}_s + 0\underline{v}_{s+1} + \ldots + 0\underline{v}_t = \underline{0},$$

e dunque $\underline{v}_1, \ldots, \underline{v}_t$ sono linearmente dipendenti.

PROPOSIZIONE **4.** *Siano* $\underline{v}_1, \ldots, \underline{v}_t \in V$ *(con* $t \geq 2$*). Risulta:*

$\underline{v}_1, \ldots, \underline{v}_t$ *sono linearmente dipendenti* $\Longleftrightarrow$ **almeno** *uno di essi è combinazione lineare dei rimanenti.*

DIM. ($\Longrightarrow$). Sia $c_1\underline{v}_1 + \ldots + c_t\underline{v}_t = \underline{0}$, con $c_1, \ldots, c_t$ non tutti nulli. Per semplificare le notazioni assumiamo $c_1 \neq 0$. Da $c_1\underline{v}_1 = -c_2\underline{v}_2 - \ldots - c_t\underline{v}_t$ segue:

$$\underline{v}_1 = -c_1^{-1}c_2\underline{v}_2 - \ldots - c_1^{-1}c_t\underline{v}_t$$

e quindi $\underline{v}_1$ è combinazione lineare di $\underline{v}_2, \ldots, \underline{v}_t$.

($\Longleftarrow$). Se ad esempio $\underline{v}_1$ è combinazione lineare di $\underline{v}_2, \ldots, \underline{v}_t$, allora (per opportuni $a_2, \ldots, a_t \in K$) $\underline{v}_1 = a_2\underline{v}_2 + \ldots + a_t\underline{v}_t$ e dunque

$$\underline{v}_1 - a_2\underline{v}_2 - \ldots - a_t\underline{v}_t = \underline{0},$$

cioè $\underline{v}_1, \ldots, \underline{v}_t$ sono linearmente dipendenti. □

PROPOSIZIONE **5.** *Siano* $\underline{v}_1, \ldots, \underline{v}_t \in V$*. Risulta:*

$\underline{v}_1, \ldots, \underline{v}_t$ *sono linearmente indipendenti* $\Longleftrightarrow$ *vale la seguente condizione:*

$$\textit{se } \sum_{i=1}^{t} c_i\underline{v}_i = \sum_{i=1}^{t} d_i\underline{v}_i, \quad \textit{allora } c_1 = d_1, \ldots, c_t = d_t.$$

DIM. ($\Longrightarrow$). Dall'ipotesi segue: $\sum_{i=1}^{t}(c_i - d_i)\underline{v}_i = \underline{0}$ e quindi, per definizione di indipendenza lineare, $c_1 - d_1 = \ldots = c_t - d_t = 0$.

($\Longleftarrow$). Sia $\sum_{i=1}^{t} a_i\underline{v}_i = \underline{0}$. Poiché $\underline{0} = \sum_{i=1}^{t} 0\underline{v}_i$, allora $\sum_{i=1}^{t} a_i\underline{v}_i = \sum_{i=1}^{t} 0\underline{v}_i$. Per ipotesi, $a_1 = 0, \ldots, a_t = 0$. Dunque $\underline{v}_1, \ldots, \underline{v}_t$ sono linearmente indipendenti. □

OSSERVAZIONE **8.** Vogliamo indicare il *significato geometrico* della dipendenza linea-

re di due o di tre vettori dell'$\mathbb{R}$-spazio vettoriale $\mathcal{V}$ dei vettori liberi.

Definiamo per i vettori di $\mathcal{V}$ i concetti di parallelismo e di complanarità. Due vettori $\underline{v}_1, \underline{v}_2 \in \mathcal{V}$ sono detti *paralleli* se [applicati in uno stesso punto A e posto $\underline{v}_1 = \overrightarrow{AB_1}$, $\underline{v}_2 = \overrightarrow{AB_2}$] i tre punti A, B_1, B_2 sono allineati. Analogamente, tre vettori $\underline{v}_1, \underline{v}_2, \underline{v}_3 \in \mathcal{V}$ sono detti *complanari* se [applicati in uno stesso punto A e posto $\underline{v}_i = \overrightarrow{AB_i}$ $(i = 1, 2, 3)$] i quattro punti A, B_1, B_2, B_3 sono complanari.

Invitiamo il lettore a dimostrare i due seguenti risultati (per i quali rinviamo all'Eserc. **13**):

(i) $\underline{v}_1, \underline{v}_2$ sono linearmente dipendenti $\iff$ sono paralleli;
(ii) $\underline{v}_1, \underline{v}_2, \underline{v}_3$ sono linearmente dipendenti $\iff$ sono complanari.

Introduciamo ora la definizione di *sistema di generatori* di uno spazio vettoriale. Ricordiamo [cfr. Esempio **8**(ii)] che, assegnati i vettori $\underline{v}_1, \dots, \underline{v}_t \in V$, il sottospazio generato da $\underline{v}_1, \dots, \underline{v}_t$ è

$$\langle \underline{v}_1, \dots, \underline{v}_t \rangle = \Big\{ \sum_{i=1}^{t} c_i \underline{v}_i, \ \forall\, c_i \in K \Big\},$$

cioè è l'insieme di tutte le combinazioni lineari di $\underline{v}_1, \dots, \underline{v}_t$. Si noti che $\langle \underline{v}_1, \dots, \underline{v}_t \rangle$ è *il più piccolo sottospazio vettoriale contenente* $\underline{v}_1, \dots, \underline{v}_t$ [infatti, se W è un sottospazio vettoriale contenente $\underline{v}_1, \dots, \underline{v}_t$, allora W contiene ogni loro combinazione lineare e quindi $W \supseteq \langle \underline{v}_1, \dots, \underline{v}_t \rangle$]. Inoltre $\langle \underline{v}_1, \dots, \underline{v}_t \rangle$ coincide anche con *l'intersezione di tutti i sottospazi vettoriali contenenti* $\underline{v}_1, \dots, \underline{v}_t$, cioè

$$\langle \underline{v}_1, \dots, \underline{v}_t \rangle = \bigcap_{W \ni \underline{v}_1, \dots \underline{v}_t} W.$$

[Infatti, poiché l'intersezione di sottospazi vettoriali è ancora un sottospazio vettoriale, allora $\bigcap W \supseteq \langle \underline{v}_1, \dots, \underline{v}_t \rangle$. Viceversa, poiché $\langle \underline{v}_1, \dots, \underline{v}_t \rangle$ è uno dei sottospazi W la cui intersezione è $\bigcap W$, allora $\langle \underline{v}_1, \dots, \underline{v}_t \rangle \supseteq \bigcap W$].

DEFINIZIONE **12.** *Sia V un K-spazio vettoriale e siano $\underline{v}_1, \dots, \underline{v}_t \in V$. Se risulta $\langle \underline{v}_1, \dots, \underline{v}_t \rangle = V$, diremo che $\{\underline{v}_1, \dots, \underline{v}_t\}$ è un* ***sistema di generatori di*** *V. Più generalmente, sia W un sottospazio vettoriale di V e siano $\underline{w}_1 \dots, \underline{w}_s \in W$. Se $\langle \underline{w}_1, \dots, \underline{w}_s \rangle = W$, diremo che $\{\underline{w}_1, \dots, \underline{w}_s\}$ è un* ***sistema di generatori di*** *W.*

OSSERVAZIONE **9.** È opportuno rilevare che *non* ogni spazio vettoriale ammette un sistema di generatori *finito* (cioè formato da un numero finito di vettori): ad esempio $K[x]$, $\mathcal{F}_I$ e Σ (cfr. Esempio **7**) non hanno sistemi di generatori finiti (cfr. Eserc. **15**). Conviene quindi estendere la definizione di sistema di generatori al caso di un numero infinito di vettori. Precisamente:

Sia V un K-spazio vettoriale e sia U un sottoinsieme di V. Diremo che U è un sistema di generatori di V se, $\forall \underline{v} \in V$, esiste un numero finito di vettori $\underline{u}_1, \ldots, \underline{u}_s \in U$ [dipendenti da $\underline{v}$] tali che $\underline{v} = c_1\underline{u}_1 + \ldots + c_s\underline{u}_s$.

Diremo infine che V è un K-spazio vettoriale *finitamente generato* se ammette un sistema di generatori finito.

Una *base* di uno spazio vettoriale altro non è che un sistema di generatori formato da vettori linearmente indipendenti. Formalizziamo questa definizione.

DEFINIZIONE **13.** *Sia V un K-spazio vettoriale e siano $\underline{v}_1, \ldots, \underline{v}_n \in V$. Diremo che $\{\underline{v}_1, \ldots, \underline{v}_n\}$ è una **base** di V se:*

(i) $\underline{v}_1, \ldots, \underline{v}_n$ sono linearmente indipendenti;

(ii) $\langle \underline{v}_1, \ldots, \underline{v}_n \rangle = V$.

OSSERVAZIONE **10.** Tenuto conto dell'Oss. **9**, rileviamo subito che *non* ogni spazio vettoriale ammette una base *finita* (cioè formata da un numero finito di vettori): ad esempio $K[x]$ non ha basi finite. È opportuno allora generalizzare la precedente definizione di base al caso di un numero infinito di vettori. A tale scopo è sufficiente estendere il concetto di indipendenza lineare ad un insieme arbitrario U di vettori di V. Precisamente:

Sia U un sottoinsieme di V. U è un insieme di vettori linearmente indipendenti di V se ogni sottoinsieme finito di U è formato da vettori linearmente indipendenti (nel senso di Def. **11***).*

Ovviamente U è una base di V se U è un sistema di generatori di V ed è un insieme di vettori linearmente indipendenti.

Quasi sempre nel seguito assumeremo che uno spazio vettoriale V ammetta una base finita. In tal caso è possibile associare ad ogni vettore *le sue coordinate* (rispetto alla base scelta). Per definire tali coordinate è necessario premettere la seguente proposizione.

PROPOSIZIONE **6.** *Sia V un K-spazio vettoriale e siano $\underline{v}_1, \ldots, \underline{v}_n \in V$. Le seguenti condizioni sono equivalenti:*

(i) $\{\underline{v}_1, \ldots, \underline{v}_n\}$ è una base di V;

(ii) ogni vettore $\underline{v} \in V$ si scrive **in modo unico** *come combinazione lineare dei vettori $\underline{v}_1, \ldots, \underline{v}_n$ [cioè $\exists!\, (c_1, \ldots, c_n) \in K^n$ tale che $\underline{v} = \sum_{i=1}^{n} c_i \underline{v}_i$].*

DIM. $(i) \Longrightarrow (ii)$. Poiché $\{\underline{v}_1, \ldots, \underline{v}_n\}$ è un sistema di generatori di V, risulta: $\underline{v} = \sum_{i=1}^{n} c_i \underline{v}_i$ (per opportuni $c_1, \ldots, c_n \in K$). Poiché $\underline{v}_1, \ldots, \underline{v}_n$ sono linearmente indipendenti, dalla Prop. **5** segue che tale combinazione lineare è unica.

$(ii) \Longrightarrow (i)$. Per ipotesi, ogni vettore $\underline{v} \in V$ può essere scritto nella forma: $\underline{v} = \sum_{i=1}^{n} c_i \underline{v}_i$. Dunque $\{\underline{v}_1, \ldots, \underline{v}_n\}$ è un sistema di generatori di V. Se poi $\sum_{i=1}^{n} c_i \underline{v}_i = \underline{0}$, allora $\sum_{i=1}^{n} c_i \underline{v}_i = \sum_{i=1}^{n} 0\, \underline{v}_i$ e dunque, per ipotesi, $c_1 = \ldots = c_n = 0$. Dunque i vettori $\underline{v}_1, \ldots, \underline{v}_n$ sono linearmente indipendenti. □

In altri termini, la proposizione ora dimostrata afferma che esiste un'applicazione biunivoca $V \to K^n$, così definita:

$$\underline{v} \to (c_1, \ldots, c_n), \quad \forall\, \underline{v} = \sum_{i=1}^{n} c_i \underline{v}_i \in V.$$

Tale biiezione, che ovviamente dipende dalla scelta della base $\{\underline{v}_1, \ldots, \underline{v}_n\}$ di V, permette di associare ad un vettore una n-pla. Precisiamo tale fatto nella definizione che segue.

DEFINIZIONE **14.** *Sia V un K-spazio vettoriale e sia $\{\underline{v}_1, \ldots, \underline{v}_n\}$ una sua base. Per ogni $\underline{v} = \sum_{i=1}^{n} c_i \underline{v}_i \in V$, la n-pla $(c_1, \ldots, c_n) \in K^n$ è detta* ***n-pla delle coordinate di $\underline{v}$ rispetto alla base*** *$\{\underline{v}_1, \ldots, \underline{v}_n\}$.*

OSSERVAZIONE **11.** In K^n consideriamo gli n vettori:

$$\underline{e}_1 = (1, 0, 0, \ldots, 0, 0),\ \underline{e}_2 = (0, 1, 0, \ldots, 0, 0),\ \ldots,\ \underline{e}_n = (0, 0, 0, \ldots, 0, 1).$$

Risulta:

(i) $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ è un sistema di generatori di K^n. Infatti, $\forall\, \underline{a} = (a_1, \ldots, a_n) \in K^n$, risulta:

$$\underline{a} = a_1 \underline{e}_1 + a_2 \underline{e}_2 + \ldots + a_n \underline{e}_n.$$

(ii) i vettori $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n$ sono linearmente indipendenti. Infatti, se $\sum_{i=1}^{n} c_i \underline{e}_i = \underline{0}$, allora:

$$(0, 0, \ldots, 0) = c_1(1, 0, \ldots, 0) + \ldots + c_n(0, 0, \ldots, 1) = (c_1, \ldots, c_n)$$

e dunque $c_1 = \ldots = c_n = 0$.

Si conclude quindi che $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ è una base di K^n. Si noti che le coordinate della n-pla $\underline{a} = (a_1, \ldots, a_n)$ (rispetto a tale base) sono esattamente le n componenti $a_1, \ldots, a_n$ di $\underline{a}$. Tale fatto [che ovviamente non sussiste per le altre ba-

si di K^n] rende la base $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ di K^n più 'semplice' e più 'naturale' delle altre basi. Per questo motivo tale base viene chiamata *base canonica* (o *base standard*) di K^n.

1.4 Alcuni risultati sugli spazi vettoriali.

Dimostreremo in questo conclusivo paragrafo quattro importanti teoremi relativi agli spazi vettoriali (aventi una base finita). Ne anticipiamo sommariamente il contenuto:

(*i*) ogni base ha lo stesso numero di vettori (*Teorema della dimensione*).

(*ii*) è possibile aggiungere ad un insieme di vettori linearmente indipendenti altri vettori in modo da ottenere una base (*Teorema del completamento*).

(*iii*) è possibile, viceversa, estrarre, da ogni sistema di generatori, una base.

(*iv*) le dimensioni di due sottospazi vettoriali sono legate da una precisa formula alla dimensione del sottospazio somma e del sottospazio intersezione (*Formula di Grassmann*).

Accanto a questi teoremi dimostreremo alcuni corollari, che saranno molto spesso utilizzati nei successivi capitoli.

TEOREMA **1.** (Teorema della dimensione). *Sia V un K-spazio vettoriale e sia $\{\underline{v}_1, \ldots, \underline{v}_n\}$ una sua base. Ogni altra base di V ha ancora n vettori.*

La dimostrazione del teorema è una semplice conseguenza del seguente lemma.

LEMMA **1.** *Sia $\{\underline{v}_1, \ldots, \underline{v}_n\}$ un sistema di generatori di V. Siano $\underline{w}_1, \ldots, \underline{w}_m$ m vettori di V, con $m > n$. Tali vettori sono linearmente dipendenti.*

DIM. [Lemma **1**]. Consideriamo i primi n vettori $\underline{w}_1, \ldots, \underline{w}_n$. Se tali vettori fossero linearmente indipendenti, allora [in base a Oss. **7**(*iii*)] anche $\underline{w}_1, \ldots, \underline{w}_m$ sarebbero linearmente dipendenti (e dunque la tesi del lemma sarebbe già verificata). *Assumeremo quindi che $\underline{w}_1, \ldots, \underline{w}_n$ siano linearmente indipendenti.*

Per provare il lemma basterà dimostrare che:

$$(\star) \qquad \langle \underline{w}_1, \ldots, \underline{w}_n \rangle = V.$$

[Infatti, se $(\star)$ è dimostrato, il vettore $\underline{w}_{n+1}$ è combinazione lineare di $\underline{w}_1, \ldots, \underline{w}_n$ e dunque $\underline{w}_1, \ldots, \underline{w}_n, \underline{w}_{n+1}$ sono linearmente dipendenti. Ma allora anche $\underline{w}_1, \ldots, \underline{w}_m$ sono linearmente dipendenti]. Dimostriamo quindi $(\star)$.

Consideriamo il vettore $\underline{w}_1$. Certamente $\underline{w}_1 \neq \underline{0}$ [altrimenti $\underline{0}, \underline{w}_2, \ldots, \underline{w}_n$ sarebbero linearmente dipendenti]. Poiché, per ipotesi, $V = \langle \underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n \rangle$, allora

$$\underline{w}_1 = a_1 \underline{v}_1 + \ldots + a_n \underline{v}_n.$$

I coefficienti $a_1, \dots, a_n$ non sono tutti nulli [in quanto $\underline{w}_1 \neq \underline{0}$] ed assumiamo, per semplificare le notazioni, che sia $a_1 \neq 0$. Si ha allora:

$$\underline{v}_1 = \tfrac{1}{a_1}\,\underline{w}_1 - \tfrac{a_2}{a_1}\,\underline{v}_2 - \dots - \tfrac{a_n}{a_1}\,\underline{v}_n$$

e dunque $\underline{v}_1 \in \langle \underline{w}_1, \underline{v}_2, \dots, \underline{v}_n \rangle$. Poiché $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n \in \langle \underline{w}_1, \underline{v}_2, \dots, \underline{v}_n \rangle$, allora:

$$\langle \underline{v}_1, \underline{v}_2, \dots, \underline{v}_n \rangle \subseteq \langle \underline{w}_1, \underline{v}_2, \dots, \underline{v}_n \rangle;$$

ma, poiché $\langle \underline{v}_1, \underline{v}_2, \dots, \underline{v}_n \rangle = V$, allora:

$$\langle \underline{w}_1, \underline{v}_2, \dots, \underline{v}_n \rangle = V.$$

Se $n = 1$, l'affermazione $(\star)$ è dimostrata. Supponiamo quindi $n \geq 2$ e consideriamo il vettore $\underline{w}_2$. Ovviamente $\underline{w}_2 \in \langle \underline{w}_1, \underline{v}_2, \dots, \underline{v}_n \rangle$ e quindi

$$\underline{w}_2 = b_1\underline{w}_1 + b_2\underline{v}_2 + \dots + b_n\underline{v}_n.$$

I coefficienti $b_2, \dots, b_n$ non sono tutti nulli [altrimenti si avrebbe che $\underline{w}_2 = b_1\underline{w}_1$ e dunque $\underline{w}_1, \dots, \underline{w}_n$ sarebbero linearmente dipendenti]. Possiamo supporre [eventualmente riordinando i vettori $\underline{v}_2, \dots, \underline{v}_n$] che sia $b_2 \neq 0$. Allora:

$$\underline{v}_2 = \tfrac{1}{b_2}\,\underline{w}_2 - \tfrac{b_1}{b_2}\,\underline{w}_1 - \tfrac{b_3}{b_2}\,\underline{v}_3 - \dots - \tfrac{b_n}{b_2}\,\underline{v}_n$$

e dunque $\underline{v}_2 \in \langle \underline{w}_2, \underline{w}_1, \underline{v}_3, \dots, \underline{v}_n \rangle$. Poiché $\underline{v}_2, \underline{w}_1, \underline{v}_3, \dots, \underline{v}_n \in \langle \underline{w}_2, \underline{w}_1, \underline{v}_3, \dots, \underline{v}_n \rangle$, allora:

$$V = \langle \underline{v}_2, \underline{w}_1, \underline{v}_3, \dots, \underline{v}_n \rangle \subseteq \langle \underline{w}_2, \underline{w}_1, \underline{v}_3, \dots, \underline{v}_n \rangle$$

e dunque

$$\langle \underline{w}_2, \underline{w}_1, \underline{v}_3, \dots, \underline{v}_n \rangle = V.$$

Ripetendo tale procedimento si otterrà successivamente:

$$V = \langle \underline{w}_3, \underline{w}_2, \underline{w}_1, \underline{v}_4, \dots, \underline{v}_n \rangle = \dots = \langle \underline{w}_n, \underline{w}_{n-1}, \dots, \underline{w}_1 \rangle,$$

cioè la formula $(\star)$. □

Possiamo ora dimostrare il Teor. **1**.

DIM. [Teorema **1**]. Sia $\{\underline{w}_1, \dots, \underline{w}_m\}$ un'altra base di V. Dobbiamo dimostrare che $n = m$.

Osserviamo che $\{\underline{v}_1, \dots, \underline{v}_n\}$ e $\{\underline{w}_1, \dots, \underline{w}_m\}$ sono sistemi di generatori di V. In base al Lemma **1**, se fosse $n > m$, i vettori $\underline{v}_1, \dots, \underline{v}_n$ sarebbero linearmente dipendenti [e ciò è assurdo]. Se invece fosse $m > n$, i vettori $\underline{w}_1, \dots, \underline{w}_m$ sarebbero linearmente dipendenti [e anche questo è assurdo]. Dunque $n = m$. □

DEFINIZIONE **15.** *Sia V un K-spazio vettoriale che ammette una base finita. Il numero di vettori di tale base [e quindi di ogni altra base di V] è detto* ***dimensione*** *di V e sarà denotato $dim_K(V)$ oppure $dim(V)$ o anche $dim\, V$.*

ESEMPIO **9.** Indichiamo la dimensione di alcuni spazi vettoriali.

(*i*) $dim_K(K^n) = n$. Infatti $\{\underline{e}_1, \dots, \underline{e}_n\}$ è una base di K^n (cfr. Oss. **11**).

(*ii*) $dim_{\mathbb{R}}(\mathcal{V}) = 3$. Infatti tre vettori non complanari formano una base di $\mathcal{V}$ (cfr. Eserc. **14**).

(*iii*) Il K-spazio vettoriale nullo $\{\underline{0}\}$ non ha basi [infatti $\underline{0}$, il suo unico vettore, è linearmente dipendente]. Si conviene di porre $dim\,\{\underline{0}\} = 0$.

(*iv*) Se $V = \langle \underline{v} \rangle$, con $\underline{v} \neq \underline{0}$, $dim\,\langle \underline{v} \rangle = 1$ [infatti $\langle \underline{v} \rangle$ ha base $\{\underline{v}\}$].

(*v*) $dim_K(K[x]) = +\infty$. Infatti $K[x]$ ha basi infinite (cfr. Eserc. **15**).

Il seguente corollario del Lemma **1** ci fornisce un utile 'sconto' per verificare se un insieme di n vettori (in uno spazio vetttoriale di dimensione n) è una base.

COROLLARIO **1.** *Sia* $dim_K(V) = n$. *Risulta:*

(i) n *vettori linearmente indipendenti formano una base.*

(ii) un sistema di generatori di V *formato da* n *vettori è una base.*

DIM. Sia $\{\underline{v}_1, \dots, \underline{v}_n\}$ una base di V.

(*i*) Siano $\underline{w}_1, \dots, \underline{w}_n$ n vettori linearmente indipendenti. Vogliamo dimostrare che sono anche un sistema di generatori di V, cioè che $\langle \underline{w}_1, \dots, \underline{w}_n \rangle = V$.

Per ogni $\underline{v} \in V$, consideriamo gli $n+1$ vettori $\underline{v}, \underline{w}_1, \dots, \underline{w}_n$. Tali vettori sono linearmente dipendenti (in base al Lemma **1**) e dunque ammettono una combinazione lineare non banale di $\underline{0}$, ad esempio:

$$a\underline{v} + b_1\underline{w}_1 + \dots + b_n\underline{w}_n = \underline{0}.$$

Si ha: $a \neq 0$ [altrimenti $b_1, \dots, b_n$ non sarebbero tutti nulli e quindi $\underline{w}_1, \dots, \underline{w}_n$ sarebbero linearmente dipendenti, contro l'ipotesi]. Pertanto:

$$\underline{v} = -\tfrac{b_1}{a}\,\underline{w}_1 - \dots - \tfrac{b_n}{a}\,\underline{w}_n,$$

cioè $\underline{v} \in \langle \underline{w}_1, \dots, \underline{w}_n \rangle$. Ciò dimostra che $\langle \underline{w}_1, \dots, \underline{w}_n \rangle = V$.

(*ii*) Sia ora $\langle \underline{w}_1, \dots, \underline{w}_n \rangle = V$. Dobbiamo verificare che i vettori $\underline{w}_1, \dots, \underline{w}_n$ sono linearmente indipendenti. Per assurdo, ciò non sia vero: dunque almeno uno di essi [e supponiamo che sia $\underline{w}_1$] è combinazione lineare degli altri, cioè:

$$\underline{w}_1 = c_2\underline{w}_2 + \dots + c_n\underline{w}_n.$$

Allora $\langle \underline{w}_1, \dots, \underline{w}_n \rangle = \langle \underline{w}_2, \dots, \underline{w}_n \rangle$ e quindi $\{\underline{w}_2, \dots, \underline{w}_n\}$ è un sistema di generatori di V. In base al Lemma **1**, i vettori $\underline{v}_1, \dots, \underline{v}_n$ sarebbero linearmente dipendenti: assurdo. □

COROLLARIO **2.** *Sia* $dim_K(V) = n$ *e siano* W, W_1, W_2 *tre sottospazi vettoriali di* V. *Risulta:*

(i) $dim_K(W) \leq dim_K(V)$. *Inoltre* $dim_K(W)$ *è il massimo numero di vettori linearmente indipendenti contenuti in* W.

(ii) Se $W_1 \subseteq W_2$, *allora* $dim_K(W_1) \leq dim_K(W_2)$. *Inoltre:*

$$dim_K(W_1) = dim_K(W_2) \iff W_1 = W_2.$$

DIM. (i) Osserviamo preliminarmente che vettori linearmente indipendenti in W lo sono anche in V.

Denotiamo con m il massimo numero possibile di vettori linearmente indipendenti in W. Poiché $dim_K(V) = n$, $n+1$ vettori di V sono sempre linearmente dipendenti (in base al Lemma **1**). Dunque $m \leq n$.

Scegliamo ora in W m vettori linearmente indipendenti $\underline{w}_1, \ldots, \underline{w}_m$. Vogliamo dimostrare che $\langle \underline{w}_1, \ldots, \underline{w}_m \rangle = W$ [e da ciò segue che $dim_K(W) = m$ e quindi (i) è dimostrato]. Scelto arbitrariamente $\underline{w} \in W$, i vettori $\underline{w}, \underline{w}_1, \ldots, \underline{w}_m$ sono linearmente dipendenti [perché sono $m+1$] e dunque $\exists\, a, b_1, \ldots, b_m \in K$ non tutti nulli, tali che:

$$a\underline{w} + b_1\underline{w}_1 + \ldots + b_m\underline{w}_m = \underline{0}.$$

Si ha: $a \neq 0$ [altrimenti $\underline{w}_1, \ldots, \underline{w}_m$ sarebbero linearmente dipendenti]. Ne segue che $\underline{w} \in \langle \underline{w}_1, \ldots, \underline{w}_m \rangle$. Dunque $\langle \underline{w}_1, \ldots, \underline{w}_m \rangle = W$.

(ii) Poiché W_1 è un sottospazio vettoriale di W_2, da (i) segue che $dim_K(W_1) \leq dim_K(W_2)$. È evidente che se $W_1 = W_2$, allora $dim_K(W_1) = dim_K(W_2)$. Viceversa, assumiamo che:

$$W_1 \subseteq W_2 \quad \text{e} \quad dim_K(W_1) = dim_K(W_2).$$

Poniamo $t = dim_K(W_1)$ e scegliamo una base $\{\underline{w}_1, \ldots, \underline{w}_t\}$ di W_1. I vettori $\underline{w}_1, \ldots, \underline{w}_t$ sono linearmente indipendenti in W_1 e quindi anche in W_2. In base al Cor. **1**(i), $\{\underline{w}_1, \ldots, \underline{w}_t\}$ è una base di W_2. Dunque $W_2 = \langle \underline{w}_1, \ldots, \underline{w}_t \rangle = W_1$, cioè $W_2 = W_1$. □

OSSERVAZIONE **12.** (i) Sia $dim_K(V) = n$. Dal Cor. **2**(ii) segue che V ha un unico sottospazio vettoriale di dimensione n, cioè V stesso. Inoltre ogni sottospazio vettoriale W non nullo ha dimensione ≥ 1 [infatti, se $W \ni \underline{v} \neq \underline{0}$, allora $dim_K(V) \geq dim \langle \underline{v} \rangle = 1$]. Ne segue in particolare che V possiede un unico sottospazio vettoriale di dimensione 0, cioè $\{\underline{0}\}$.

(ii) Esaminiamo gli $\mathbb{R}$-sottospazi vettoriali di $\mathcal{V}$. Sappiamo che $\mathcal{V}$ ha i seguenti sottospazi vettoriali:

$\mathcal{V}$ [unico sottospazio vettoriale di dimensione 3]; $\{\underline{0}\}$ [unico sottospazio vettoriale di dimensione 0]; infinite rette vettoriali $\langle \overrightarrow{AB} \rangle$, $\forall\, A, B \in \mathcal{E}$, $A \neq B$ [sottospazi vettoriali di dimensione 1]; infiniti piani vettoriali $\langle \overrightarrow{AB}, \overrightarrow{AC} \rangle$, $\forall\, A, B, C \in \mathcal{E}$ punti non allineati [sottospazi vettoriali di dimensione 2].

Dal Cor. **2**(ii) segue che $\mathcal{V}$ non ha altri tipi di sottospazi vettoriali. Se infatti, per assurdo, $\mathcal{V}$ ammettesse ad esempio un sottospazio vettoriale W tale che

$$\langle \underline{0} \rangle \subset \langle \underline{u}_1 \rangle \subset W \subset \langle \underline{u}_1, \underline{u}_2 \rangle,$$

allora $1 < dim_{\mathbb{R}}(W) < 2$: assurdo.

TEOREMA **2.** (Teorema del completamento). *Sia* $dim_K(V) = n$ *e siano* $\underline{w}_1, \ldots, \underline{w}_t \in V$ t *vettori linearmente indipendenti, con* $t < n$. *Esistono* $n - t$ *vettori* $\underline{w}_{t+1}, \ldots, \underline{w}_n \in V$ *tali che* $\{\underline{w}_1, \ldots, \underline{w}_n\}$ *è una base di* V.

[Dunque un insieme di vettori linearmente indipendenti può essere 'completato' sino ad ottenere una base].

DIM. $\{\underline{w}_1, \ldots, \underline{w}_t\}$ non è un sistema di generatori di V [altrimenti sarebbe una base di V e dunque, in base al Teor. **1**, $t = n$]. Dunque $V \supset \langle \underline{w}_1, \ldots, \underline{w}_t \rangle$.

Possiamo quindi scegliere un vettore $\underline{w}_{t+1} \in V - \langle \underline{w}_1, \ldots, \underline{w}_t \rangle$. Verifichiamo che i vettori $\underline{w}_1, \ldots, \underline{w}_t, \underline{w}_{t+1}$ sono linearmente indipendenti. Poniamo:

$$c_1 \underline{w}_1 + \ldots + c_t \underline{w}_t + c_{t+1} \underline{w}_{t+1} = \underline{0}.$$

Se fosse $c_{t+1} \neq 0$, allora $\underline{w}_{t+1} \in \langle \underline{w}_1, \ldots, \underline{w}_t \rangle$, contro l'ipotesi fatta sopra. Dunque $c_{t+1} = 0$; ma allora $c_1 \underline{w}_1 + \ldots + c_t \underline{w}_t = \underline{0}$ e, poiché i vettori $\underline{w}_1, \ldots, \underline{w}_t$ sono linearmente indipendenti, $c_1 = \ldots = c_t = 0$. Ne segue che $\underline{w}_1, \ldots, \underline{w}_t, \underline{w}_{t+1}$ sono linearmente indipendenti.

Se $n = t+1$, il teorema è dimostrato. Se $n > t+1$, allora $\langle \underline{w}_1, \ldots, \underline{w}_t, \underline{w}_{t+1} \rangle \subset V$ e quindi possiamo scegliere un vettore $\underline{w}_{t+2} \in V - \langle \underline{w}_1, \ldots, \underline{w}_t, \underline{w}_{t+1} \rangle$ per poi dimostrare (come fatto sopra) che i vettori $\underline{w}_1, \ldots, \underline{w}_t, \underline{w}_{t+1}, \underline{w}_{t+2}$ sono linearmente indipendenti. Dopo un numero finito di passi si ottengono n vettori linearmente indipendenti $\underline{w}_1, \ldots, \underline{w}_n$. Tali vettori formano una base di V (in base al Cor. **1**). □

TEOREMA **3.** *Sia* $dim_K(V) = n$ *e sia* $\{\underline{v}_1, \ldots, \underline{v}_m\}$ *un sistema di generatori di* V *[si noti che in ogni caso* $m \geq n$, *in base al Lemma* **1***]. Esistono* n *vettori*

$$\underline{v}_{i_1}, \ldots, \underline{v}_{i_n} \in \{\underline{v}_1, \ldots, \underline{v}_m\}$$

formanti una base di V.

[Dunque da un sistema di generatori si può 'estrarre' una base].

DIM. Possiamo assumere che i vettori $\underline{v}_1, \ldots, \underline{v}_m$ siano tutti non nulli [infatti eventuali vettori nulli tra $\underline{v}_1, \ldots, \underline{v}_m$ possono essere eliminati, ed i restanti vettori sono ancora un sistema di generatori di V]. Consideriamo dunque il vettore (non nullo) $\underline{v}_1$ e poniamo $\underline{v}_{i_1} = \underline{v}_1$. Esaminiamo ora i successivi vettori $\underline{v}_2, \ldots, \underline{v}_m$ (nell'ordine assegnato). Indichiamo con $\underline{v}_{i_2}$ il primo tra questi vettori tale che

$$\langle \underline{v}_1 \rangle \subset \langle \underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{i_2} \rangle.$$

[Pertanto $\langle \underline{v}_1 \rangle = \langle \underline{v}_1, \underline{v}_2 \rangle = \ldots = \langle \underline{v}_1, \ldots, \underline{v}_{i_2-1} \rangle \subset \langle \underline{v}_1, \ldots, \underline{v}_{i_2} \rangle = \langle \underline{v}_1, \underline{v}_{i_2} \rangle$]. Si noti che un siffatto vettore $\underline{v}_{i_2}$ può non esistere: in tal caso

$$\langle \underline{v}_1 \rangle = \langle \underline{v}_1, \underline{v}_2, \ldots, \underline{v}_m \rangle = V,$$

e quindi $\{\underline{v}_1\}$ è una base di V *estratta* da $\{\underline{v}_1, \ldots, \underline{v}_m\}$, come richiesto. Se invece $\underline{v}_{i_2}$ esiste, indicheremo con $\underline{v}_{i_3}$ il primo (eventuale) vettore tra $\underline{v}_{i_2+1}, \ldots, \underline{v}_m$ tale che

$$\langle \underline{v}_1, \underline{v}_{i_2} \rangle \subset \langle \underline{v}_1, \underline{v}_{i_2}, \ldots, \underline{v}_{i_3} \rangle.$$

[Pertanto $\langle \underline{v}_1, \underline{v}_{i_2} \rangle = \langle \underline{v}_1, \ldots, \underline{v}_{i_3-1} \rangle \subset \langle \underline{v}_1, \underline{v}_{i_2}, \underline{v}_{i_3} \rangle$]. Proseguendo in maniera analoga, si ottiene una successione di vettori:

$$\underline{v}_1 = \underline{v}_{i_1}, \underline{v}_{i_2}, \underline{v}_{i_3}, \ldots, \underline{v}_{i_s}$$

con $1 = i_1 < i_2 < i_3 < \ldots < i_s \leq m$ e

$$\langle \underline{v}_1 \rangle \subset \langle \underline{v}_1, \underline{v}_{i_2} \rangle \subset \langle \underline{v}_1, \underline{v}_{i_2}, \underline{v}_{i_3} \rangle \subset \ldots \subset \langle \underline{v}_1, \underline{v}_{i_2}, \ldots, \underline{v}_{i_s} \rangle = V.$$

Ovviamente $\{\underline{v}_{i_1}, \underline{v}_{i_2}, \ldots, \underline{v}_{i_s}\}$ è un sistema di generatori di V. Se dimostriamo che tali vettori sono linearmente indipendenti, allora formano una base di V, del tipo cercato [e si noti che in tal caso $s = n$, in base al Teor. **1**]. Sia quindi:

$$\sum_{k=1}^{s} a_k \underline{v}_{i_k} = \underline{0}.$$

Dobbiamo verificare che $a_1 = \ldots = a_s = 0$. Per assurdo, assumiamo che tali coefficienti non siano tutti nulli e denotiamo con a_r l'ultimo coefficiente non nullo. È evidente che almeno un altro coefficiente a_k è non nullo e dunque $2 \leq r \leq s$]. Risulta:

$$a_r \underline{v}_{i_r} = -\sum_{k=1}^{r-1} a_k \underline{v}_{i_k}$$

e quindi $\underline{v}_{i_r} \in \langle \underline{v}_{i_1}, \underline{v}_{i_2}, \ldots, \underline{v}_{i_{r-1}} \rangle$, da cui:

$$\langle \underline{v}_{i_1}, \underline{v}_{i_2}, \ldots, \underline{v}_{i_{r-1}} \rangle = \langle \underline{v}_{i_1}, \underline{v}_{i_2}, \ldots, \underline{v}_{i_{r-1}}, \underline{v}_{i_r} \rangle,$$

in contrasto con la catena di inclusioni strette scritta sopra: assurdo. □

COROLLARIO **3.** *Sia* $dim_K(V) = n$ *e sia* W *un sottospazio vettoriale di* V*, con sistema di generatori* $\{\underline{w}_1, \ldots, \underline{w}_t\}$*. Risulta:*

dim W *è il massimo numero di vettori linearmente indipendenti tra* $\underline{w}_1, \ldots, \underline{w}_t$*.*

DIM. Basta applicare a W il Teor. **3** e tener presente il Cor. **2**(i)). □

DEFINIZIONE **16.** *Sia* $dim_K(V) = n$ *e siano* $\underline{w}_1, \ldots, \underline{w}_t \in V$*. Si chiama* ***rango*** *di* $\underline{w}_1, \ldots, \underline{w}_t$ *[denotato* $rg(\underline{w}_1, \ldots, \underline{w}_t)$*] la dimensione del sottospazio vettoriale gene-*

rato da $\underline{w}_1, \dots, \underline{w}_t$, *cioè:*

$$rg(\underline{w}_1, \dots, \underline{w}_t) = dim\,\langle \underline{w}_1, \dots, \underline{w}_t \rangle.$$

[Si tratta del massimo numero di vettori linearmente indipendenti tra $\underline{w}_1, \dots, \underline{w}_t$. *Ovviamente risulta*

$$rg(\underline{w}_1, \dots, \underline{w}_t) \leq min\{t, dim_K(V)\}.]$$

Rinviamo all'Eserc. **28** la dimostrazione della seguente proposizione, che sarà usata nel Cap. **II** (per dimostrare un teorema relativo al rango di matrici).

PROPOSIZIONE **7.** *Siano* V *e* V' *due* K*-spazi vettoriali. Siano* $\underline{v}_1, \dots, \underline{v}_n \in V$ *e* $\underline{v}'_1, \dots, \underline{v}'_n \in V'$ *tali che:*

$$\sum_{i=1}^{n} a_i \underline{v}_i = \underline{0} \iff \sum_{i=1}^{n} a_i \underline{v}'_i = \underline{0}$$

[cioè $\{\underline{v}_1, \dots, \underline{v}_n\}$ *e* $\{\underline{v}'_1, \dots, \underline{v}'_n\}$ *verificano le stesse (eventuali) relazioni di dipendenza lineare (ovvero hanno le stesse combinazioni lineari di* $\underline{0}$*)]. Risulta:*

$$rg(\underline{v}_1, \dots, \underline{v}_n) = rg(\underline{v}'_1, \dots, \underline{v}'_n).$$

TEOREMA **4.** (Formula di Grassmann). *Siano* U_1, U_2 *due sottospazi vettoriali di un* K*-spazio vettoriale* V. *Supponiamo che* U_1, U_2 *abbiano dimensione finita [ad esempio* $dim_K(U_1) = n_1$, $dim_K(U_2) = n_2$*]. Risulta:*

$$dim_K(U_1) + dim_K(U_2) = dim_K(U_1 + U_2) + dim_K(U_1 \cap U_2).$$

DIM. $U_1 \cap U_2$ ha dimensione finita $[\leq min\{n_1, n_2\}$, in quanto è sottospazio vettoriale di U_1 e di $U_2]$. Poniamo:

$$dim_K(U_1 \cap U_2) = i$$

e scegliamo in $U_1 \cap U_2$ una base $\{\underline{z}_1, \dots, \underline{z}_i\}$. In base al Teor. **2**, possiamo 'completare' i vettori $\underline{z}_1, \dots, \underline{z}_i$ [che sono linearmente indipendenti sia in U_1 che in U_2] sino ad ottenere basi di U_1 e di U_2. Dunque:

$\exists\, \underline{u}_1, \dots, \underline{u}_t \in U_1$ tali che $\{\underline{z}_1, \dots, \underline{z}_i, \underline{u}_1, \dots, \underline{u}_t\}$ è una base di U_1 e
$\exists\, \underline{w}_1, \dots, \underline{w}_s \in U_2$ tali che $\{\underline{z}_1, \dots, \underline{z}_i, \underline{w}_1, \dots, \underline{w}_s\}$ è una base di U_2.

[Si noti che: $t + i = n_1$ e $s + i = n_2$]. Ora consideriamo tutti i vettori introdotti sino ad ora:

$$\underline{z}_1, \dots, \underline{z}_i, \underline{u}_1, \dots, \underline{u}_t, \underline{w}_1, \dots, \underline{w}_s.$$

[Si tratta di $i + t + s = n_1 + s = n_1 + n_2 - i$ vettori]. Se dimostriamo che tali vettori sono una base di $U_1 + U_2$, allora:

$$dim_K(U_1 + U_2) = n_1 + n_2 - i = dim_K(U_1) + dim_K(U_2) - dim_K(U_1 \cap U_2),$$

cioè la tesi.

Per verificare che tali vettori sono una base di $U_1 + U_2$, dobbiamo verificare che:

(i) costituiscono un sistema di generatori di $U_1 + U_2$;
(ii) sono linearmente indipendenti.

(i) Sia $\underline{v}_1 + \underline{v}_2$ un generico vettore di $U_1 + U_2$. Si ha:

$$\underline{v}_1 = a_1\underline{z}_1 + \ ... \ + a_i\underline{z}_i + b_1\underline{u}_1 + \ ... \ + b_t\underline{u}_t,$$
$$\underline{v}_2 = a'_1\underline{z}_1 + \ ... \ + a'_i\underline{z}_i + c_1\underline{w}_1 + \ ... \ + c_s\underline{w}_s,$$

per opportuni coefficienti $a_1, \ ..., a'_1, \ ..., b_1, \ ..., c_1, \ ... \in K$. Allora:

$$\underline{v}_1 + \underline{v}_2 = (a_1 + a'_1)\underline{z}_1 + \ .. \ + (a_i + a'_i)\underline{z}_i + b_1\underline{u}_1 + \ ... \ + b_t\underline{u}_t + c_1\underline{w}_1 + \ ... \ + c_s\underline{w}_s$$

e dunque $\underline{v}_1 + \underline{v}_2 \in \langle \underline{z}_1, \ ..., \underline{z}_i, \underline{u}_1, \ ..., \underline{u}_t, \underline{w}_1, \ ..., \underline{w}_s \rangle$.

(ii) Scriviamo una combinazione lineare nulla dei vettori assegnati:

$$(\bullet) \qquad a_1\underline{z}_1 + \ ... \ + a_i\underline{z}_i + b_1\underline{u}_1 + \ ... \ + b_t\underline{u}_t + c_1\underline{w}_1 + \ ... \ + c_s\underline{w}_s = \underline{0}.$$

Per comodità di notazioni, poniamo:

$$\underline{z} = a_1\underline{z}_1 + \ ... \ + a_i\underline{z}_i, \ \underline{u} = b_1\underline{u}_1 + \ ... \ + b_t\underline{u}_t, \ \underline{w} = c_1\underline{w}_1 + \ ... \ + c_s\underline{w}_s.$$

Dunque $\underline{z} + \underline{u} + \underline{w} = \underline{0}$. Allora:

$$\underline{w} = -(\underline{z} + \underline{u}) \in U_1 \cap U_2$$

[infatti $\underline{w} \in U_2$ e $-(\underline{z} + \underline{u}) \in U_1$]. Pertanto $\underline{w}$ si può esprimere in base $\{\underline{z}_1, \ ..., \underline{z}_i\}$ e si ha:

$$\underline{w} = -(\underline{z} + \underline{u}) = d_1\underline{z}_1 + \ ... \ + d_i\underline{z}_i.$$

Dall'ultima uguaglianza segue che:

$$\underline{z} + \underline{u} + d_1\underline{z}_1 + \ ... \ + d_i\underline{z}_i = \underline{0},$$

cioè:

$$a_1\underline{z}_1 + \ ... \ + a_i\underline{z}_i + b_1\underline{u}_1 + \ ... \ + b_t\underline{u}_t + d_1\underline{z}_1 + \ ... \ + d_i\underline{z}_i = \underline{0},$$

ovvero:

$$(a_1 + d_1)\underline{z}_1 + \ ... \ + (a_i + d_i)\underline{z}_i + b_1\underline{u}_1 + \ ... \ + b_t\underline{u}_t = \underline{0}.$$

Essendo $\underline{z}_1, \ ..., \underline{z}_i, \underline{u}_1, \ ..., \underline{u}_t$ linearmente indipendenti, risulta, in particolare, che $b_1 = \ ... = b_t = 0$. Quindi, sostituendo tali valori, l'espressione $(\bullet)$ diventa:

$$a_1\underline{z}_1 + \ ... \ + a_i\underline{z}_i + c_1\underline{w}_1 + \ ... \ + c_s\underline{w}_s = \underline{0}.$$

Dall'indipendenza lineare di $\underline{z}_1, \ ..., \underline{z}_i, \underline{w}_1, \ ..., \underline{w}_s$, segue che anche

$$a_1 = \ ... = a_i = c_1 = \ ... = c_s = 0$$

e dunque tutti i coefficienti di $(\bullet)$ sono nulli. Pertanto i vettori $\underline{z}_1, \ ..., \underline{z}_i, \underline{u}_1, \ ..., \underline{u}_t, \underline{w}_1, \ ..., \underline{w}_s$ sono linearmente indipendenti. □