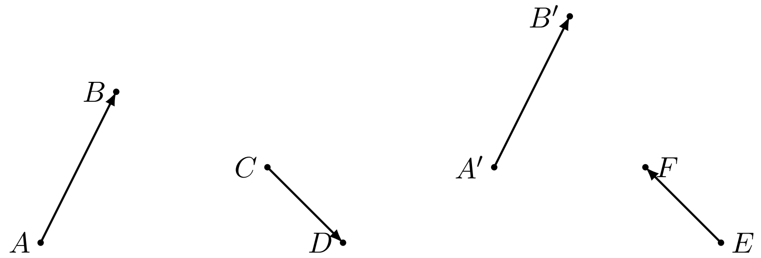
Corso di GEOMETRIA
Dipartimento di Ingegneria ed Architettura
Università degli Studi di Trieste
Prof. Fabio Perroni

1. VETTORI GEOMETRICI E SPAZI VETTORIALI

1 Vettori geometrici

Consideriamo uno spazio affine $\mathbb{A}$ (per il momento si pensi ad $\mathbb{A}$ come una retta, un piano o lo spazio, la definizione di spazio affine verrà data in seguito). Un **vettore applicato** (di $\mathbb{A}$) è dato da una coppia ordinata di punti di $\mathbb{A}$: un **punto iniziale** A (detto anche **punto di applicazione**) ed un **punto finale** B. Il vettore applicato con punto di applicazione A e punto finale B verrà denotato AB (nei libri di testo spesso si usa la notazione $\overrightarrow{AB}$ per indicare un vettore applicato, mentre noi la useremo per indicare un vettore geometrico). Notiamo che il vettore AB in generale è diverso da BA. Nella seguente figura riportiamo alcuni esempi di vettori applicati del piano.



Osserviamo che ci sono vettori del tipo AA, cioè tali che il punto di applicazione coincide con il punto finale.

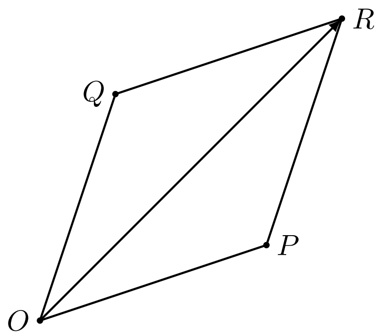
Due vettori applicati sono detti **equipollenti**, se hanno la stessa direzione, la stessa lunghezza e lo stesso verso; in altre parole se giacciono su due rette parallele e se, muovendo una delle due rette parallelamente a sé stessa, è possibile sovrapporre i due vettori in modo che i relativi punti iniziali e finali coincidano. Nella figura qui sopra il vettore AB è equipollente a $A'B'$, ma non è equipollente né a CD né a EF. CD ha la stessa direzione ed intensità di EF, ma verso opposto, così CD non è equipollente ad EF.

Si osservi che l'equipollenza è una relazione di equivalenza nell'insieme dei vettori applicati di $\mathbb{A}$. Infatti ci si convince facilmente che valgono le proprietà riflessiva, simmetrica e transitiva. Un **vettore (geometrico)** è una classe di equivalenza di vettori per la relazione di equipollenza (in questo contesto si dice anche "classe di equipollenza"). Il vettore geometrico associato al vettore applicato AB (cioè la classe di equipollenza di AB) si denota $\overrightarrow{AB}$, mentre i vettori geometrici che non sono riferiti a vettori applicati si denotano con le lettere minuscole, $u, v, w, \ldots$. Il **vettore nullo** è quel vettore rappresentato da un vettore applicato del tipo AA.

Gli spazi vettoriali descrivono la geometria dei vettori. I vettori sono di diversa natura, finora abbiamo visto i vettori geometrici, ma vedremo altri esempi di vettori, come le matrici, le funzioni, i polinomi ....

Osservazione 1. Come abbiamo osservato nel precedente capitolo, fissato un punto O di $\mathbb{A}$, ogni vettore geometrico v è rappresentato da un unico vettore OP applicato in O.

Nell'insieme dei vettori geometrici è possibile definire due operazioni. La **somma di vettori** è definita tramite la regola del parallelogramma nel modo seguente. Siano v e w due vettori geometrici, siano OP ed OQ due rappresentanti di v e w, rispettivamente, con stesso punto di applicazione. Si costruisce il parallelogramma di lati OP ed OQ e si denota con R il quarto vertice di tale parallelogramma.



La somma $v + w$ si definisce come la classe di equipollenza di OR, cioè

$$\overrightarrow{OP} + \overrightarrow{OQ} = \overrightarrow{OR}.$$

Osservazione 2. Notiamo che il punto R coincide sia con il punto finale del vettore equipollente a OQ ed avente come punto di applicazione P, che con il punto finale del vettore equipollente a OP ed avente come punto di applicazione Q.

La definizione della somma di due vettori può essere giustificata dal fatto che in fisica (ad esempio) due forze applicate in uno stesso punto materiale si sommano secondo la regola del parallelogramma.

Osserviamo che l'operazione di somma tra due vettori soddisfa le seguenti proprietà.

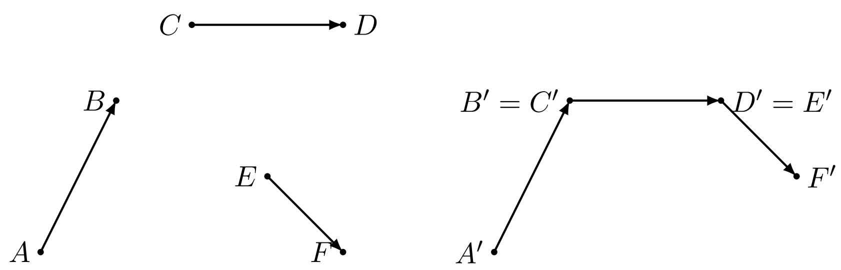
Associativa: per ogni scelta di vettori geometrici u, v, w,

$$(u+v)+w = u+(v+w)\,.$$

Sfruttando questa proprietà possiamo ad esempio scrivere espressioni come $u+v+w$, equivalentemente, svolgendo prima $u+v$ e poi aggiungendo w (in tal caso si ottiene $(u+v)+w$), oppure possiamo calcolare prima $v+w$ ed in fine aggiungere u (in tal caso si ottiene $u+(v+w)$); la proprietà associativa ci garantisce che si ottiene lo stesso vettore in entrambi i casi, che denotiamo quindi $u+v+w$.

Possiamo verificare la proprietà associativa graficamente. Si consideri ad esempio la seguente figura, dove AB, CD, EF sono rappresentanti di u, v, w, rispettivamente, ed $A'B' \sim AB$, $C'D' \sim CD$, $E'F' \sim EF$ ($\sim$ denota la relazione di equipollenza), in altre parole

$$\begin{aligned} u &= \overrightarrow{AB} = \overrightarrow{A'B'}\,, \\ v &= \overrightarrow{CD} = \overrightarrow{C'D'} = \overrightarrow{B'D'}\,, \\ w &= \overrightarrow{EF} = \overrightarrow{E'F'} = \overrightarrow{D'F'}\,. \end{aligned}$$



Sfruttando l'osservazione 2, si ha che $u+v = \overrightarrow{A'D'}$, e quindi $(u+v)+w = \overrightarrow{A'F'}$. D'altro canto $v+w = \overrightarrow{C'F'}$, quindi $u+(v+w) = \overrightarrow{A'F'}$. In conclusione abbiamo che

$$(u+v)+w = \overrightarrow{A'F'} = u+(v+w)\,.$$

Commutativa: per ogni coppia di vettori geometrici u, v,

$$u+v = v+u\,.$$

Questa proprietà segue direttamente dalla definizione di somma secondo la regola del parallelogramma.

Esistenza dell'elemento neutro: se denotiamo con 0 il vettore nullo, allora per ogni vettore geometrico v vale:

$$v+0 = 0+v = v\,.$$

Esistenza dell'opposto: per ogni vettore geometrico v, esiste il suo opposto, cioè un vettore geometrico $-v$, tale che

$$v+(-v) = (-v)+v = 0\,,$$

dove 0 è il vettore nullo.

Per dimostrare questa affermazione, si consideri un rappresentante AB di v, e si definisca $-v$ come la classe di equipollenza di BA. Quindi

$$v + (-v) = \overrightarrow{AB} + \overrightarrow{BA} = \overrightarrow{AA} = 0\,.$$

In seguito, per ogni coppia di vettori v, w, scriveremo semplicemente $v - w$ in luogo di $v + (-w)$.

Nell'insieme dei vettori geometrici, oltre alla somma di due vettori, possiamo definire una **moltiplicazione per scalari** come segue. Per ogni vettore geometrico v e per ogni numero reale $a \in \mathbb{R}$, (in questo contesto i numeri reali si chiamano scalari),

$$a \cdot v$$

è quel vettore geometrico che ha la stessa direzione di v, lunghezza pari a quella di v moltiplicata per il valore assoluto di a, $|a|$, verso concorde con v, se $a > 0$, altrimenti ha verso opposto. Se $a = 0$ si pone $0 \cdot v = 0$. In seguito il vettore $a \cdot v$ verrà denotato con av.

Si può verificare che l'operazione di moltiplicazione per scalari soddisfa le seguenti proprietà, per ogni coppia di vettori geometrici v, w e per ogni coppia di scalari $a, b \in \mathbb{R}$:

$$\begin{aligned}
&1v = v\,;\\
&(-1)v = -v\,;\\
&(a+b)v = av + bv\,;\\
&(ab)v = a(bv)\,;\\
&a(v+w) = av + aw\,.
\end{aligned}$$

2 Campi

Uno spazio vettoriale è sempre definito in relazione ad un campo di scalari K (nel caso dei vettori geometrici $K = \mathbb{R}$, il campo dei numeri reali).

Ricordiamo che un **campo** (di scalari) è un insieme non vuoto K dotato di due operazioni binarie, una somma $+\colon K \times K \to K$, $(a, b) \mapsto a+b$, ed un prodotto $\cdot\colon K \times K \to K$, $(a, b) \mapsto a \cdot b$ (che in seguito sarà denotato anche con ab), in modo che siano soddisfatti i seguenti assiomi, $\forall\, a, b, c \in K$:

<u>K1</u>: (commutatività) $a + b = b + a$, $ab = ba$;

<u>K2</u>: (associatività) $(a + b) + c = a + (b + c)$, $a(bc) = (ab)c$;

<u>K3</u>: (esistenza dell'elemento neutro) $\exists\, 0 \in K$, t.c. $a + 0 = a$, $\exists\, 1 \in K$, t.c. $a1 = a$;

<u>K4</u>: (esistenza dell'opposto e dell'inverso) $\exists -a \in K$, t.c. $a + (-a) = 0$; se $a \neq 0$, $\exists\, a^{-1} \in K$, t.c. $aa^{-1} = 1$ (a^{-1} verrà denotato anche con $\frac{1}{a}$);

<u>K5</u>: (distributività di $\cdot$ rispetto ad $+$) $a(b + c) = ab + ac$;

<u>K6</u>: $ab = 0 \quad \Rightarrow \quad (a = 0) \vee (b = 0)$.

Osservazione 3. K6 è una conseguenza delle precedenti K1–K5. Infatti, supponiamo per assurdo che $(a \neq 0) \wedge (b \neq 0)$. Per la K4 esisterebbe l'inverso di a, a^{-1}. Moltiplichiamo ora ambo i membri di $ab = 0$ per a^{-1}, otteniamo:

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

Ma questo è assurdo perché abbiamo supposto $b \neq 0$.

L'uguaglianza $0 = a^{-1}0$ segue dalle K1–K5, infatti, per ogni $a \in K$, si ha che $a0 = 0$. Per dimostrare questa affermazione osserviamo che $a0 = a(0 + 0) = a0 + a0$, ora sottraendo ad ambo i membri $a0$ si ottiene $0 = (a0 + a0) - a0 = a0$.

Esempio 1. I numeri razionali $\mathbb{Q}$, ed i numeri reali $\mathbb{R}$, con le operazioni usuali sono dei campi.

Nel seguito K sarà esclusivamente uno dei seguenti campi: il campo dei numeri razionali $\mathbb{Q}$; il campo dei numeri reali $\mathbb{R}$, il campo dei numeri complessi $\mathbb{C}$ (si veda la sezione 2.1). Tuttavia esistono altri campi, ad esempio i campi finiti.

Esempio 2. (Esempi di campi "finiti") Sia $\{0, 1\}$ (l'insieme dei resti della divisione per 2). Definiamo due operazioni (binarie), la somma $\oplus$, ed il prodotto $\odot$, come segue:

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

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

Si verifica facilmente che $\{0, 1\}$, con queste operazioni è un campo. Osserviamo che $\oplus$ (rispettivamente $\odot$) sono definite come segue: per ogni $a, b \in \{0, 1\}$, $a \oplus b$ (rispettivamente $a \odot b$) è il resto della divisione per 2 della somma usuale $a + b \in \mathbb{Z}$ (rispettivamente il prodotto usuale $a \cdot b \in \mathbb{Z}$).

Analogamente si può considerare l'insieme $\{0, 1, 2\}$ (dei resti della divisione per 3) e definire due operazioni (binarie), la somma $\oplus$ ed il prodotto $\odot$, come segue:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Anche in questo caso si verifica facilmente che $\{0, 1, 2\}$ con queste operazioni è un campo. Osserviamo che $\oplus$ (rispettivamente $\odot$) sono definite come segue: per ogni $a, b \in \{0,1,2\}$, $a \oplus b$ (rispettivamente $a \odot b$) è il resto della divisione per 3 della somma usuale $a + b \in \mathbb{Z}$ (rispettivamente il prodotto usuale $a \cdot b \in \mathbb{Z}$).

Esercizio 1. 1. Verificare che $\{0,1\}$ con le operazioni $\oplus, \odot$ è un campo.

2. Verificare che $\{0,1,2\}$ con le operazioni $\oplus, \odot$ è un campo.

3. In maniera analoga, definiamo due operazioni $\oplus, \odot$ sull'insieme $\{0,1,2,3\}$ (dei resti della divisione per 4):

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Dimostrare che in questo caso non si ottiene un campo.

Osservazione 4. In generale, per ogni numero naturale $n \neq 0$, si considera l'insieme $\{0, 1, 2, \ldots, n-1\}$ (dei resti della divisione per n, che si denota con $\mathbb{Z}/n\mathbb{Z}$). Si definiscono due operazioni binarie, $\oplus$ e $\odot$, come sopra: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}$, $a \oplus b$ è il resto della divisione per n di $a + b$; $a \odot b$ è il resto della divisione per n di $a \cdot b$, dove $+$ e $\cdot$ sono le usuali operazioni in $\mathbb{Z}$.

Esercizio 2. Dimostrare che le operazioni $\oplus$ e $\odot$ soddisfano le proprietà K1, K2, K3, K5, e che per ogni $a \in \mathbb{Z}/n\mathbb{Z}$ esiste l'opposto $-a$ per l'operazione $\oplus$.

Vale la seguente proposizione.

Proposizione 1. *$\mathbb{Z}/n\mathbb{Z}$ con le operazioni $\oplus, \odot$ è un campo se e solo se n è un numero primo.*

Dim. ($\Rightarrow$) Se n non fosse primo, esisterebbero $a, b \in \mathbb{Z}$ tali che $0 < a, b < n$ ed $n = ab$. Di conseguenza $a \odot b = 0$. Questo è assurdo perché contraddice la proprietà K6.

($\Leftarrow$) Basta dimostrare che, per ogni $a \in \mathbb{Z}/n\mathbb{Z}$ diverso da 0, esiste $b \in \mathbb{Z}/n\mathbb{Z}$ tale che $a \odot b = 1$ (si veda il precedente esercizio). Siccome n è primo, l'insieme $\{a \odot c \,|\, c \in \mathbb{Z}/n\mathbb{Z}\}$ è formato da n elementi distinti. Infatti $a \odot c = a \odot \tilde{c} \Leftrightarrow a \odot (c - \tilde{c}) = 0 \Leftrightarrow n$ divide $a \cdot (c - \tilde{c}) \Leftrightarrow n$ divide a oppure n divide $c - \tilde{c} \Leftrightarrow a = 0$ oppure $c - \tilde{c} = 0$. Quindi $\{a \odot c \,|\, c \in \mathbb{Z}/n\mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$, da cui segue l'esistenza di $b \in \mathbb{Z}/n\mathbb{Z}$ tale che $a \odot b = 1$. □

2.1 I numeri complessi

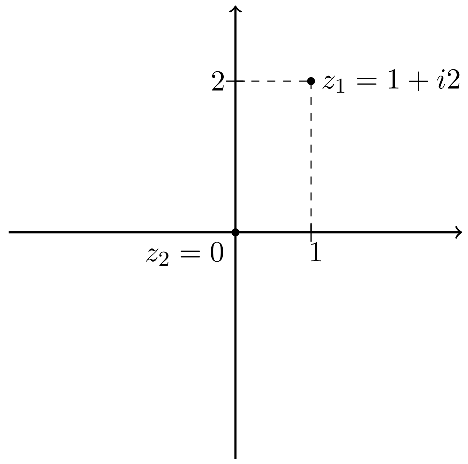
Introduciamo i numeri complessi motivati dalla ricerca di soluzioni di equazioni polinomiali. Si pensi ad esempio all'equazione $x^2 + 1 = 0$. Poiché $a^2 \geq 0$, per ogni $a \in \mathbb{R}$, non esiste alcun numero reale a t.c. $a^2 + 1 = 0$. Ricordiamo che problemi simili si incontrano nel passaggio da $\mathbb{N}$ a $\mathbb{Z}$ (per $a, b \in \mathbb{N}$, l'equazione $a + x = b$ non sempre ammette soluzioni in $\mathbb{N}$, $x = b - a \in \mathbb{Z}$), da $\mathbb{Z}$ a $\mathbb{Q}$, e da $\mathbb{Q}$ ad $\mathbb{R}$.

Per risolvere il problema di cui sopra, introduciamo un nuovo simbolo, l'**unità immaginaria** i, e richiediamo che il suo quadrato sia -1,

$$i^2 = -1\,.$$

Scriveremo anche che $i = \sqrt{-1}$. Un **numero complesso** è una espressione del tipo $a + ib$, con $a, b \in \mathbb{R}$. L'insieme dei numeri complessi si indica con $\mathbb{C}$.

Possiamo rappresentare graficamente i numeri complessi nel piano come segue. Fissato un sistema di assi cartesiani, il numero complesso $z = a + ib$ corrisponde al punto del piano avente ascissa a ed ordinata b. Nella seguente figura sono rappresentati i numeri complessi $z_1 = 1 + i2$ e $z_2 = 0 := 0 + i0$.



Se $z = a + ib \in \mathbb{C}$, a si dice **parte reale** di z, mentre b è la **parte immaginaria** di z; in simboli scriveremo anche

$$a = \mathrm{Re}(z)\,, \qquad b = \mathrm{Im}(z)\,.$$

Ogni numero reale $a \in \mathbb{R}$ può essere pensato come un numero complesso:

$$a = a + i0\,.$$

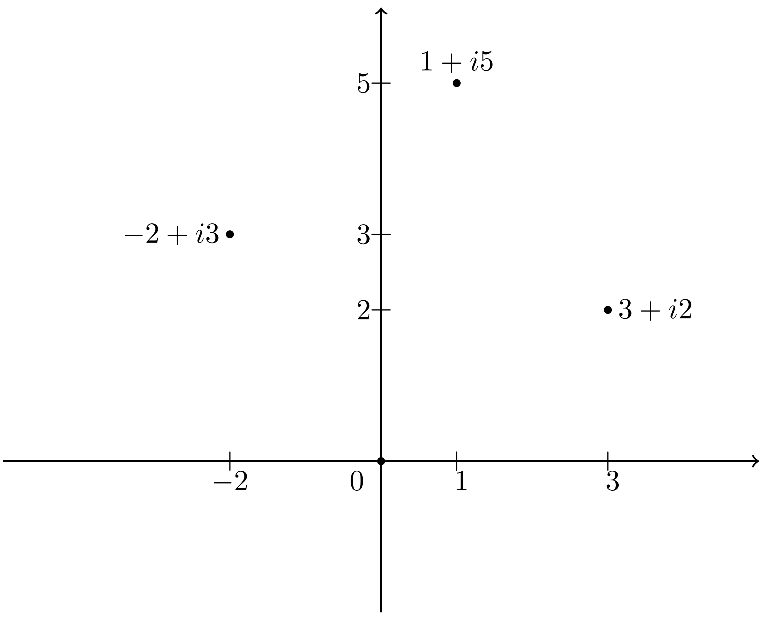
In questo modo possiamo identificare $\mathbb{R}$ come un sottoinsieme di $\mathbb{C}$,

$$\mathbb{R} = \{a + ib \in \mathbb{C} \,|\, b = 0\} \subset \mathbb{C}\,.$$

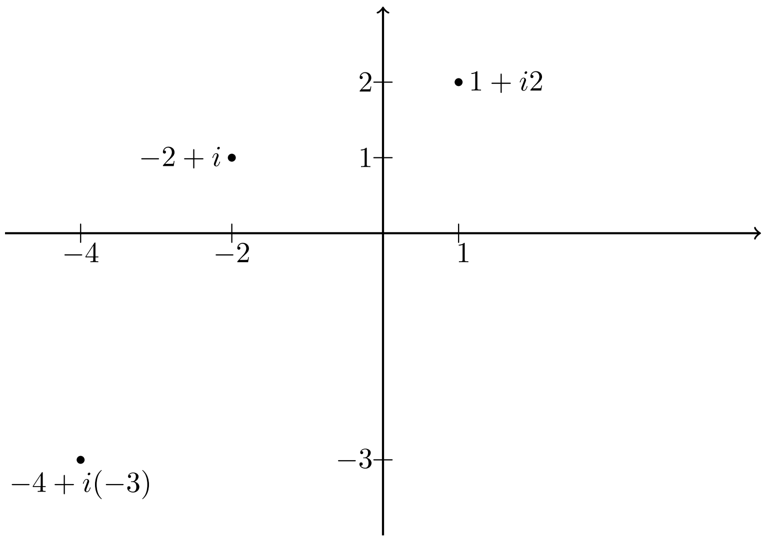
Possiamo estendere a $\mathbb{C}$ le operazioni di somma e prodotto di $\mathbb{R}$ come segue. Siano $z_1 = a + ib, z_2 = c + id \in \mathbb{C}$, allora definiamo

$$\begin{aligned} z_1 + z_2 &:= (a + c) + i(b + d)\,; \\ z_1 z_2 &:= (ac - bd) + i(ad + bc)\,. \end{aligned}$$

Esempio 3. 1. $(3 + i2) + (-2 + i3) = 1 + i5$.



2. $(1+i2)(-2+i) = -4+i(-3)$.



3. Per ogni $r \in \mathbb{R}$, $r(a+ib) = ra + irb$.

Osserviamo che il numero complesso $0 = 0 + i0$ è elemento neutro per la somma e che ogni numero complesso $z = a+ib$ ha un opposto, $-z := -a+i(-b)$. Analogamente $1 = 1 + i0$ è elemento neutro per il prodotto e, se $z = a + ib \neq 0$, allora

$$z^{-1} := \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$$

è l'opposto moltiplicativo di z.

Esercizio 3. Verificare che $\mathbb{C}$ con le operazioni definite sopra è un campo.

Osservazione 5. In $\mathbb{C}$ l'equazione $x^2 + 1 = 0$ ha due soluzioni, $\pm i$. Più in generale, ogni numero reale a, sia positivo che negativo, ha due radici quadrate complesse: $\pm\sqrt{a}$, se $a \geq 0$; $\pm i\sqrt{-a}$, se $a < 0$.

Da questo segue che ogni equazione di secondo grado a coefficienti reali,

$$ax^2 + bx + c = 0 \quad (\text{con } a \neq 0)\,,$$

ammette sempre due soluzioni complesse (eventualmente coincidenti), $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. Ad esempio, $x^2 + x + 1 = 0$ ha come soluzioni $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$.

Per ogni numero complesso $z = a + ib$, il suo **coniugato** si definisce come il numero complesso $\bar{z} = a - ib$. Osserviamo che valgono le seguenti proprietà, per ogni $z, z_1, z_2 \in \mathbb{C}$:

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2}\,; \\ \overline{z_1 \cdot z_2} &= \overline{z_1} \cdot \overline{z_2}\,; \\ z \in \mathbb{R} &\Leftrightarrow z = \bar{z}\,. \end{aligned}$$

Sia $z = a + ib \in \mathbb{C}$. Il **modulo** di z è il numero reale (≥ 0)

$$|z| := \sqrt{a^2 + b^2} = \sqrt{z\bar{z}}\,.$$

Esso coincide con la distanza dall'origine del punto del piano che rappresenta z, in particolare, $z \neq 0 \Leftrightarrow |z| \neq 0$. In tal caso, osserviamo che vale la seguente uguaglianza: $z^{-1} = \frac{\bar{z}}{|z|^2}$.

Sia $z = a + ib \neq 0$. Scriviamo

$$z = a + ib = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2 + b^2}} + i\frac{b}{\sqrt{a^2 + b^2}}\right)\,,$$

ed osserviamo che $\frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}}$ è un numero complesso di modulo 1. Siccome i numeri complessi di modulo 1 corrispondono ai punti della circonferenza di centro l'origine 0 e raggio 1, esiste un angolo θ, tale che

$$\frac{a}{\sqrt{a^2 + b^2}} + i\frac{b}{\sqrt{a^2 + b^2}} = \cos\theta + i\sin\theta\,.$$

Si ha quindi

$$z = |z|(\cos\theta + i\sin\theta)\,.$$

Una tale espressione si dice **rappresentazione trigonometrica** di z. Notiamo che l'angolo θ è definito a meno di multipli interi di $2\pi = 360°$, cioè

$$z = |z|\left(\cos(\theta + 2k\pi) + i\sin(\theta + 2k\pi)\right)\,, \quad \forall\, k \in \mathbb{Z}\,.$$

Esempio 4. 1. Scriviamo in forma trigonometrica $z = i$. Il modulo di i è 1, e l'angolo $\theta = \frac{\pi}{2} = 90°$. Quindi $i = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right)$.

2. $z = 1+i$, allora $|z| = \sqrt{2}$ e $z = \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$. L'angolo $\theta = \frac{\pi}{4} = 45°$, quindi

$$1 + i = \sqrt{2}\left(\cos\left(\frac{\pi}{4} + 2k\pi\right) + i\sin\left(\frac{\pi}{4} + 2k\pi\right)\right)\ , \quad \forall\, k \in \mathbb{Z}\,.$$

3. $z = \sqrt{3} + i$. Il modulo di z è 2, quindi $\sqrt{3} + i = 2\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right)$. L'angolo $\theta = \frac{\pi}{6} = 30°$, quindi

$$\sqrt{3} + i = 2\left(\cos\left(\frac{\pi}{6} + 2k\pi\right) + i\sin\left(\frac{\pi}{6} + 2k\pi\right)\right)\ , \quad \forall\, k \in \mathbb{Z}\,.$$

Il prodotto di due numeri complessi, scritti in forma trigonometrica, assume una espressione particolarmente semplice. Siano

$$\begin{aligned} z &= |z|(\cos\theta + i\sin\theta)\,, \\ w &= |w|(\cos\varphi + i\sin\varphi)\,, \end{aligned}$$

allora

$$\begin{aligned} zw &= |z|\cdot|w|\left((\cos\theta\cos\varphi - \sin\theta\sin\varphi) + i(\cos\theta\sin\varphi + \sin\theta\cos\varphi)\right) \\ &= |z|\cdot|w|\left(\cos(\theta+\varphi) + i\sin(\theta+\varphi)\right)\ , \end{aligned} \tag{1}$$

dove nell'ultimo passaggio abbiamo utilizzato le formule di addizione del seno e coseno. Quindi zw è quel numero complesso di modulo $|z|\cdot|w|$ ed angolo $\theta+\varphi$.

Esempio 5. 1. Per calcolare $(1+i)^5$, usando la rappresentazione trigonometrica di $1+i$ (Esempio 4.1.), abbiamo che

$$\begin{aligned} (1+i)^5 &= (\sqrt{2})^5\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)^5 \\ &= 4\sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) \\ &= 4\sqrt{2}\left(-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) \\ &= -4 - 4i\,. \end{aligned}$$

2. Vogliamo calcolare $(1-i)^6$. La rappresentazione trigonometrica di $1-i$ è come segue

$$\begin{aligned} 1 - i &= \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right) \\ &= \sqrt{2}\left(\cos\left(\frac{7\pi}{4}\right) + i\sin\left(\frac{7\pi}{4}\right)\right)\,. \end{aligned}$$

Quindi

$$\begin{aligned}(1-i)^6 &= (\sqrt{2})^6\left(\cos\left(-\frac{6\pi}{4}\right)+i\sin\left(-\frac{6\pi}{4}\right)\right)\\ &= 8\left(\cos\left(-\frac{3\pi}{2}\right)+i\sin\left(-\frac{3\pi}{2}\right)\right)\\ &= 8i\,.\end{aligned}$$

3. Calcoliamo ora $(\sqrt{3}+i)^6$. Usando l'esempio 4.3. abbiamo che

$$\begin{aligned}(\sqrt{3}+i)^6 &= 2^6\left(\cos\left(\frac{6\pi}{6}\right)+i\sin\left(\frac{6\pi}{6}\right)\right)\\ &= -64\,.\end{aligned}$$

La rappresentazione trigonometrica è utile anche per determinare le radici n-me dei numeri complessi. Sia $w \in \mathbb{C}$, e sia $n \in \mathbb{N}$. Ricordiamo che una radice n-ma di w è un numero (complesso) $z \in \mathbb{C}$, t.c. $z^n = w$. Scrivendo w e z in forma trigonometrica, $w = |w|(\cos\varphi + i\sin\varphi)$, $z = |z|(\cos\theta + i\sin\theta)$, dalla uguaglianza (1) segue che $z^n = w$, se e solo se

$$|z|^n\left(\cos(n\theta)+i\sin(n\theta)\right) = |w|(\cos\varphi + i\sin\varphi)\,.$$

Da questa equazione si deduce facilmente che

$$\begin{cases}|z|^n = |w| & \Rightarrow\ |z| = \sqrt[n]{|w|}\,,\\ n\theta = \varphi + 2k\pi & \Rightarrow\ \theta = \frac{\varphi+2k\pi}{n}\,, \quad k \in \mathbb{Z}\,.\end{cases}$$

Quindi le radici n-me di w sono date dalla seguente espressione:

$$z_k = \sqrt[n]{|w|}\left(\cos\left(\frac{\varphi+2k\pi}{n}\right)+i\sin\left(\frac{\varphi+2k\pi}{n}\right)\right)\,, \quad k \in \mathbb{Z}\,. \tag{2}$$

Osserviamo infine che, se $r \in \{0,1,2,\ldots,n-1\}$ è il resto della divisione di k per n, allora $z_k = z_r$. Infatti, se sostituiamo $k = nq + r$ in (2), otteniamo

$$\begin{aligned}z_k &= \sqrt[n]{|w|}\left(\cos\left(\frac{\varphi+2k\pi}{n}\right)+i\sin\left(\frac{\varphi+2k\pi}{n}\right)\right)\\ &= \sqrt[n]{|w|}\left(\cos\left(\frac{\varphi+2(nq+r)\pi}{n}\right)+i\sin\left(\frac{\varphi+2(nq+r)\pi}{n}\right)\right)\\ &= \sqrt[n]{|w|}\left(\cos\left(\frac{\varphi}{n}+2q\pi+\frac{2r\pi}{n}\right)+i\sin\left(\frac{\varphi}{n}+2q\pi+\frac{2r\pi}{n}\right)\right) = z_r\,.\end{aligned}$$

D'altro canto, se $h,k \in \{0,1,\ldots,n-1\}$ sono distinti, allora gli angoli $\frac{\varphi+2k\pi}{n}$ e $\frac{\varphi+2h\pi}{n}$ differiscono per l'angolo

$$\frac{\varphi+2k\pi}{n} - \frac{\varphi+2h\pi}{n} = \frac{2(k-h)\pi}{n}\,,$$

che è strettamente inferiore ad un angolo giro, e quindi $z_h \neq z_k$. Ne segue che, se $w \neq 0$, ci sono esattamente n radici n-me distinte di w, date dai numeri complessi $z_0, z_1, \ldots, z_{n-1}$ definiti nella formula (2).

Esempio 6. 1. Determiniamo le radici quadrate di -1. In questo caso $n = 2$, $w = -1 = \cos\pi + i\sin\pi$, quindi $|w| = 1$ e $\varphi = \pi$. Applicando la formula (2) troviamo due radici

$$\begin{aligned} z_0 &= \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right) = i\,, \\ z_1 &= \cos\left(\frac{\pi}{2} + \pi\right) + i\sin\left(\frac{\pi}{2} + \pi\right) = -i\,. \end{aligned}$$

Ritroviamo in questo modo le due radici quadrate di -1, cioè $\pm i$.

2. Determiniamo le radice terze dell'unità. In questo caso $n = 3$, $w = 1 = \cos 0 + i\sin 0$, quindi $\varphi = 0$. Ci sono 3 radici distinte che si ottengono sostituendo i valori $k = 0, 1, 2$ in (2):

$$\begin{aligned} z_0 &= 1\,, \\ z_1 &= \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}\,, \\ z_2 &= \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}\,. \end{aligned}$$

Graficamente, z_0, z_1, z_2 corrispondono ai tre punti sul cerchio di raggio 1 e centro 0 che si ottengono ruotando il punto 1 in senso antiorario di un angolo pari a $0°, 120°, 240°$, rispettivamente.

3. Determiniamo le radici quadrate di $w = 1 + i$. In questo caso $n = 2$, $|w| = \sqrt{2}$, $\varphi = \frac{\pi}{4}$. Applicando la formula (2) troviamo 2 radici quadrate di w,

$$\begin{aligned} z_0 &= \sqrt[4]{2}\left(\cos\left(\frac{\pi}{8}\right) + i\sin\left(\frac{\pi}{8}\right)\right)\,, \\ z_1 &= \sqrt[4]{2}\left(\cos\left(\frac{\pi}{8} + \pi\right) + i\sin\left(\frac{\pi}{8} + \pi\right)\right) = -z_0\,. \end{aligned}$$

Concludiamo osservando che le radici n-me di w altro non sono che le radici del polinomio $z^n - w$ (cioè le soluzioni dell'equazione polinomiale $z^n - w = 0$). Dalla precedente discussione segue che tale polinomio ha n radici $(z_0, \ldots, z_{n-1})$, esse sono distinte se $w \neq 0$, altrimenti sono tutte coincidenti $(z_0 = \ldots = z_{n-1} = 0)$. In generale vale il seguente risultato.

Teorema 1 (Fondamentale dell'algebra)**.** *Ogni polinomio di grado $n > 0$ a coefficienti complessi*

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$$

(dove $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{C}$ sono i coefficienti del polinomio $P(z)$ ed $a_n \neq 0$) si fattorizza come prodotto di polinomi di grado 1 (non necessariamente distinti):

$$P(z) = a_n(z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_n)\,. \tag{3}$$

Definizione 1. *Come nel precedente teorema, siano $z_1, \dots, z_n \in \mathbb{C}$ le* ***radici*** *di $P(z)$. La* ***molteplicità algebrica*** *di una radice λ si definisce come il numero delle volte in cui il polinomio $z - \lambda$ compare nella fattorizzazione* (3).

Osservazione 6. Le radici di $P(z)$ coincidono con le soluzioni dell'equazione $P(z) = 0$. Infatti, per ogni $w \in \mathbb{C}$, vediamo che $a_n(w-z_1)\cdot(w-z_2)\cdot\ldots\cdot(w-z_n) = 0$ se e solo se $w = z_i$, per qualche $i = 1, \dots, n$ ($a_n \neq 0$ poiché $P(z)$ ha grado $n > 0$).

Osservazione 7. Siano $\lambda_1, \dots, \lambda_m \in \mathbb{C}$ le radici distinte di $P(z)$, cioè $\{\lambda_1, \dots, \lambda_m\} = \{z_1, \dots, z_n\}$, e $\lambda_i \neq \lambda_j$ per $i \neq j$. Allora possiamo riscrivere la (3) come segue:

$$P(z) = a_n(z - \lambda_1)^{\mu_1} \cdot (z - \lambda_2)^{\mu_2} \cdot \ldots \cdot (z - \lambda_m)^{\mu_m} .$$

Per ogni $i = 1, \dots, m$, l'esponente μ_i coincide con la molteplicità algebrica di λ_i.

Esempio 7. 1. $z^2 + 1 = (z - i)(z + i)$, come si vede facilmente sviluppando il prodotto nel lato destro dell'equazione. D'altro canto le radici quadrate di -1 sono $\pm i$.

2. Abbiamo visto nell'osservazione 5 che il polinomio $z^2 + z + 1$ ha come radici $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. Si ha infatti che $z^2 + z + 1 = \left(z + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)(z + \frac{1}{2} + i\frac{\sqrt{3}}{2})$.

3. $z^n - 1 = (z - z_0)(z - z_1)\ldots(z - z_{n-1})$, dove $z_0, \dots, z_{n-1}$ sono le radici n-me di 1 date da (2).

4. Ci proponiamo ora di fattorizzare il polinomio $P(z) = z^5 - 5z^3 - 2z^2 + 6z + 4$. Come osservato sopra, questo equivale a trovare le sue radici. A tale scopo iniziamo cercando eventuali radici tra i numeri interi $\mathbb{Z}$. Siccome $P(z)$ ha coefficienti interi, se $n \in \mathbb{Z}$ e $P(n) = 0$, allora n divide il termine noto (4 nel nostro esempio). Si vede subito che $P(-1) = 0$, quindi -1 è una radice di $P(z)$. Applicando ora il teorema di Ruffini, deduciamo che $P(z)$ è divisibile per $z + 1$. Infatti dividendo $P(z)$ per $z+1$ troviamo che $P(z) = (z+1)(z^4-z^3-4z^2+2z+4)$. Ora cerchiamo le radici di $Q(z) := z^4 - z^3 - 4z^2 + 2z + 4$. Vediamo che $Q(2) = 0$, e dividendo $Q(z)$ per $z - 2$ troviamo che $Q(z) = (z - 2)(z^3 + z^2 - 2z - 2)$. Quindi

$$\begin{aligned} P(z) &= (z+1)(z-2)(z^3+z^2-2z-2) \\ &= (z+1)(z-2)[z^2(z+1) - 2(z+1)] \\ &= (z+1)(z-2)(z+1)(z^2-2) \\ &= (z+1)^2(z-2)(z-\sqrt{2})(z+\sqrt{2}) . \end{aligned}$$

Le radici distinte di $P(z)$ sono quindi $-1, 2, \pm\sqrt{2}$. La molteplicità algebrica di -1 è 2, mentre le altre radici hanno molteplicità algebrica 1.

5. Il polinomio $P(z) = z^2 + 2iz - 1$ ha la seguente fattorizzazione: $P(z) = (z + i)(z + i)$. Quindi $P(z)$ ha un'unica radice, $\lambda = i$, con molteplicità algebrica 2.

6. Il polinomio $P(z) = z^3 - 3z - 2$ ha la seguente fattorizzazione: $P(z) = (z + 1)^2(z - 2)$. Quindi $P(z)$ ha due radici: $\lambda_1 = -1$, con molteplicità 2; $\lambda_2 = 2$, con molteplicità 1.

2.2 Principio di identità dei polinomi

Sia K un campo, ricordiamo che un polinomio a coefficienti in K nella indeterminata t è un'espressione del tipo

$$a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n \,,$$

per qualche $n \in \mathbb{N}$, dove $a_0, a_1, \ldots, a_n \in K$ sono i **coefficienti** del polinomio. L'insieme dei polinomi a coefficienti in K nella indeterminata t si denota con $K[t]$. Tali polinomi verranno anche denotati $P(t), Q(t)$, ecc.. Il polinomio nullo ha tutti i coefficienti uguali a 0. Ricordiamo che, se $P(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n$ è diverso dal polinomio nullo, allora il grado di $P(t)$ si definisce come il massimo indice i tale che $a_i \neq 0$ e si denota con $\mathrm{gr}(P(t))$.

Per definizione due polinomi $P(t)$ e $Q(t)$ sono uguali se e solo se hanno lo stesso grado e, posto $P(t) = a_0+a_1t+a_2t^2+\ldots+a_nt^n$ e $Q(t) = b_0+b_1t+b_2t^2+\ldots+b_nt^n$ con $a_n \neq 0$ e $b_n \neq 0$, allora $a_i = b_i$ per ogni $i = 0, \ldots, n$.

La **somma** ed il **prodotto** di due polinomi $P(t) = a_0+a_1t+a_2t^2+\ldots+a_nt^n$ e $Q(t) = b_0 + b_1 t + b_2 t^2 + \ldots + b_n t^n$ si definiscono come segue:

$$P(t) + Q(t) = \sum_{i=0}^{n} (a_i + b_i) t^i \,, \quad P(t) \cdot Q(t) = \sum_{k=0}^{2n} (\sum_{i=0}^{k} a_i b_{k-i}) t^k \,,$$

dove si pone $a_i = b_i = 0$ per tutti gli $i > n$. Osserviamo che è sempre possibile supporre che $P(t)$ e $Q(t)$ siano di questa forma, a meno di aggiungere potenze di t con coefficiente nullo.

Se i polinomi $P(t)$ e $Q(t)$ sono entrambi diversi dal polinomio nullo allora $P(t) \cdot Q(t) \neq 0$ e la **formula del grado** afferma che

$$\mathrm{gr}(P(t) \cdot Q(t)) = \mathrm{gr}(P(t)) + \mathrm{gr}(Q(t)) \,.$$

Nel caso in cui $P(t) + Q(t) \neq 0$ si ha

$$\mathrm{gr}(P(t) + Q(t)) \leq \max\{\mathrm{gr}(P(t)), \mathrm{gr}(Q(t))\}$$

e vale l'uguaglianza se $\mathrm{gr}(P(t)) \neq \mathrm{gr}(Q(t))$.

Sia $P(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n \in K[t]$. La funzione $f_P \colon K \to K$ che associa ad ogni $a \in K$ lo scalare $f_P(a) := P(a) = a_0 + a_1 a + a_2 a^2 + \ldots + a_n a^n$ è detta **funzione polinomiale** associata al polinomio $P(t)$.

Teorema 2 (Principio di identità dei polinomi)**.** *Sia K un campo infinito e siano $P(t), Q(t) \in K[t]$. Allora $P(t) = Q(t)$ se e solo se $f_P = f_Q$.*

Osserviamo che se K è un campo finito il principio di identità dei polinomi non vale. Per esempio, sia $K = \mathbb{Z}/2\mathbb{Z}$ e siano $P(t) = 1 + t$, $Q(t) = 1 + t + t^2 + t^3$, allora $P(t) \neq Q(t)$, mentre $f_P(a) = f_Q(a)$ per ogni $a \in \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$.

Ricordiamo il seguente

Teorema 3 (Quoziente e resto)**.** *Siano* $P(t), G(t) \in K[t]$*, con* $G(t) \neq 0$*. Allora esistono e sono unici* $Q(t), R(t) \in K[t]$ *tali che*

$$P(t) = G(t)Q(t) + R(t)\,,$$

dove $R(t) = 0$ *oppure* $\mathrm{gr}(R(t)) < \mathrm{gr}(G(t))$*.*

I polinomi $Q(t)$ ed $R(t)$ sono, rispettivamente, il **quoziente** ed il **resto** della divisione di $P(t)$ per $G(t)$. Diremo che $G(t)$ **divide** $P(t)$ se $R(t) = 0$.

Teorema 4 (Ruffini)**.** *Siano* $P(t) \in K[t]$ *ed* $a \in K$*. Allora il resto della divisione di* $P(t)$ *per* $t - a$ *vale* $P(a)$*. In particolare* $t - a$ *divide* $P(t)$ *se e solo se* $P(a) = 0$*.*

Dim. Dal teorema del quoziente e resto abbiamo che

$$P(t) = (t - a)Q(t) + R(t)\,, \tag{4}$$

dove $R(t) = 0$ oppure ha grado 0, quindi è costante. Ponendo $t = a$ in (4) si ha $P(a) = R(t)$. □

Sia $P(t) \in K[t]$. Una **radice** (o uno **zero**) di $P(t)$ è un elemento $a \in K$ tale che $P(a) = 0$.

Corollario 1. *Un polinomio non nullo di grado* n *ha al più* n *radici.*

Dim. Segue direttamente dal teorema di Ruffini e dalla formula del grado. □

Dimostrazione del principio di identità dei polinomi. Se $P(t) = Q(t)$ si ha evidentemente l'uguaglianza $f_P = f_Q$. Viceversa, se $f_P = f_Q$, allora $P(t) - Q(t)$ è un polinomio con infinite radici. Dal precedente corollario segue che $P(t) - Q(t)$ è il polinomio nullo, da cui il risultato. □

3 Spazi vettoriali

Sia K un campo fissato.

Definizione 2. *Uno* **spazio vettoriale** *su* K *è un insieme non vuoto* V *su cui sono definite due operazioni, una somma* $+\colon V \times V \to V$*,* $(v, w) \mapsto v + w$*, ed un prodotto per scalari* $\cdot\colon K \times V \to V$*,* $(a, v) \mapsto a \cdot v$ *(in seguito scriveremo spesso* av *in luogo di* $a \cdot v$*) in modo che siano soddisfatte le seguenti proprietà, per ogni* $u, v, w \in V$ *e per ogni* $a, b \in K$*:*

SV1: (associativa) $(u + v) + w = u + (v + w)$*;*

SV2: (esistenza del vettore nullo) $\exists 0 \in V$*, t.c.* $0 + v = v + 0 = v$*;*

SV3: (esistenza dell'opposto) $\exists -v \in V$*, t.c.* $v + (-v) = (-v) + v = 0$*;*

SV4: (commutativa) $u + v = v + u$*;*

SV5: (distributiva di $\cdot$ rispetto a $+$) $a(u+v) = au + av$;

SV6: (distributiva di $\cdot$ rispetto alla somma del campo) $(a+b)v = av + bv$;

SV7: $(ab)v = a(bv)$;

SV8: $1v = v$.

Notiamo che abbiamo utilizzato lo stesso simbolo 0 per denotare sia il vettore nullo che lo zero del campo, per non appesantire la notazione. Inoltre, nel seguito, espressioni del tipo $v + (-w)$ verranno semplificate con $v - w$.

Esempio 8. 1. L'insieme dei vettori applicati in un punto O di uno spazio affine $\mathbb{A}$ è uno spazio vettoriale, con la somma data dalla regola del parallelogramma ed il prodotto per scalari.

2. L'insieme dei vettori geometrici con le operazioni descritte all'inizio del capitolo è uno spazio vettoriale su $\mathbb{R}$.

3. Sia

$$\mathbb{R}^n := \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, x_2, \ldots, x_n \in \mathbb{R} \right\}.$$

Definiamo su $\mathbb{R}^n$ due operazioni come segue:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

e, per ogni $a \in \mathbb{R}$,

$$a \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{pmatrix}.$$

Si verifica facilmente che $\mathbb{R}^n$ con queste operazioni è uno spazio vettoriale su $\mathbb{R}$. In particolare il vettore nullo è $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, e l'opposto di $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ è $\begin{pmatrix} -x_1 \\ -x_2 \\ \vdots \\ -x_n \end{pmatrix}$. Gli elementi $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ si chiamano anche vettori colonna, per ogni $i = 1, \ldots, n$, x_i è la componente i-ma di x.

4. Sostituendo nel precedente esempio $\mathbb{R}$ con un campo K si ottiene in maniera analoga lo spazio vettoriale K^n.

5. Sia X un insieme non vuoto. Sia $V := \{f : X \to \mathbb{R}\}$ l'insieme delle funzioni che hanno dominio X e codominio $\mathbb{R}$. La somma di $f, g \in V$ si definisce come quella funzione $(f+g) : X \to \mathbb{R}$ che associa ad ogni $x \in X$ il numero $(f+g)(x) = f(x)+g(x)$. Per ogni scalare $a \in \mathbb{R}$ $af : X \to \mathbb{R}$ è definita come $(af)(x) = af(x)$, $\forall x \in X$. Si verifica facilmente che V è uno spazio vettoriale su $\mathbb{R}$.

Anche in questo caso, se si sostituisce $\mathbb{R}$ con un altro campo K nella definizione di V, si ottiene uno spazio vettoriale su K.

6. Sia $K[t]$ l'insieme dei polinomi a coefficienti in K nella indeterminata t. Dati due polinomi $P(t), Q(t) \in K[t]$, possiamo scrivere $P(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0, Q(t) = b_n t^n + b_{n-1}t^{n-1} + \ldots + b_1 t + b_0 \in K[t]$, per qualche n. Con questa notazione, la somma $P(t) + Q(t)$ è il polinomio

$$(a_n + b_n)t^n + (a_{n-1} + b_{n-1})t^{n-1} + \ldots + (a_1 + b_1)t + (a_0 + b_0)\,.$$

Ad esempio $(3t^3 + t - 5) + (-t^5 + t^3 + 2t^2 - t + 2) = -t^5 + 4t^3 + 2t^2 - 3$. Per ogni $\lambda \in K$, il prodotto $\lambda P(t)$ è il polinomio

$$(\lambda a_n)t^n + (\lambda a_{n-1})t^{n-1} + \ldots + (\lambda a_1)t + (\lambda a_0)\,.$$

Si verifica facilmente che $K[t]$ con queste operazioni è uno spazio vettoriale su K. Il vettore nullo è il polinomio nullo.

7. Si consideri $\mathbb{R}^2$ con la seguente operazione:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \tilde{+} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 - b_2 \end{pmatrix}\,.$$

Sono soddisfatte le proprietà (SV1)–(SV4)?

7. Si consideri $\mathbb{R}^2$ con le seguenti operazioni:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \hat{+} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ 0 \end{pmatrix}\,, \quad a \hat{\cdot} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a \cdot a_1 \\ 0 \end{pmatrix}\,,$$

per ogni $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in \mathbb{R}^2$, $a \in \mathbb{R}$. Si dica se $\mathbb{R}^2$ con queste operazioni è uno spazio vettoriale su $\mathbb{R}$.

Osservazione 8. Sia V uno spazio vettoriale sul campo K. Dagli assiomi SV1–SV8 seguono le seguenti proprietà di V.

1. Per ogni $v \in V$, $0v = 0$, dove il primo 0 a sinistra è lo zero di K, mentre lo 0 a destra è il vettore nullo.
Dim. Sfruttando il fatto che $0 \in K$ è l'elemento neutro per la somma e la SV6, abbiamo le seguenti uguaglianze: $0v = (0+0)v = 0v + 0v$. Aggiungendo ora $-0v$ a destra e sinistra e sfruttando la SV3, concludiamo che $0 = 0v$. $\square$

2. Per ogni $a \in K$, $a0 = 0$, dove 0 denota il vettore nullo.
Dim. Sfruttando le SV2 e SV5 deduciamo che $a0 = a(0+0) = a0 + a0$. Aggiungendo $-a0$ a destra e sinistra, e sfruttando SV3, concludiamo che $0 = a0$. $\square$

3. In V esiste un solo vettore nullo.
Dim. Supponiamo per assurdo che esistano due vettori nulli, $0, \tilde{0} \in V$, cioè tali che $v+0 = 0+v = v$ e $v+\tilde{0} = \tilde{0}+v = v$, $\forall v \in V$. Allora si avrebbe: $0 = 0+\tilde{0} = \tilde{0}$. Quindi un assurdo. $\square$

4. Ogni vettore $v \in V$ ha un solo opposto.
Dim. Se v avesse due opposti, $-v$ e $\widetilde{-v}$, allora si avrebbe:

$$-v = -v + 0 = -v + (v + (\widetilde{-v})) = (-v + v) + (\widetilde{-v}) = 0 + (\widetilde{-v}) = (\widetilde{-v})\,.$$

Che è un assurdo. $\square$

5. Per ogni $v \in V$, $(-1) \cdot v = -v$.
Dim. $v + (-1)v = 1v + (-1)v = (1-1)v = 0v = 0$. Quindi $(-1)v$ è un vettore opposto di v, ma poiché l'opposto è unico, esso coincide con $-v$. $\square$