Università degli Studi di Padova

Algebra Lineare e Geometria

Student :
Alex Gasparini

2 marzo 2026

Indice

1 Numeri Complessi

Definizione 1: Numeri Complessi

Definiamo un nuovo simbolo i, che chiamiamo **unità immaginaria** definita come

$$i^2 = -1$$

Con questo possiamo definire un **numero complesso** z definito come

$$z = a + bi \qquad a, b \in \mathbb{R}$$

L'insieme di tutti i numeri complessi è definito come

$$\mathbb{C} = \{a + bi \mid \forall a, b \in \mathbb{R}\}$$

In principio i numeri comlessi sono nati per risolvere le equazioni di secondo grado, dato che se il discriminante è minore di zero l'equazione non aveva soluzioni nei reali, mentre nei numeri complessi possiamo sempre trovare due valori. Infatti se prendiamo la seguente e quazione e proviamo a risolverla abbiamo che

$$\begin{aligned} x^2 - 4x + 13 = 0 \implies x_{1/2} &= \frac{4 \pm \sqrt{16 - 52}}{2} \\ &= \frac{4 \pm \sqrt{-36}}{2} \\ &= \frac{4 \pm 6i}{2} \\ &= 2 \pm 3i \end{aligned}$$

Detto ciò, capiamo come sono le operazioni tra numeri complessi, e trattiamo la parte immaginaria come se fosse una variabile. Prendiamo due numeri complessi $z_1 = a + bi$ e $z_2 = c + di$, e guardiamo la loro somma

$$\begin{aligned} z_1 + z_2 &= (a + bi) + (c + di) \\ &= a + c + bi + di \\ &= (a + c) + (b + d)i \end{aligned}$$

Chiaramente funziona analogamente per la sottrazione, mentre guardiamo il prodotto

$$\begin{aligned} z_1 \cdot z_2 &= (a + bi) \cdot (c + di) \\ &= ac + adi + bic + bdi^2 \\ &= ac + adi + bci - bd \\ &= ac - bd + adi + bci \\ &= (ac - bd) + (ad + bc)i \end{aligned}$$

Il quoziente lo analiziamo dopo.

Definizione 2: Complesso Coniugato

Sia $z = a + bi$ un numero complesso definiamo il suo **complesso coniugato** il numero complesso

$$\overline{z} = a - bi$$

Quindi il complesso coniugato non è altro che lo stesso numero complesso ma girato il segno alla parte immaginaria, vediamo qualche proprietà

Teorema 1: Proprietà Complesso Coniugato

Siano $z_1 = a + bi$, $z_2 = c + di$ due numeri complessi, allora vale

$$\text{(i)} \quad \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$$

$$\text{(ii)} \quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$$

$$\text{(iii)} \quad \overline{z} = z \iff z \in \mathbb{R}$$

Dimostrazione. (i) Proviamo a semplificare ambo i membri

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{(a + bi) + (c + di)} \\ &= \overline{(a + c) + (b + d)i} \\ &= (a + c) - (b + d)i \end{aligned}$$

$$\begin{aligned} \overline{z_1} + \overline{z_2} &= \overline{a + bi} + \overline{c + di} \\ &= (a - bi) + (c - di) \\ &= (a + c) - (b + d)i \end{aligned}$$

Si nota che sono uguali.

(ii) Ora seguiamo lo stesso ragionamento

$$\begin{aligned} \overline{z_1 \cdot z_2} &= \overline{(a + bi) \cdot (c + di)} \\ &= \overline{(ac - bd) + (ad + bc)i} \\ &= (ac - bd) - (ad + bc)i \end{aligned}$$

$$\begin{aligned} \overline{z_1} \cdot \overline{z_2} &= \overline{a + bi} \cdot \overline{c + di} \\ &= (a - bi) \cdot (c - di) \\ &= (ac - (-b)(-d)) + (a(-d) + (-b)c)i \\ &= (ac - bd) - (ad + bc)i \end{aligned}$$

(iii) Controlliamo l'implicazione ($\implies$)

$$\overline{z} = z \implies a - bi = a + bi \implies -bi = bi \implies 2bi = 0 \implies b = 0$$

Ma un numero complesso con $b = 0$ lo si scrive $z = a + 0i = a \in \mathbb{R}$, ragionamento analogo per l'implicazione inversa.

□

Possiamo notare un qualcosa di interessante se moltiplichiamo un numero complesso $z = a + bi$ per il suo complesso coniugato:

$$\begin{aligned}\overline{z} \cdot z = (a - bi) \cdot (a + bi) &= (a \cdot a - (-b)(b)) + (a \cdot b + (-b) \cdot a)i \\ &= a^2 + b^2 + (ab - ab)i \\ &= a^2 + b^2\end{aligned}$$

Con questo possiamo calcolare il quoziente tra due numeri complessi z_1 e z_2, infatti possiamo moltiplicare e dividere per il quoziente per il complesso coniugato del denominatore abbiamo

$$\frac{z_1}{z_2} = \frac{z_1}{z_2} \cdot \frac{\overline{z_2}}{\overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{(a + bi) \cdot (c - di)}{c^2 + d^2} = \frac{(ac + db) + (bc - bd)i}{c^2 + d^2} = \frac{ac + db}{c^2 + d^2} + \frac{bc - bd}{c^2 + d^2} i$$

Tornando al motivo per cui sono nati i numeri complessi, abbiamo visto che un polinomio di grado 2 ha sempre 2 soluzioni complesse, e ed al più 2 soluzioni reali. C'è una qualche relazione tra il grado e il numero di soluzioni?

Teorema 2: Teorema Fondamentale dell'Algebra

Sia $f(z)$ un polinomio di grado $n \in \mathbb{N}$ a coefficienti complessi, allora l'equazione

$$f(z) = 0$$

Ammette esattamente n radici complesse (contanto anche le molteplicità) e al più n radici reali.

La dimostrazione è omessa, però questo teorema ci garantisce che qualsiasi polinomio noi prendiamo, ci sarà sempre un numero complesso che renda zero tutto il polinomio, però lo stesso non vale per i numeri reali ma questo già lo sapevamo dato che ci sono equazioni che non hanno nessuna soluzione reale, come $x^2 + 1 = 0$.

Teorema 3: Relazione tra Radici di un Polinomio a Coefficienti Reali

Sia $f(z)$ un polinomio di grado $n \in \mathbb{N}$ a coefficienti reali, allora se $z_0 \in \mathbb{C}$ è una radice di $f(z)$, allora anche $\overline{z_0}$ è una radice di $f(z)$

Dimostrazione. Partiamo scrivendo il polinomio in forma estesa, e dato che z è una radice deve valere

$$a_n z_0^n + ... + a_2 z_0^2 + a_1 z_0^1 + a_0 = 0$$

Possiamo applicare il complesso coniugato ad ambo i menbri

$$\overline{a_n z_0^n + ... + a_2 z_0^2 + a_1 z_0^1 + a_0} = \overline{0}$$

Utilizzando le proprietà dei complessi coniugati

$$\begin{aligned}\overline{a_n z_0^n} + ... + \overline{a_2 z_0^2} + \overline{a_1 z_0^1} + \overline{a_0} &= \overline{0} \\ \overline{a_n}\,\overline{z_0^n} + ... + \overline{a_2}\,\overline{z_0^2} + \overline{a_1}\,\overline{z_0^1} + \overline{a_0} &= \overline{0}\end{aligned}$$

Ricordiamo che i coefficienti (a_i) sono reali per le condizioni, e quindi il loro complesso coniugato è il numero stesso. Ragionamento analogo per lo 0

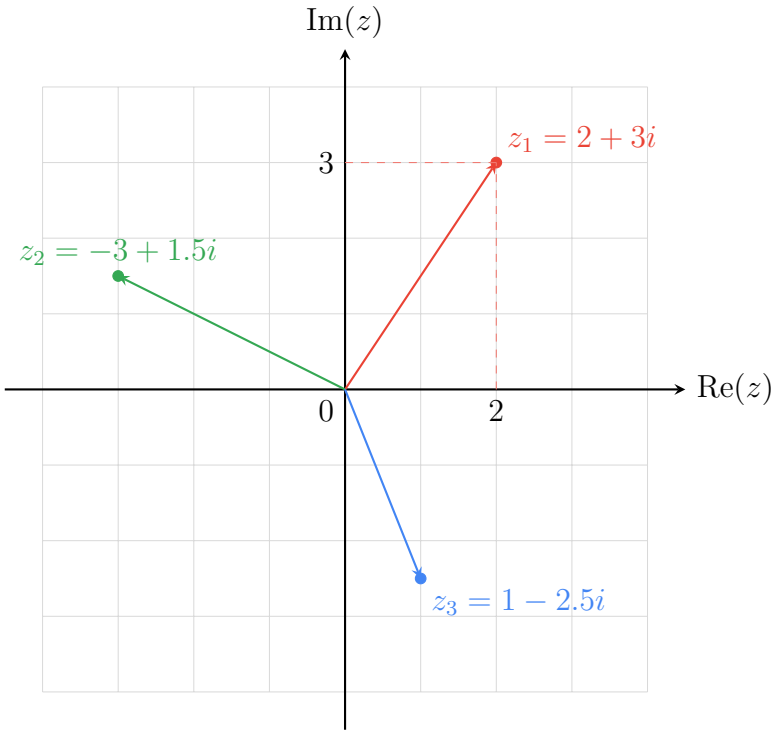
$$a_n\overline{z_0^n} + ... + a_2\overline{z_0^2} + a_1\overline{z_0^1} + a_0 = 0$$

Ma questo non è altro che

$$f(\overline{z_0}) = 0$$

Quindi anche $\overline{z_0}$ è uno zero del polinomio, come volevasi dimostrare. □

I numeri complessi li possiamo rappresentare graficamente sul piano di **Argand-Gauss**, che è l'equivalente del piano cartesiano per le funzioni. Nel piano di Argand-Gauss l'asse delle ascisse è detto **asse reale**, mentre l'asse delle ordinate è detto **asse immaginario**, un numero complesso è composto da una parte reale, che si indica con $\mathrm{Re}(z)$, mentre la parte immaginaria si indica con $\mathrm{Im}(z)$. I numeri complessi li possiamo rappresentare anche come **vettori**, ovvero delle freccie, come possiamo vedere in figura



Con questo notiamo che possiamo rappresentare un numero complesso anche in un'altra forma, ovvero quella trigonometrica, nel senso un qualsiasi numero complesso lo possiamo scrivere come

$$z = \rho(\cos(\theta) + i\sin(\theta))$$

Con ρ la lunghezza del vettore e θ l'angolo che forma rispetto al semiasse positivo dei reali. Se abbiamo un numero complesso in forma algebrica $z = a + bi$ possiamo convertirlo in forma trigonometrica calcolando ρ e θ nel seguente modo

$$\rho = \sqrt{a^2 + b^2} \qquad \theta = \arctan\left(\frac{b}{a}\right)$$

Stando attenti che se $a < 0$ dobbiamo aggiungere a π all'angolo θ dato che l'arcotangente restituisce solo valori nell'intervallo $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

Possiamo scrivere i numeri complessi in un'ulteriore forma, però dobbiamo fare qualche ragionamento prima. Scriviamo gli sviluppi di Taylor in $x = 0$ delle funzioni e^x, $\sin(x)$ e $\cos(x)$.

$$e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + ...$$
$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} + ...$$
$$\cos(x) = 1 - \frac{x^2}{2} + \frac{x^4}{4!} + ...$$

Ora proviamo a mettere xi al posto di x nello sviluppo di e^x e notiamo una cosa

$$\begin{aligned} e^{xi} &= 1 + xi + \frac{(xi)^2}{2} + \frac{(xi)^3}{3!} + \frac{(xi)^4}{4!} + \frac{(xi)^5}{5!} + ... \\ &= 1 + xi + \frac{x^2 i^2}{2} + \frac{x^3 i^3}{3!} + \frac{x^4 i^4}{4!} + \frac{x^5 i^5}{5!} + ... \end{aligned}$$

Per definizione sappiamo che $i^2 = -1$, quindi $i^3 = i^2 \cdot i = -i$, con lo stesso ragionamento possiamo calcolare $i^4 = i^2 \cdot i^2 = -1 \cdot (-1) = 1$ e così via, possiamo calcolare tutte le potenza di i, e quindi le tre funzioni diventano

$$e^{xi} = 1 + xi - \frac{x^2}{2} - \frac{x^3}{3!}i + \frac{x^4}{4!} + \frac{x^5}{5!}i + ...$$

Ora raggruppiamo tutti i termini con la i e quelli senza

$$e^{xi} = \left(1 - \frac{x^2}{2} + \frac{x^4}{4!} + ...\right) + \left(x - \frac{x^3}{3!} + \frac{x^5}{5!} + ...\right) i$$

Riconoscete qualcosa? Ebbenesì questi sono gli sviluppi di Taylor del seno e del coseno, quindi possiamo scrivere

$$e^{xi} = \cos(x) + i\sin(x)$$

Quindi un numero complesso lo possiamo scrivere anche come

$$z = \rho(\cos\theta + i\sin\theta) = \rho e^{\theta i}$$

Con questo abbiamo capito che cos'è l'esponenziale di un numero puramente immaginario, ma cos'è un esponenziale di un numero complesso del tipo $z = a + bi$? La risposta è semplice, basta usare le proprietà degli esponenziali

$$e^z = e^{a+bi} = e^a \cdot e^{bi} = e^a\left(\cos(b) + i\sin(b)\right)$$

Ora controlliamo la seguente espressione presi $z_1 = a + bi$ e $z_2 = c + di$

$$e^{z_1 + z_2} = e^{z_1} \cdot e^{z_2}$$

Anche se sembra ovvio dobbiamo controllarla, infatti sistemando l'espressione alla sinistra abbiamo che

$$e^{z_1+z_2} = e^{(a+c)+(b+d)i} = e^{a+c}\left(\cos(b+d) + i\sin(b+d)\right)$$

Mentre l'espressione alla destra

$$\begin{aligned} e^{z_1} \cdot e^{z_2} &= e^{a+bi} \cdot e^{c+di} \\ &= e^{a}\left(\cos(b) + i\sin(b)\right) \cdot e^{c}\left(\cos(d) + i\sin(d)\right) \\ &= e^{a} \cdot e^{c} \cdot \left(\cos(b) + i\sin(b)\right)\left(\cos(d) + i\sin(d)\right) \\ &= e^{a+c}\left(\cos(b)\cos(d) + i\cos(b)\sin(d) + i\sin(b)\cos(d) + i^2\sin(b)\sin(d)\right) \\ &= e^{a+c}\left(\cos(b)\cos(d) - \sin(b)\sin(d) + i(\cos(b)\sin(d) + \sin(b)\cos(d))\right) \end{aligned}$$

Ma queste solo le formule di addizione di seno e coseno quindi

$$e^{z_1} \cdot e^{z_2} = e^{a+c}\left(\cos(b+d) + i\sin(b+d)\right)$$

Per finire il capitolo dei numeri complessi torniamo al motivo per cui li abbiamo inventati, ovvero risolvere le equazioni. In più abbiamo scoperto che una equazione polinomiale di grado n ha esattamente n soluzioni (contando anche la molteplicità), quindi come possiamo risolvere la seguente equazione polinomiale

$$x^6 + 1 = 0$$

notiamo subito che nei reali non ha soluzioni, dato che richiede una radice sesta di -1. Per risolverla dobbiamo isolare x^6 e riscrivere il -1 in forma esponenziale ricordando che lo possiamo scrivere come $-1 + 0i$, quindi calcoliamo ρ e θ come abbiamo visto prima

$$z = -1 + 0i \implies \begin{cases} \rho = \sqrt{(-1)^2 + 0^2} \\ \theta = \pi + \arctan\left(\frac{0}{-1}\right) \end{cases} \implies \begin{cases} \rho = 1 \\ \theta = \pi \end{cases}$$

Poi dato che stiamo risolvendo una equazione dobbiamo aggiungere anche il termine $+2k\pi$ (con $k \in \mathbb{Z}$) dato che il numero -1, lo possiamo rappresentare sul piano di Argand-Gauss con gli angoli π, 3π, 5π... dato che l'angolo è lo stesso e compie k giri. Quindi $\theta = \pi + 2k\pi$. Ora possiamo riscrivere l'equazione e risolvere

$$\begin{aligned} x^6 + 1 = 0 \implies x^6 = -1 \implies x^6 = 1e^{(\pi+2k\pi)i} &\implies \sqrt[6]{x^6} = \sqrt[6]{e^{(\pi+2k\pi)i}} \\ &\implies x = e^{\frac{\pi+2k\pi}{6}i} \end{aligned}$$

Ora le soluzioni le troviamo dando dei valori a k, e dato che l'equazione inizialmente era di grado 6 dovremo dare a k i valori $k \in \{0, 1, 2, 3, 4, 5\}$

$$\begin{aligned} x_1 &= e^{\frac{\pi}{6}i} = \frac{\sqrt{3}}{2} + \frac{1}{2}i & x_2 &= e^{\frac{3\pi}{6}i} = i & x_3 &= e^{\frac{5\pi}{6}i} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i \\ x_4 &= e^{\frac{7\pi}{6}i} = -\frac{\sqrt{3}}{2} - \frac{1}{2}i & x_5 &= e^{\frac{9\pi}{6}i} = -i & x_6 &= e^{\frac{11\pi}{6}i} = \frac{\sqrt{3}}{2} - \frac{1}{2}i \end{aligned}$$

Con questo siamo riusciti a trovare tutte le 6 soluzioni della equazione, in più possiamo notare le soluzioni sono uno il complesso coniugato di un'altra soluzione, come avevamo visto nel teorema del complesso coniugato.

Definizione 3: Insieme Chiuso rispetto ad Una Operazione

Sia $A \neq \varnothing$ un insieme, sia $\oplus : A \times A \to A$ una operazione binaria, diciamo che A è **chiuso** rispetto a $\oplus$ se vale

$$\forall a_1, a_2 \in A : \quad a_1 \oplus a_2 \in A$$

Ricordiamo i principali insiemi matematici

- Numeri Primi ($\mathbb{P}$) è definito come

  $$\mathbb{P} = \{p \in \mathbb{N} \,|\, \forall a \in \mathbb{N}, 1 < a < p : p \nmid a\}$$

  Questo insieme non è chiuso rispetto alle 4 operazioni fondamentali (somma, sottrazione, prodotto, divisione) dato che se prendiamo due numeri primi avremo sempre un numero pari (dato che i numeri primi sono tutti dispari), però un numero pari non è un numero primo, e quindi la somma di due numeri primi non è mai un numero primo (caso particolare se $p = 2$, ma poco conta). Mentre moltiplicando due numeri primi sicuramente non otteremo mai un numero primo dato che il nuovo numero è divisibile per i due numeri primi.

- Numeri Naturali ($\mathbb{N}$) è definito come

  $$\mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$$

  L'insieme $\mathbb{N}$ è chiuso rispetto alla somma e al prodotto, dato che possiamo prendere due numeri qualsiasi $n_1, n_2 \in \mathbb{N}$ e la loro somma e il loro prodotto sarà sempre in $\mathbb{N}$. Invece $\mathbb{N}$ non è chiuso rispetto a sottrazione e divisione dato che se prendiamo $n_1 = 2$,$n_2 = 5$ allora $n_1 - n_2 \notin \mathbb{N}$, ragionamento analogo per la divisione.

- Numeri Interi ($\mathbb{Z}$) è definito come

  $$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, ...\}$$

  Al contrario di $\mathbb{N}$, l'insieme $\mathbb{Z}$ è chiuso anche per la sottrazione, ma comunque non è chiuso rispetto alla divisione

- Numeri Razionali ($\mathbb{Q}$) è definito come

  $$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$$

  L'insieme $\mathbb{Q}$ è finalemente chiuso rispetto alle 4 operazioni fondamentali, ed è anche un **campo**, che tra poco vedremo che vuol dire

- Numeri Reali ($\mathbb{R}$), che chiaramente è chiuso rispetto alle 4 operazioni ed anch'esso è un campo

- Numeri Immaginari ($\mathbb{C}$) è definito come

  $$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

  Come $\mathbb{Q}$ e $\mathbb{R}$, anche $\mathbb{C}$ è chiuso rispetto le 4 operazioni fondamentali ed è un campo.

Definizione 4: Campo

Sia $K \neq \varnothing$ un insieme, sia $+ : K \times K \to K$ una operazione binaria che chiamiamo "somma", sia $\cdot : K \times K \to K$ una operazione binaria che chiamiamo "prodotto". Diciamo che K è un **campo** se valgono le seguenti affermazioni per $\forall a, b, c \in K$

(i) Proprietà associativa rispetto alla somma:

$$(a + b) + c = a + (b + c)$$

(ii) Proprietà commutativa rispetto alla somma:

$$a + b = b + a$$

(iii) Elemento nullo rispetto alla somma:

$$\exists O \in K : \quad a + O = O + a = a$$

(iv) Elemento inverso addittivo:

$$\exists -a \in K : \quad a + (-a) = (-a) + a = O$$

(v) Proprietà associativa rispetto al prodotto:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(vi) Proprietà commutativa rispetto al prodotto:

$$a \cdot b = b \cdot a$$

(vii) Elemento unitario rispetto al prodotto:

$$\exists I \in K : \quad a \cdot I = I \cdot a = a$$

(viii) Elemento inverso moltiplicativo:

$$\exists a^{-1} \in K : \quad a \cdot a^{-1} = a^{-1} \cdot a = I \quad (a \neq O)$$

(ix) Proprietà distributiva:

$$c \cdot (a + b) = (a \cdot c) + (b \cdot c)$$

N.B. Nella definizione è menzionato l'operatore somma $(+)$ e prodotto $(\cdot)$, **NON** è detto che siano la somma ed il prodotto come la conosciamo, possono anche essere due operazioni completamente diverse ed inventante a seconda di quello che ci serve. Quindi non pensate alla somma ed il prodotto in modo classico, pensate che siano due funzioni che prendono due elementi di K e in output ne esce un'altro elemento di K, dopo vedremo un caso in cui ci inventeremo noi le funzioni somma e prodotto.

Prima abbiamo detto che $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono campi, proviamo a controllare per $\mathbb{Q}$ (il procedimento è analogo per gli altri due insiemi). Prendiamo come operatore somma e prodotto quelli a cui siamo abitutati. Chiaramente le proprietà associative, commutative e distributiva (sia somma che prodotto) sono rispettare delle regole fondamentali dell'algebra. Ora l'elemente neutro per la somma (O) è 0, mentre l'elemento unitario per il prodotto (I) è 1, e chiaramente sono rispettate le regole (iii) e (vii). Preso un numero razionale $\frac{p}{q}$, il suo inverso addittivo è $\frac{-p}{q}$ (che possiamo sempre trovare) e il suo inverso moltiplicativo è $\frac{q}{p}$ (e questo lo possiamo fare dato che l'inverso moltiplicato lo dobbiamo cercare per i valori diversi dall'elemento nullo, e pertanto $p \neq 0$ e quindi possiamo trovare sempre un inverso moltiplicativo).

Gli insiemi $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono dei campi e su questo siamo sicuri, e notiamo una cosa: ovvero che tutti e tre hanno una cardinalità infinita (cioè hanno infiniti elementi), quindi una possibile domanda che ci possiamo fare è se esistono campi finiti (ovvero con un numero finito di elementi). La risposta è sì e adesso vediamo che cosa ne sappiamo su questi campi. In primis stando alla definizione l'insieme deve contenere almeno due elementi: l'elemento neutro (O) e l'elemento unitario (I), quindi non può esistere un campo con un elemento. Però esiste un campo con esattamente 2 elementi? proviamo a inventare due funzioni "somma" e "prodotto" in modo tale da rende un campo con gli elementi $\{0, 1\}$. Se abbiamo solo due elementi allora avremo da gestire le seguenti operazioni

$$\begin{array}{ll} 0+0=? & 0\cdot 0=? \\ 0+1=? & 0\cdot 1=? \\ 1+0=? & 1\cdot 0=? \\ 1+1=? & 1\cdot 1=? \end{array}$$

Affinchè questo sia un campo dobbiamo far valere le condizioni (iii) e (vii), quindi sappiamo che

$$\begin{array}{ll} 0+0=0 & 0\cdot 0=? \\ 0+1=1 & 0\cdot 1=0 \\ 1+0=1 & 1\cdot 0=0 \\ 1+1=? & 1\cdot 1=1 \end{array}$$

Possiamo scegliere $0 \cdot 0 = 0$, mentre per $1 + 1$ dobbiamo fare qualche ragionamento in più. Infatti non possiamo scegliere 2 dato che $2 \notin \{0, 1\}$ e quindi non sarebbe nel campo. Per decidere cosa deve valere quest'ultima espressione, dobbiamo ricorrere alla condizione (iv), ovvero che ogni elemento di un campo deve avere un inverso addittivo, ma fino ad ora non abbiamo ancora trovato un numero che sommato ad 1 dia 0. Pertanto per soddisfare la condizione (iv) dobbiamo imporre $1 + 1 = 0$, perchè altrimenti non esisterebbe nessun numero $a \in \{0, 1\}$ tale che $1 + a = 0$. Quindi le operazioni devono rispettare le seguenti regole

$$\begin{array}{ll} 0+0=0 & 0\cdot 0=0 \\ 0+1=1 & 0\cdot 1=0 \\ 1+0=1 & 1\cdot 0=0 \\ 1+1=0 & 1\cdot 1=1 \end{array}$$

Scegliendo queste operazioni abbiamo costruito un campo finito con due soli elementi, chiaramente dovendo "ricostruire" la somma e il prodotto. Tra l'altro è interessante notare che la somma ha la tabella di verità della **xor**, mentre il prodotto quella della **and**.

Siamo riusciti a costruire un campo con 2 elementi, quindi possiamo sempre costruire un campo con p elementi?

Teorema 4: Teorema di Classificazione dei Campi Finiti

Esiste sempre un campo di n elementi se e solo se $n = p^k$ con $p \in \mathbb{P}$, $p > 1$ e $k \in \mathbb{N}$.

La dimostrazione è omessa, ma questo ci fa capire che, ad esempio, non esiste un campo di 6 elementi dato che $6 = 2 \cdot 3$, quindi non è un numero primo.

Definizione 5: Spazio Vettoriale

Sia $V \neq \varnothing$ un insieme, sia $K \neq \varnothing$ un campo, siano due operazioni binarie "somma" $(+)$ e "prodotto" $(\cdot)$ definite come

$$+ : V \times V \to V$$

$$\cdot : K \times V \to V$$

Diciamo che V è uno **spazio vettoriale** su K con le operazioni "somma" e "prodotto" se valgono le seguente proprietà per $\forall v, u, w \in V$ e $\forall \alpha, \beta \in K$

(i) Elemento nullo rispetto alla somma

$$\exists O \in V \quad : \quad v + O = v = O + v$$

(ii) Proprietà associativa rispetto alla somma

$$(u + v) + w = u + (v + w)$$

(iii) Elemento inverso addittivo

$$\exists -v \in V \quad : \quad v + (-v) = O = (-v) + v$$

(iv) Proprietà commutativa rispetto alla somma

$$v + u = u + v$$

(v) Elemento unitario rispetto al prodotto

$$\exists I \in V \quad : \quad I \cdot v = v$$

(vi) Proprietà associativa rispetto al prodotto

$$\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$$

(vii) Proprietà distributiva I

$$(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$$

(viii) Proprietà distributiva II

$$\alpha \cdot (v + u) = \alpha \cdot v + \alpha \cdot u$$

Vediamo qualche esempio di spazi vettoriali. Se prendiamo $\mathbb{R}^2$, cioè prendiamo una coppia di numeri reali, che è definito come

$$\mathbb{R}^2 = \{(a_1, a_2) \mid a_i \in \mathbb{R}\}$$

Se difiniamo la somma di due punti in $\mathbb{R}^2$ come

$$(a, b) + (c, d) = (a + c, b + d)$$

E se prendiamo un $\lambda \in \mathbb{R}$, definiamo il prodotto come

$$\lambda \cdot (a, b) = (\lambda a, \lambda b)$$

Con queste definizioni è facile mostrare che $\mathbb{R}^2$ è uno spazio vettoriale dato che rispetta tutti i criteri. Analogamente possiamo vedere come $\mathbb{R}^3$ è uno spazio vettoriale, definito come

$$\mathbb{R}^3 = \{(a_1, a_2, a_3) \mid a_i \in \mathbb{R}\}$$

e definendo la somma e prodotto allo stesso modo

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f) \qquad \lambda \cdot (a, b, c) = (\lambda a, \lambda b, \lambda c)$$

Chiaramente questo si può estendere a qualsiasi dimensione n, infatti per ogni $n \in \mathbb{N}$ l'insieme $\mathbb{R}^n$ è uno spazio vettoriale. Questo concetto lo possiamo estendere con il seguente teorema

Teorema 5

Sia K un campo, allora K^n è uno spazio vettoriale $\forall n \in \mathbb{N}$

Questo ci conferma quanto abbiamo detto prima, ma ci permette di dire anche che $\mathbb{Q}^n$ oppure $\mathbb{C}^n$ sono spazi vettoriali.

Definizione 6: Vettori Linearmente Indipendenti

Sia K un campo, V uno spazio vettoriale su K, siano

$$v_1, v_2, v_3, ..., v_n \in V$$

$$a_1, a_2, a_3, ..., a_n \in K$$

Definiamo una **combinazione lineare** la seguente espressione

$$a_1v_1 + a_2v_2 + a_3v_3 + ... + a_nv_n \in V$$

Se poniniamo la combinazione lineare uguale al vettore nullo $(\vec{0})$, se l'unica soluzione a questa equazione è

$$a_1 = a_2 = a_3 = ... = a_4 = 0$$

Allora diciamo che i vettori $v_1, v_2, v_3, ..., v_n$ sono **linearmente indipendenti**, altrimeti si dicono **linearmente dipendenti**.

Vediamo subito un esempio, prendiamo $V = \mathbb{R}^2$, controlliamo se $v_1 = (3,1)$ e $v_2 = (2,5)$ sono linearmente indipendenti rispetto a V, per farlo scriviamo la loro combinazione con a_1,$a_2 \in \mathbb{R}$

$$a_1v_1 + a_2v_2 = a_1(3,+1) + a_2(2,5) = (3a_1, a_1) + (2a_2, 5a_2) = (3a_1 + 2a_2, a_1 + 5a_2)$$

Ora dobbiamo importo uguale al vettore nullo, che in V è $(0,0)$

$$(3a_1 + 2a_2, a_1 + 5a_2) = (0,0) \implies \begin{cases} 3a_1 + 2a_2 = 0 \\ a_1 + 5a_2 = 0 \end{cases}$$

Risolviamolo

$$\begin{cases} 3a_1 + 2a_2 = 0 \\ a_1 = -5a_2 \end{cases} \implies \begin{cases} 3(-5a_2) + 2a_2 = 0 \\ a_1 = -5a_2 \end{cases} \implies \begin{cases} 12a_2 = 0 \\ a_1 = -5a_2 \end{cases} \implies \begin{cases} a_2 = 0 \\ a_1 = 0 \end{cases}$$

Dato che le uniche soluzioni che abbiamo trovato sono $(0,0)$ allora possiamo affermare che v_1 e v_2 sono linearmente indipendenti. Vediamo un altro caso, sia $V = \mathbb{R}^2$ e $v_1 = (1,2)$ e $v_2 = (2,4)$ vediamo se sono linearmente indipendenti o dipendenti

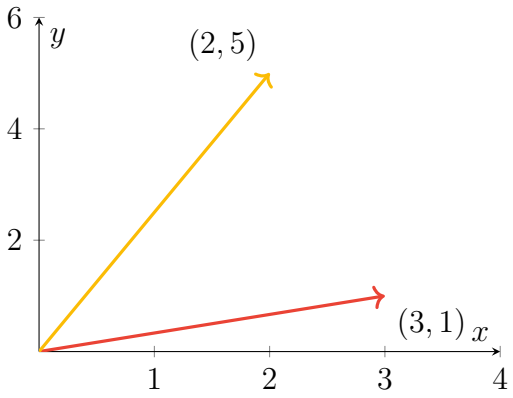
$$a_1v_1 + a_2v_2 = (a_1, 2a_1) + (2a_2, 4a_4) = (a_1 + 2a_2, 2a_1 + 4a_2) = (0,0)$$

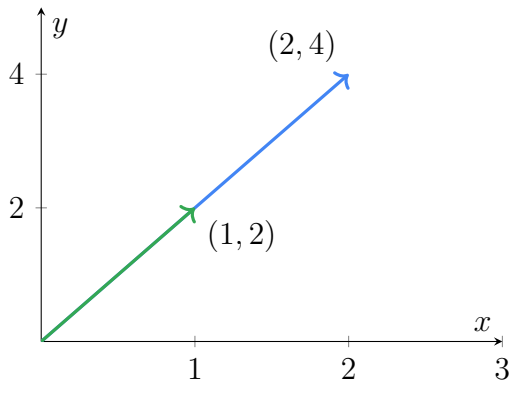
Risolviamo il sistema

$$\begin{cases} a_1 + 2a_2 = 0 \\ 2a_1 + 4a_2 = 0 \end{cases} \implies \begin{cases} a_1 = -2a_2 \\ 2(-2a_2) + 4a_2 = 0 \end{cases} \implies \begin{cases} a_1 = -2a_2 \\ 0a_2 = 0 \end{cases}$$

Qua invece scorpiamo qualcosa di strano, dato che possiamo scegliere un qualsiasi a_2 che la seconda equazione è soddisfatta, pertanto per questo esercizio abbiamo infinite soluzioni, pertanto non sono linearmente indipendenti, e quindi diciamo che sono linearmente dipendenti.

In generale in $\mathbb{R}^2$ due vettori sono linearmente indipendenti se non sono paralleli, infatti prendendo il primo esempio (3,1) e (2,5) non sono paralleli e lo possiamo vedere nel primo grafico, mentre il secondo problema dato che sono paralleli dato che $v_2 = 2v_1$, allora non sono linearmente indipendenti.





Sia $V = \mathbb{R}^2$, siano $v_1 = (3, -2)$,$v_2 = (3, 1)$,$v_3 = (1, 3)$ vediamo se sono linearmente indipendenti

$$\begin{cases} 3a_1 + 3a_2 + a_3 = 0 \\ -2a_1 + a_2 + 3a_3 = 0 \end{cases} \implies \begin{cases} a_3 = 3a_1 - 3a_2 \\ a_2 = 2a_1 - 3a_3 \end{cases} \implies \begin{cases} a_3 = 3a_1 - 3(2a_1 - 3a_3) \\ a_2 = 2a_1 - 3(3a_1 - 3a_2) \end{cases}$$

$$\implies \begin{cases} a_3 = -3a_1 + 9a_3 \\ a_2 = -7a_1 + 9a_2 \end{cases} \implies \begin{cases} a_3 = \frac{3}{8}a_1 \\ a_2 = \frac{7}{8}a_1 \end{cases}$$

Risolvendo notiamo che abbiamo infinite soluzioni, dato che preso un $a_1 \in \mathbb{R}$ possiamo sempre trovare un a_2,a_3, pertanto abbiamo infinite soluzioni e quindi sono linearmente dipendenti. In generale se abbiamo $\mathbb{R}^n$ al massimo n vettori possono essere linearmente indipendenti, in questo caso avevamo $\mathbb{R}^2$ ma avevamo 3 vettori quindi erano dipendenti. Se invece abbiamo meno vettori di quanto è la dimensione dello spazio vettoriale, i vettori possono essere indipendenti, però vedremo più avanti che formano uno sotto-spazio vettoriale dato che non riescono a generare tutti i vettori dello spazio.

Ora controlliamo se in $V = \mathbb{R}^3$ i vettori $v_1 = (2, 0, 1)$,$v_1 = (-1, 1, 0)$ e $v_3 = (3, 3, 1)$ sono linearmente indipendenti.

$$a_1 v1 + a_2 v_2 + a_3 v_3 = \begin{pmatrix} 2a_1 \\ 0 \\ a_1 \end{pmatrix} + \begin{pmatrix} -a_2 \\ a_2 \\ 0 \end{pmatrix} + \begin{pmatrix} 3a_3 \\ 3a_3 \\ a_3 \end{pmatrix} = \begin{pmatrix} 2a_1 - a_2 + 3a_3 \\ a_2 + 3a_3 \\ a_1 + a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Impostiamo il sistema

$$\begin{cases} 2a_1 - a_2 + 3a_3 = 0 \\ a_2 + 3a_3 = 0 \\ a_1 + a_3 = 0 \end{cases} \implies \begin{cases} 2a_1 - a_2 + 3a_3 = 0 \\ a_2 = -3a_3 \\ a_1 = -a_3 \end{cases} \implies \begin{cases} -2a_3 + 3a_3 + 3a_3 = 0 \\ a_2 = -3a_3 \\ a_1 = -a_3 \end{cases}$$

$$\implies \begin{cases} 4a_3 = 0 \\ a_2 = -3a_3 \\ a_1 = -a_3 \end{cases} \implies \begin{cases} a_3 = 0 \\ a_2 = 0 \\ a_1 = 0 \end{cases}$$

Dal sistema si evince che i vettori sono linearmente indipendenti.