

# Teoria degli Insiemi

↗ Project	<b>+ Matematica Discreta</b>
☑ Done	<input checked="" type="checkbox"/>
Σ Due Status	Done!
Σ Current Task	

Inizieremo questo capitolo andando a specificare delle nozioni fondamentali che ci serviranno in maniera particolare durante tutto il corso. A partire dalla **simbologia** che utilizzeremo praticamente in ogni sezione del corso:

- $\emptyset$ : **insieme vuoto**.
- $\mathbb{N}$ : insieme dei numeri **naturali**  $\{1, 2, 3, 4 \dots\}$ .
- $\mathbb{N}_0$ : insieme dei numeri naturali, compreso lo zero  $\{0, 1, 2, 3, 4, \dots\}$ .
- $\mathbb{Z}$ : insieme dei numeri **interi relativi**  $\{\dots, -2, -1, 0, 1, 2, \dots\}$ .
- $\mathbb{Q}$ : insieme dei numeri **razionali**  $\{\frac{3}{5}, \frac{2}{3}, \frac{3}{2}, \dots\}$ .
- $\mathbb{R}$ : insieme dei numeri **reali**  $\{\Pi, \frac{7}{5}, \sqrt{3}\}$ .
- $\mathbb{C}$ : insieme dei numeri **complessi**  $\{i, i + 2, \dots\}$ .
- $\in$ : appartiene, indica che un elemento appartiene ad un insieme.
- $\notin$ : non appartiene, indica che un elemento non appartiene ad un insieme.
- $\exists$ : **quantificatore esistenziale**, indica l'esistenza di una determinata proprietà o elemento.
- $|A|$ : **cardinalità**, indica il numero di elementi di un insieme.
- $\cup$ : **unione** tra due insiemi, indica gli elementi che appartengono ad entrambi gli insiemi.
- $\cap$ : **intersezione** tra due insiemi, indica gli elementi in comune ad entrambi.
- $\subset$ : **sottoinsieme proprio**.

- $\subseteq$ : **sottoinsieme**, la differenza con quello di sopra è che i due possono coincidere.
- $\setminus$ : **differenza** tra due insiemi, cioè gli elementi del primo senza gli elementi dell'altro.
- $\times$ : **prodotto cartesiano**, insieme di tutte le possibili coppie ordinate tra due insiemi.
- $\{x\}$ : **singleton**, insieme costituito da un solo elemento.
- $\mathcal{P}(A)$ : **insieme delle parti**, ossia l'insieme costituito da tutti e soli i sottoinsieme di  $A$ .

A proposito dell'insieme dei numeri naturali compreso lo 0,  $\mathbb{N}_0$ , esistono alcune proprietà molto importanti di questo insieme, che ci aiuteranno a capire molte cose durante il corso. In  $\mathbb{N}_0$  vale la **proprietà di tricotomia**, dove per ogni  $a, b \in \mathbb{N}_0$  sussiste una e una sola delle seguenti asserzioni:  $a < b$ ,  $b < a$ ,  $a = b$ .

Siano sempre  $a, b \in \mathbb{N}_0$ . Diciamo che  $a$  **divide**  $b$  se esiste un numero  $k \in \mathbb{N}_0$  tale che  $b = ak$  e scriveremo  $a|b$ . Diciamo anche che  $a$  è un **divisore** di  $b$  o che  $b$  è un **multiplo** di  $a$ . Sempre all'interno di questo insieme, diremo che un numero naturale positivo  $p$  si dice **primo** se  $p \neq 1$  e se gli unici divisori di  $p$  sono 1 e  $p$ . Da queste diciture nasce il **teorema fondamentale dell'aritmetica**.

- **T.H.** = sia  $n \geq 2$  un numero naturale. Allora avremo che  $n = p_1 p_2 \dots p_t$ , con  $t \geq 1$  e  $p_1 p_2 \dots p_t$  primi. In pratica, questo numero può essere scritto come prodotto di numeri primi.

L'argomento principale di questo capitolo introduttivo è sicuramente il **principio di induzione**, che ci fornisce un metodo dimostrativo efficace all'interno dell'insieme dei numeri naturali. Consideriamo una qualsiasi proposizione  $P(n)$  dove  $n \in \mathbb{N}$  e  $n_0$  è il numero iniziale. Partiamo da una **base induttiva**, dove verifichiamo che  $P(n_0)$  sia vera. Una volta verificato, andiamo a supporre per vera l'**ipotesi induttiva**  $P(n)$  iniziale. Dopodiché, passiamo al **passo induttivo**, in cui verificheremo che la proposizione  $P(n + 1)$  sia vera. Se coincide con  $P(n)$ , allora essa sarà vera per qualsiasi numero naturale  $n \geq n_0$ . Per chiarire, andremo a vedere un pratico esempio.

- **ES** = vogliamo dimostrare, per induzione, che  $\forall n \geq 2$ , risulta vero:

$$\circ 3^2 + 3^3 + 3^4 + \dots + 3^n = \frac{3^{n+1} - 9}{2}$$

Per prima cosa, verifichiamo la base dell'induzione, quindi il nostro numero più piccolo 2:

- o  $3^2 = \frac{3^{2+1}-9}{2} \rightarrow 9 = \frac{18}{2} \rightarrow 9 = 9 \rightarrow \text{VERIFICATO}$

Supponendo per vera che l'ipotesi sia vera per  $n$ , dimostriamo che lo sia anche per  $n + 1$ , dimostrando che:

- o  $3^2 + 3^3 + 3^4 + \dots + 3^n + 3^{n+1} = \frac{3^{n+1+1}-9}{2}$

Nell'ipotesi, abbiamo supposto per vero che il blocco colorato in rosso sia vero, quindi andiamo a porre vero in base alle nostra ipotesi.

- o  $\frac{3^{n+1}-9}{2} + 3^{n+1} = \frac{3^{n+2}-9}{2} \rightarrow \frac{3^{n+1}-9+2 \cdot 3^{n+1}}{2} = \frac{3^{n+2}-9}{2}$

Grazie alle proprietà delle potenze, la parte di sinistra dell'espressione possiamo scriverla in questo modo:

- o  $\frac{3 \cdot 3^{n+1}-9}{2} = \frac{3^{n+2}-9}{2}$

Ovviamente, sempre per la proprietà delle potenze, possiamo scrivere 3 come  $3^1$  e, quindi, trovarci con l'asserzione:

- o  $\frac{3^{n+2}-9}{2} = \frac{3^{n+2}-9}{2} \rightarrow \text{VERIFICATO}$



# Relazioni tra Insiemi

↗ Project	<a href="#">Matematica Discreta</a>
☑ Done	
Σ Due Status	Done!
Σ Current Task	

Siano  $A$  e  $B$  due insiemi. Diremo che un sottoinsieme  $\mathcal{R}$  di  $A \times B$  è una **relazione**, o **corrispondenza** tra  $A$  e  $B$ . Ma com'è definita questa relazione? Prendendo un arbitrario elemento  $x \in A$  e  $y \in B$ , tali che  $(x, y) \in \mathcal{R}$ , allora diremo che  $x$  è nella relazione  $\mathcal{R}$  con  $y$ . Gli insiemi, i nostri  $A$  e  $B$  sono detti rispettivamente **dominio** e **codominio**. Avendo introdotto questi due concetti, andiamo ad analizzare un caso speciale di relazione, ossia la **funzione** o **applicazione**. Una funzione è definita come segue:

- $\mathcal{R}$  è una funzione di  $A$  in  $B: \iff \forall x \in A, \exists!y \in B : x\mathcal{R}y.$

Cosa significa questo? In altre parole, ogni elemento del dominio è associato in modo unico a un elemento del codominio. Mentre, invece, in una relazione generica, un elemento del dominio può avere più di un elemento associato nel codominio. Ogni relazione può godere di alcune proprietà fondamentali, che ci aiuteranno a definire altri tipi di relazioni più complesse.

- **relazione riflessiva** -  $x\mathcal{R}x.$
- **relazione simmetrica** -  $x, y \in A$ , da  $x\mathcal{R}y$  allora  $y\mathcal{R}x.$
- **relazione transitiva** -  $x, y, z \in A$ , se  $x\mathcal{R}y$  e  $y\mathcal{R}z$  allora  $x\mathcal{R}z.$

Dopo aver definito le relazioni generiche, come detto, è giusto soffermarci sulle funzioni, che abbiamo appena accennato prima. Nella funzione, un'**immagine**, denotata con  $Im(f)$  è il sottoinsieme del codominio che rappresenta tutti i valori che la funzione può restituire quando si applica ad elementi del dominio. Possiamo distinguere diversi tipi di funzione e una prima catalogazione basica viene fatta in questo modo:

- una funzione si dice **iniettiva** quando, ad elementi distinti del dominio, corrispondono immagini distinte del codominio. In simboli  $f(x)$  è iniettiva se e

solo se  $x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$ .

- una funzione si dice **suriettiva** quando ogni elemento del codominio, è immagine di almeno un elemento del dominio. In simboli  $f(x)$  è suriettiva se e solo se  $\forall y \in B, \exists x \in A : f(x) = y$ .
- una funzione si dice **biettiva** se è sia iniettiva che suriettiva, quindi se ad ogni elemento dell'insieme  $A$  corrisponde uno ed un solo elemento dell'insieme  $B$  e viceversa. In simboli  $f(x)$  è biettiva se e solo se  $\forall x \in A, \exists!y \in B : f(x) = y$  e viceversa.

Quando ci troviamo di fronte ad una funzione biettiva  $f : A \rightarrow B$ , avrebbe senso definire la **funzione inversa**  $f^{-1}$  di  $B$  in  $A$ . Semplicemente, nell'applicazione inversa, viene associato ad ogni elemento di  $B$ , l'unico elemento di  $A$  di cui è immagine in  $f$ . Siano  $f : A \rightarrow B$  e  $g : B \rightarrow C$  due funzioni tali che il codominio di  $f$  coincide col dominio di  $g$ . Parleremo di **funzione composta**,  $f \circ g$ , di  $A$  in  $C$ , che ad ogni elemento  $x \in A$  associa l'elemento di  $C$  che si ottiene applicando  $g$  all'elemento  $f(x)$  di  $B$ . In simboli:

- $g \circ f : x \in A \rightarrow g(f(x)) \in C$ .

Definite in maniera dettagliate le funzioni, andiamo a concentrarci su altri casi particolari di relazioni e partiamo dalle **relazioni d'equivalenza**. Prima di parlarne nel dettaglio, però, soffermiamoci su alcuni concetti. Partiamo col dire che, dato un insieme  $A$  non vuoto e sia  $F$  un insieme di sottoinsiemi di  $S$ .  $F$  sarà detto **partizione** di  $S$  se e solo se ogni elemento di  $F$  è un sottoinsieme non vuoto di  $S$  e gli elementi di  $F$  sono a due a due disgiunti e la loro unione restituisce  $F$ . Il concetto di partizione è strettamente legato a quello di relazione d'equivalenza. Partiamo col dire che una relazione di equivalenza è una relazione che è riflessiva, simmetrica e transitiva. Sia  $A$  un insieme e sia  $\mathcal{R}$  una relazione d'equivalenza definita su di esso. Se  $x \in A$ , il sottoinsieme di  $A$ , costituito da tutti e soli gli elementi che sono in relazione con  $x$  sarà chiamato **classe di equivalenza** di  $x$  modulo  $\mathcal{R}$ , denotato col simbolo  $[x]_{\mathcal{R}}$ . L'insieme di tutte le classi di equivalenza è detto **insieme quoziente** ed è denotato con  $A/\mathcal{R}$ . Da qui, deriva il **teorema fondamentale delle relazioni d'equivalenza**:

- **T.H.** = Sia  $A$  un insieme non vuoto. Se  $\mathcal{R}$  è una relazione di equivalenza in  $A$ , l'insieme quoziente  $A/\mathcal{R}$  è una partizione di  $S$ . Se  $F$  è una partizione di  $A$ , esiste una e una sola relazione d'equivalenza  $\mathcal{R}_F$  tale che  $F = A/\mathcal{R}_F$ .

L'ultimo tipo di relazione che andremo a vedere, sono le **relazioni d'ordine**. Una relazione è d'ordine se è riflessiva, asimmetrica e transitiva. Di solito, una qualsiasi

d'ordine  $\mathcal{R}$  viene denotata col simbolo  $\leq$ . La coppia  $(A, \leq)$  con  $A$  un insieme non vuoto e  $\leq$  la relazione d'ordine su di esso, viene detto **insieme parzialmente ordinato**. Sia  $(A, \leq)$  un insieme parzialmente ordinato,  $x, y \in A$  sono detti **confrontabili** se si verifica che  $x \leq y$  o  $y \leq x$ . Se  $x$  e  $y$  sono confrontabili, allora l'insieme sarà detto **insieme totalmente ordinato**. Sia  $(A, \leq)$  un insieme ordinato, esso può essere facilmente rappresentato dal **diagramma di Hasse**, una rappresentazione grafica che usa un criterio particolare. Gli elementi sono insiemi di punti e, se confrontabili, vengono collegati dai segmenti. Se  $x < y$ , allora  $x$  è più basso rispetto a  $y$  nel diagramma. Dal diagramma di Hasse possiamo ricavare diversi elementi importanti. Sia sempre  $(A, \leq)$  un insieme ordinato. Un elemento  $a \in A$  si dice **minimo** di  $A$  se è confrontabile con ogni elemento  $x$  di  $A$  e risulta sempre  $a \leq x$ . In pratica, indichiamo l'elemento più in basso nel diagramma. Analogamente, un qualsiasi elemento  $b \in A$  si dice **massimo** se è confrontabile con ogni elemento  $x$  di  $A$  e risulta sempre  $x \leq b$ . Analogamente, sarà l'elemento più in alto all'interno del diagramma. Un insieme può essere privo di massimo e minimo ma, se esistono, essi sono unici. Sia sempre  $(A, \leq)$  un insieme ordinato. Sia  $x \in A$ , esso si dice **minimale** se non esiste  $a$  tale che  $a \leq x$ , cioè se al di sotto non c'è nessun elemento. Sembra essere un concetto analogo a quello di minimo, ma in realtà il minimo è unico, mentre gli elementi minimali possono essere anche di più. Analogamente, questo elemento  $x$  si dirà **massimale** se e solo se non esiste un  $x$  tale che  $x \leq a$ . Se un punto è minimo, o massimo, allora è anche minimale, o massimale. Ma non viceversa. Sia sempre  $(A, \leq)$  un insieme ordinato e sia  $B \subseteq A$ . Un elemento  $a \in A$  si dice **minorante** di  $B$  in  $A$  se è confrontabile con ogni elemento di  $B$  e risulta  $a \leq x$  per ogni  $x \in B$ . Analogamente, l'elemento  $a$  si dice **maggiorante** di  $B$  in  $A$  se e solo se è confrontabile con ogni elemento di  $B$  e risulta  $x \leq a$  per ogni  $x \in B$ . Date le condizioni di prima, se  $a$  è il massimo dell'insieme dei minoranti di  $B$ , allora si chiamerà **estremo inferiore** di  $B$ . Viceversa, se  $a$  risulta il minimo dei maggioranti, allora sarà l'**estremo superiore** di  $B$ . In un insieme ordinato  $(A, \leq)$ , se esiste estremo inferiore e superiore, allora l'insieme prende nome di **reticolo**.



# Elemento di Calcolo Combinatorio

↗ Project	<b>+ Matematica Discreta</b>
☒ Done	<input checked="" type="checkbox"/>
Σ Due Status	🎉 Done!
Σ Current Task	∅

Prima di entrare nel merito delle strategie di calcolo combinatorio vero e proprio, vengono fuori alcuni principi importanti, che non hanno bisogno di dimostrazione e che enunceremo brevemente.

- **principio di addizione**: siano  $A$  e  $B$  insiemi disgiunti, allora  $|A \cup B| = |A| + |B|$ .
- **principio di inclusione-esclusione**: siano  $A$  e  $B$  insiemi finiti, allora  $|A \cup B| = |A| + |B| - |A \cap B|$ .
- **principio di moltiplicazione**: siano  $A$  e  $B$  insiemi finiti, allora  $|A \times B| = |A| \cdot |B|$ .
- **principio dei cassetti (piccionaia)**: siano  $m$  ed  $n$  numeri naturali tale che  $m > n$ . Se vogliamo riporre  $m$  oggetti in  $n$  cassetti, almeno un cassetto deve contenere più di un oggetto. Qui possiamo abbozzare una dimostrazione, dicendo banalmente che, se ogni cassetto contenesse al più un oggetto, il numero totale degli oggetti sarebbe al più  $n$ , andando contro alla dicitura iniziale  $m > n$ .

Il calcolo combinatorio studia i raggruppamenti che si possono ottenere con un dato numero  $n$  di oggetti, disposti su un dato numero  $k$  di posti. I raggruppamenti possono essere formati con o senza **ripetizioni** degli  $n$  oggetti. Abbiamo tre tipi di raggruppamenti:

- **permutazioni**: quando  $n = k$  e conta l'ordine con cui si dispongono gli elementi.

- **disposizioni**: quando  $n \neq k$  e conta l'ordine su cui si dispongono gli elementi.
- **combinazioni**: quando  $n \neq k$  e non conta l'ordine con cui si dispongono gli elementi.

Quindi, come abbiamo visto, ogni tipo di raggruppamento si calcola in maniera differente in base al fatto se contano le ripetizioni o no. Qui di seguito verranno elencati banalmente i calcoli.

<i>n oggetti, k posti</i>	<i>senza ripetizioni</i>	<i>con ripetizione r di oggetti</i>
<b>Permutazioni, <math>n = k</math></b>	$n!$	$\frac{n!}{r_1!r_2!...r_k!}$
<b>Disposizioni, <math>n \neq k</math></b>	$\frac{n!}{(n-k)!}$	$n^k$
<b>Combinazioni, <math>n \neq k</math></b>	$\frac{n!}{k!(n-k)!}$	$\frac{(n+k-1)!}{k!(n-1)!}$



# Strutture Algebriche

↗ Area	<a href="#">Studio</a>
↗ Project	<a href="#">Matematica Discreta</a>
☑ Done	
Σ Due Status	Done!
Σ Current Task	

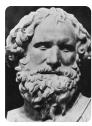
Le strutture algebriche sono un elemento fondamentale dell'algebra e servono a descrivere le proprietà e le relazioni tra gli oggetti matematici, come i numeri, le funzioni, i vettori e così via. Prima di scendere nel dettaglio, diciamo che, dato un insieme  $A$ , una funzione  $\perp : A \times A \rightarrow A$  si chiama **operazione interna**.

Consideriamo l'operazione  $\perp$  nell'insieme  $A$ . Dati due elementi  $x, y \in A$ , essi sono detti **permutabili** se, nella coppia  $(A, \perp)$  si ha  $x \perp y = y \perp x$ . Se si verifica questa condizione, allora l'operazione sarà **commutativa**. L'operazione è detta **associativa** se e solo se  $(x \perp y) \perp z = x \perp (y \perp z)$ . Se  $A$  è un insieme finito e  $\perp$  è la sua operazione interna, è possibile rappresentare tale operazione all'interno della tabella di moltiplicazione, che ha più o meno questo aspetto.

$\perp$	$x_1$	$x_2$	$\cdots$	$x_n$
$x_1$	$x_1 \perp x_1$	$x_1 \perp x_2$	$\cdots$	$x_1 \perp x_n$
$x_2$	$x_2 \perp x_1$	$x_2 \perp x_2$	$\cdots$	$x_2 \perp x_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$x_n$	$x_n \perp x_1$	$x_n \perp x_2$	$\cdots$	$x_n \perp x_n$

Ogni insieme, può essere dotato di elementi particolari, che ora andiamo a definire. Sia  $(A, \perp)$  una struttura algebrica generica. Un elemento  $e \in A$  si dice **neutro** se si ha che  $e \perp x = x$ , con  $x$  un qualsiasi elemento di  $A$ . Per esempio, in  $(\mathbb{N}_0, +)$ , l'elemento neutro è, ovviamente, lo 0. Sia sempre  $(A, \perp)$  una struttura algebrica dotata di elemento neutro  $e$  e sia  $x \in A$ . Un elemento  $x'$  si dice **simmetrico** di  $x$  se si ha che  $x \perp x' = e$ . A sua volta, se dotato di simmetrico, allora  $x$  si dice **simmetrizzabile**. Prendiamo sempre in considerazione  $(A, \perp)$  come struttura algebrica generica. Un elemento  $a \in A$  si dice **regolare a sinistra** rispetto a  $\perp$  se da  $a \perp x = a \perp y$  segue che  $x = y$ . A sua volta, sarà **regolare a destra** se da

$x \perp a = y \perp a$  segue che  $x = y$ . Un elemento regolare a destra e a sinistra si dice **regolare** rispetto a  $\perp$ . Fino ad ora abbiamo parlato di strutture algebriche con un'operazione interna, ma possiamo avere anche un'**operazione esterna**. Siano  $A$  e  $B$  insiemi, una funzione  $\star : B \times A \rightarrow A$  si dice operazione esterna di  $A$  con **dominio di operatori** in  $B$ . Gli elementi di  $B$  si chiamano, solitamente, **scalari**. Esistono alcune strutture algebriche notevoli, che andremo a definire dato che ci serviranno, in futuro, per poter identificare. Partiamo col dire che, se all'interno della struttura algebrica c'è una sola operazione, allora parleremo di struttura algebrica semplice. Una struttura algebrica semplice  $(A, \perp)$  si dice **semigruppo** se  $\perp$  è associativa. Se, invece, ha anche un elemento neutro, allora parliamo di **monoide**. Se, allora, ogni suo elemento è simmetrizzabile, allora parliamo di **gruppo**. Se l'operazione è anche commutativa, abbiamo un **gruppo abeliano**. In presenza di una struttura con più operazioni interne, come  $(A, \perp, \top)$ , possiamo trovarci di fronte ad un **anello** se  $(A, \perp)$  è un gruppo abeliano e  $\top$  è associativa e distributiva rispetto a  $\perp$ . Se esiste elemento neutro rispetto a  $\top$ , allora, si dice **anello unitario**. Se, invece,  $\top$  è commutativa, allora è **anello commutativo**. Un qualsiasi anello unitario  $(A, \perp, \top)$  si chiama **corpo** se, ogni elemento diverso dall'elemento neutro di  $\perp$  è simmetrizzabile rispetto a  $\top$ . Se  $\top$  è anche commutativa, allora è un **campo**. Consideriamo la struttura algebrica  $(A, \perp)$ . Una parte  $X$  di  $A$  è detta **stabile** rispetto a  $\perp$  se, da  $x, y \in X$ , segue  $x \perp y \in X$ . Siano  $(A, \perp)$  e  $(B, \top)$  due strutture algebriche. Una funzione  $f : A \rightarrow B$  è detta **omomorfismo** di  $(A, \perp)$  in  $(B, \top)$  se abbiamo che  $f(x \perp y) = f(x) \top f(y)$ . Parlando di funzioni, se ci troviamo di fronte ad un omomorfismo iniettivo, allora avremo un **monomorfismo**, mentre se è suriettivo, sarà un **epimorfismo**. In caso di omomorfismo biettivo, allora ci sarà un **isomorfismo**, mentre se l'omomorfismo è definito sulla struttura stessa, ci sarà un **endomorfismo**.



# Elementi di Aritmetica

↗ Project	<b>+ Matematica Discreta</b>
☒ Done	<input checked="" type="checkbox"/>
Σ Due Status	Done!
Σ Current Task	

Abbiamo visto che, per dimostrare il principio di induzione in  $\mathbb{N}$ , sia necessario un **buon ordinamento** dell'insieme, cioè che ogni sottoinsieme non vuoto di  $\mathbb{N}$  ammetta, di fatto, un **minimo**. Durante questo studio, siamo giunti a determinare la struttura e la costruzione dell'insieme di numeri naturali. In aiuto di tale problema, assumiamo un approccio assiomatico, introducendo gli **assiomi di Peano**. Sia  $(N, o, s)$  una terna in cui  $N$  è un insieme,  $o$  è un elemento di  $N$  e  $s : N \rightarrow N$  è una funzione. All'interno di questa terna, valgono alcune proprietà:

1.  $s$  è una funzione iniettiva
2.  $o$  non appartiene all'insieme immagine di  $s$ .
3. Se  $M \subseteq N$  ha la proprietà che  $o \in M$  e  $s(x) \in M \forall x \in M$ , allora  $M = N$ .

Asseriamo facilmente che, la terza proprietà equivale al principio di induzione. Quest'ultimo è anche dotato di una **seconda forma**, fondamentale nello studio dell'aritmetica e che ora andremo a stilare. Sia data, per ogni  $n \in \mathbb{N}$ , con  $n \geq n_0$ , una proposizione  $P(n)$ . Se sono soddisfatte le seguenti condizioni:

- $P(n_0)$  è vera
- per ogni  $n > 0$  e per ogni  $h$ , con  $n_0 \leq h \leq n$ , allora  $P(n) \Rightarrow P(h)$

Allora  $P(n)$  sarà vera per ogni  $n \geq n_0$ . Per quanto si tratti di una generalizzazione della prima forma, risulta più complessa, perché bisognerà verificare due condizioni al passo induttivo. Un altro importante teorema che trae profitto dal principio di induzione all'interno dell'aritmetica elementare, è l'**algoritmo euclideo della divisione**.

- **T.H.** = siano  $a, b \in \mathbb{Z}$ , con  $b \neq 0$ . Allora esistono, e sono univocamente determinati, due interi  $q, r \in \mathbb{Z}$ , ossia **quoziente** e **resto**, in modo tale che  $a =$

$bq + r$ , con  $0 \leq r \leq |b|$ .

Da qui deriva il concetto di **divisibilità tra interi**. Dati due  $a, b \in \mathbb{Z}$ , diremo che  $a$  divide  $b$ , oppure  $b$  è divisibile per  $a$ ,  $a|b$ , se esiste almeno un elemento  $c \in \mathbb{Z}$ , tale che  $ac = b$ . Una struttura algebrica molto importante all'interno numeri interi, è l'esistenza di un **massimo comune divisore**,  $MCD$ .

- **T.H.** = siano  $a, b \in \mathbb{Z}$ . Un elemento  $d \in \mathbb{Z}$  si dice  $MCD$  tra  $a$  e  $b$  se  $d|a$  e  $d|b$  e ogni elemento  $e \in \mathbb{Z}$ , che soddisfa  $e|a$  e  $e|b$ , soddisfa anche  $e|d$ . Alcuni casi particolari prevedono:
  - $MCD(0, 0) = 0$ ;
  - $MCD(a, 0) = a$ ;
  - siano  $a, b, q, r \in \mathbb{Z}$ , tali che  $a = bq + r$ . Allora, se esiste  $MCD(b, r)$ , esiste anche  $MCD(a, b)$  e si ha  $MCD(a, b) = MCD(b, r)$ .

L'ultima proprietà definita, ci consente di stilare una strategia piuttosto efficace per trovare l' $MCD$  tra due numeri. Potremo eseguire la divisione euclidea  $a = bq + r$  e sostituire la coppia  $(a, b)$  con quella  $(b, r)$ . Così, renderemo il secondo elemento della coppia più piccolo di quello della coppia precedente. Reiterando in più passi questa procedura otterremo una coppia del tipo  $(n, 0)$  che possiede sicuramente un  $MCD$ , la cui determinazione è immediata. Vediamo un esempio.

- **ES** = vogliamo determinare l' $MCD$  tra 1001 e 273. Possiamo effettuare la divisione euclidea e otterremo:  $1001 = 3 \cdot 273 + 182$ , dove 3 è il quoziente della divisione tra 1001 e 273, mentre 182 è quanto ci manca tra  $819(3 \cdot 273)$  per raggiungere 1001. Quindi potremo scrivere  $MCD(1001, 273) = MCD(273, 182)$ . Continuiamo:  $273 = 1 \cdot 182 + 91$ , quindi  $MCD(273, 182) = MCD(182, 91)$ .  $182 = 2 \cdot 91 + 0$ , quindi  $MCD(91, 0)$  che è, ovviamente, 91. Per cui, l' $MCD(1001, 273)$  è 91.

Da questa procedura, deriva un teorema molto importante, detto **teorema di Bézout**.

- **T.H.** = siano  $a, b \in \mathbb{Z}$  e sia  $d = MCD(a, b)$ . Allora esistono  $v, w \in \mathbb{Z}$  tali che  $d = av + bw$ . In particolare, se  $a$  e  $b$  sono coprimi, esistono  $v, w \in \mathbb{Z}$  tali che  $1 = av + bw$ .

Partendo dall'esempio precedente, possiamo facilmente ricavare questi due coefficienti moltiplicativi dalla formula:

- $91 = 1 \cdot 273 - 1 \cdot 182 = 1 \cdot 273 - 1 \cdot (1 \cdot 1001 - 3 \cdot 273) = -1 \cdot 1001 + 4 \cdot 273$

Da queste definizioni che abbiamo appena dato, possiamo facilmente evincerne altre. Un intero  $p \in \mathbb{Z}$  si dice primo se  $p \neq \pm 1$  e  $D(p) = \{1, -1, p, -p\}$ . In parole più semplici, un numero è **primo** solo se è divisibile per uno e per se stesso. Inoltre, due numeri,  $a, b$ , sono detti **coprimi** se  $MCD(a, b) = 1$ . Posti questi paletti, possiamo parlare di un argomento fondamentale del corso, ossia le **congruenze**. Sia  $m$  un intero e si consideri in  $\mathbb{Z}$  la relazione  $m\mathbb{Z}$ , definita ponendo, con  $a, b \in \mathbb{Z}$ :

- $a(m\mathbb{Z})b : \iff \exists k \in \mathbb{Z} : a - b = mk.$

Concludiamo che la congruenza è una relazione di equivalenza, compatibile con le operazioni  $+$  e  $\cdot$  in  $\mathbb{Z}$ .

- **DIM** = essendo una relazione di equivalenza, dobbiamo dimostrare che sia riflessiva, simmetrica e transitiva. Per ogni  $a \in \mathbb{Z}$ , da  $m|0$  segue che  $m|a - a$ , quindi è verificato. Sia ora  $a(m\mathbb{Z})b$ , allora  $m|a - b$  e, per la proprietà del divide, vale anche  $m|b - a$ . Anche questo, è verificato. Ora, supposto  $a(m\mathbb{Z})b$  e  $b(m\mathbb{Z})c$ , segue che  $m|a - b$  e  $m|b - c$ . Sempre rifacendoci alle proprietà del divide, segue automaticamente che  $m|a - c$ . E verifichiamo anche la transitività.

Da questa definizione giustifica il termine di **congruenza modulo  $m$** . Infatti,  $m\mathbb{Z}$  si può tranquillamente scrivere  $a \equiv b \pmod{m}$ . La classe di equivalenza modulo  $m\mathbb{Z}$  di un qualunque  $x \in \mathbb{Z}$  viene denotata con  $[x]_m$ . L'insieme quoziante viene detto **insieme degli interi modulo  $m$** . Dal concetto di congruenza deriva quello di **congruenza lineare**. Una congruenza lineare nell'incognita  $x$  è un'equazione del tipo:

- $ax \equiv b \pmod{n}$ , con  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ ;

Le congruenze lineari sono molto utili, perché ci permettono di trovare soluzioni di un'equazione lineare tramite le congruenze. Infatti, l'esempio che abbiamo scritto sopra equivale a  $ax + ny = b$ . Questa equazione può ammettere soluzioni intere nelle incognite  $x$  e  $y$ , ma come facciamo ad averne la certezza? Diremo che una congruenza lineare del tipo  $ax \equiv b \pmod{n}$  ammette una o più soluzioni intere se l'  $MCD(a, n)$  è un divisore di  $b$ , quindi  $(a, n)|b$ . Per esempio, se dovessimo avere  $4x \equiv 7 \pmod{3}$ , ci basterà calcolare  $MCD(4, 3)$ , vedere che è uguale ad 1 e constatare che  $1|7$ . In questo caso, diremo che la congruenza è **compatibile**. Abbiamo detto che la congruenza è una relazione di equivalenza. Quindi, è possibile

suddividere l'insieme  $\mathbb{Z}$  in classi di equivalenza, ciascuna delle quali contiene tutti i numeri interi congrui tra loro modulo  $n$ . Quindi, la soluzione di una congruenza lineare sarà del tipo  $k \cdot \alpha$ , dove  $k$  è uguale a  $\frac{b}{d}$ , e a sua volta  $d$  rappresenta l' $MCD(a, n)$ .  $\alpha$ , invece, è il primo dei coefficienti di Bézout. Per avere chiaro il metodo di risoluzioni delle congruenze lineari, ci basterà vedere un chiaro esempio.

- **ES** = vogliamo determinare le soluzioni intere dell'equazione  $84x \equiv 108 \pmod{500}$ .
  - La prima cosa da fare è calcolare  $MCD(500, 84)$  e, per farlo, useremo l'algoritmo euclideo della divisione:
 
$$\begin{aligned} 500 &= 84 \cdot 5 + 80 \\ 84 &= 80 \cdot 1 + 4 \\ 80 &= 4 \cdot +0 \end{aligned}$$
 Ovviamente, l' $MCD(500, 84) = 4$
  - Notiamo che  $4|108$  e, quindi, la congruenza è compatibile. In questo momento, possiamo dividere l'intera equazione per 4, per avere a che fare con numeri più bassi. Lavoreremo su  $21x \equiv 27 \pmod{125}$ .
  - Nonostante sappiamo che l'equazione è compatibile, dobbiamo comunque rifare l'algoritmo euclideo della divisione, poiché ci servono i coefficienti di Bézout.
 
$$\begin{aligned} 125 &= 21 \cdot 5 + 20 \\ 21 &= 20 \cdot 1 + 1 \\ 20 &= 1 \cdot 20 + 0 \end{aligned}$$
 Necessitiamo di  $\alpha$  e possiamo ricavarla dalla formula  $d = \alpha \cdot a + \beta \cdot n$ . Nel nostro caso  $1 = \alpha \cdot 21 + \beta \cdot 125$ . Spostando i termini da destra a sinistra ci troveremo qualcosa del tipo  $1 = 21 + 20(-1)$ . Il 21 va bene, dobbiamo solo ricavarci il 125. Riscriviamo l'espressione sostituendo il 20, quindi  $21 + (125 + 21(-5))(-1) = 21 + 125(-1) + 21(5) = 21(6) + 125(-1)$ . Quindi, la nostra  $\alpha$  è 6. Banalmente, troviamo anche  $k$ , che è uguale a  $\frac{27}{1}$ . Allora  $k \cdot \alpha = 27 \cdot 6 = 162$ .
  - Diremo che 162 è una soluzione e che tutte le soluzioni costituiscono la classe di equivalenza  $[162]_{125}$ , che a sua volta è uguale a  $[37]_{125}$ , cioè il resto tra 162 e 125.

Spesso potremo trovarci di fronte ad un sistema di congruenze lineari. Esso ammette soluzioni quando tutte le congruenze sono compatibili ed esiste almeno un numero intero  $x$  che soddisfa ogni congruenza lineare.

- $$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \dots \\ a_nx \equiv b_n \pmod{n_n} \end{cases}$$

Per verificare la compatibilità di un sistema di congruenze lineari, possiamo ricorrere al **teorema cinese del resto**, che ci fornisce una condizione sufficiente affinché un sistema ammetta soluzioni. Prendendo l'esempio di sopra, gli  $n_n$  sono a due a due coprimi, nel senso che il loro  $MCD$  è uguale ad 1. Invece, i  $b_n$  sono degli interi qualsiasi. Il teorema ci garantisce che, di fronte ad un sistema di questo tipo, sono ammesse soluzioni. Attenzione: il teorema ci garantisce una soluzione sufficiente, ma non necessaria. Vale a dire che, pur non avendo i moduli a due a due coprimi, qualche volta potremo trovarci di fronte ad un sistema che ammette comunque soluzioni. Esistono, fondamentalmente, due modi per risolvere un sistema di congruenze lineari. Vediamo il primo con un esempio.

- **ES** = troviamo le soluzioni per questo sistema.

- $$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases}$$

- Fatto questo, andiamo a creare quattro variabili.

$$N = 5 \cdot 7 \cdot 11 = 385$$

$$N_1 = 7 \cdot 11 = 77$$

$$N_2 = 5 \cdot 11 = 55$$

$$N_3 = 7 \cdot 5 = 35$$

- Ora, riscriviamo un nuovo sistema.

$$\begin{cases} 77x \equiv 1 \pmod{5} \\ 55x \equiv 1 \pmod{7} \\ 35x \equiv 1 \pmod{11} \end{cases}$$

- Procedendo per passi, scriviamo ogni equazione sotto questa forma.

1.  $77x - 1 = 5k$

Generalmente, qui procediamo ad occhio. Per individuare la  $x$ , partiamo dall'1, numero minimo e sostituiamo fino a quando non troveremo il più piccolo numero che, sostituendo, dia un numero che divide 5. Per esempio, 1 non va bene, perché  $77 \cdot 1 - 1 = 76$ , che non divide 5.

Per lo stesso motivo, non va bene neanche 2, poiché  $77 \cdot 2 - 1 = 153$

, che non divide 5. Troveremo che il 3 va bene, perché  $77 \cdot 3 - 1 = 230|5$ . Andiamo a salvare il 3 in una variabile  $S_1 = 3$ .

### 2. $55x - 1 = 7k$

Procediamo alla stessa maniera, trovando il 6 come primo numero disponibile, dato che  $55 \cdot 6 - 1 = 329|7$ . Salviamolo in una variabile  $S_2 = 6$ .

### 3. $35x - 1 = 11k$

Rapidamente, verifichiamo che la  $x$  può essere sicuramente 6, perché  $35 \cdot 6 - 1 = 209|11$ . Salviamolo in una variabile  $S_3 = 6$ .

- La nostra soluzione sarà data da questa somma di prodotti. La  $B$  si riferisce, ovviamente, agli interi  

$$(N_1 \cdot B_1 \cdot S_1) + (N_2 \cdot B_2 \cdot S_2) + (N_3 \cdot B_3 \cdot S_3) =$$
  

$$(77 \cdot 3 \cdot 3) + (55 \cdot 3 \cdot 6) + (35 \cdot 9 \cdot 6) = 3573$$
- Quindi, la soluzione espressa in classi di equivalenza sarà  $[3573]_{385}$ , con 385 prodotto dei moduli. A sua volta, la soluzione generica, sarà  $[108]_{385}$  perché  $3573 = 385 \cdot 9 - 108$ .

Come abbiamo visto, questa scelta potrebbe essere un po' complessa, dato che bisogna procedere per iterazioni e potremo dover effettuare molti calcoli in più. Per questo, individuiamo una seconda tecnica, totalmente analoga, ma faremo un esempio su un sistema più semplice.

- **ES** = troviamo le soluzioni di questo sistema.
  - $\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4} \end{cases}$
  - Partiamo dalla prima equazione, possiamo scriverla in questo modo.  
 $x = 4 + 5k$ , con  $k \in \mathbb{Z}$
  - Imponiamola come soluzione della seconda equazione. La seconda equazione che otteniamo è un semplice spostamento da sinistra a destra.  
 $4 + 5k \equiv 3 \pmod{4} \rightarrow 5k \equiv -1 \pmod{4}$
  - Data la necessità di dover ottenere per forza un numero compreso tra 0 e  $n - 1$ , andiamo a sommare il modulo fino a quando non lo otteniamo, quindi  $-1 + 4 = 3$ .  
 $5k \equiv 3 \pmod{4}$

- Essendo una congruenza lineare, possiamo andare a risolverla col meccanismo che già conosciamo. Vediamo ad occhio che  $MCD(5, 4) = 1$ , ma è meglio scrivere i passi dell'algoritmo per trovare più facilmente i coefficienti di Bézout.

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0$$

- Mettendo in evidenza, troviamo i nostri coefficienti

$$1 = 1 \cdot 5 - 4$$

- La nostra  $\alpha$  è uguale a 1, quindi.

$$k = b \cdot v \rightarrow k = 1 \cdot 3 \rightarrow k = 3$$

- Sostituiamo la  $k$

$$4 + 5 \cdot 3 = 19$$

- La classe di equivalenza delle soluzioni è, quindi,  $[19]_{20}$ .

Ovviamente, ci fossero state più di due equazioni, dovevamo ripetere la procedura, impostando la classe di equivalenza come  $19 + 20k$ , con  $k \in \mathbb{Z}$ .

In ambito di questo capitolo, acquisisce una particolare importanza la **funzione di Eulero**, spesso indicata con  $\varphi(n)$ , con  $n$  un qualsiasi intero maggiore di 0. Essa identifica il numero degli interi positivi minori di  $n$  e coprimi con  $n$ . Essa mi permette di trovare numeri coprimi di un numero qualsiasi  $n$ . Ad esempio,  $\varphi(20) = 8$ , perché i numeri minori di 20 coprimi tra loro sono 1, 3, 7, 9, 11, 13, 17 e 19, dato che andando a fare l' $MCD$  a due a due, esso sarà sempre uguale ad 1. Una proprietà molto interessante della  $\varphi$  è la proprietà moltiplicativa, che mi permette la fattorizzazione in numeri coprimi. Se due numeri,  $k$  e  $j$ , sono coprimi tra loro, allora vale questa proposizione.

- $\varphi(k \cdot j) = \varphi(k) \cdot \varphi(j)$

Ovviamente, questo vale anche se i fattori sono più di due, cioè per esempio  $k$ ,  $j$  e  $i$ . In questo caso, devono comunque essere a due a due coprimi. Rifacendoci all'esempio precedente,  $\varphi(20)$ , possiamo scomporlo in due fattori tra loro coprimi, come 4 e 5, quindi  $\varphi(4 \cdot 5)$ . Seguendo la proposizione, allora  $\varphi(4) \cdot \varphi(5)$ . Da qui, è relativamente più semplice, perché  $\varphi(4) = 2$ , quindi 1 e  $\varphi(5) = 4$ . Allora  $\varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$ . Ci troviamo il numero precedente, avendo semplificato notevolmente i calcoli.

La funzione di Eulero gode anche di un'altra importante proprietà che può venirci in aiuto. Se un numero intero  $p$  è un numero primo, allora  $\varphi(p)$  è uguale:

- $\varphi(p^x) = p^x - p^{x-1}$

Così facendo, scomponendo un numero in fattori primi, possiamo velocizzare ulteriormente il procedimento. La funzione di Eulero permette di applicare il **piccolo teorema di Fermat** anche al modulo di un numero non primo.

- **T.H.** = sia  $p$  un numero primo e l'intero  $a$  non è un multiplo di  $p$ , allora  $a^p - 1 \equiv 1 \pmod{p}$ .

Tuttavia, come dice il teorema, esso è applicabile solo ai numeri primi. Sostituendo  $p$  con la funzione di Eulero  $\varphi(n)$ , otteniamo il **teorema di Fermat-Eulero**.

- **T.H.** = dati due numeri interi coprimi  $a$  e  $n$ , il numero intero elevato alla funzione di Eulero  $\varphi(n)$  è congruo ad 1 modulo  $n$ , quindi  $a^{\varphi(n)} \equiv 1 \pmod{n}$ , che posso, quindi, usare con un qualsiasi positivo  $n$ .



# Algebra delle Matrici

↗ Project	<a href="#">Matematica Discreta</a>
☑ Done	
Σ Due Status	Done!
Σ Current Task	

Una matrice è una tabella rettangolare le cui entrate sono organizzate in **righe** orizzontali e **colonne** verticali.

$$\bullet \quad A = \begin{pmatrix} 1 & 2 \\ 4 & 0 \\ 3 & -1 \end{pmatrix}$$

Questa matrice, con tre righe e due colonne, si dice che ha **taglia**  $3 \cdot 2$ . Un'altra matrice come questa:

$$\bullet \quad B = \begin{pmatrix} 3 & 0 & 1 \\ 2 & 5 & -1 \\ 1 & 4 & 2 \end{pmatrix}$$

$B$  si dice matrice **quadrata**, avendo lo stesso numero di righe e di colonne. Quella di sopra, invece, è **rettangolare**. Le entrate di una matrice sono detti **elementi**. Le matrici sono generalmente denotate con una lettera maiuscola. Per individuare la posizione di un elemento in una matrice, si usano due indici che specificano in quale riga e in quale colonna esso si trova.

$$\bullet \quad \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1p} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2p} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3p} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{np} \end{pmatrix}$$

Gli elementi  $a_{11}, a_{22}, a_{33}$  si dicono **elementi diagonali**. Una matrice di taglia  $n \cdot n$  si dice quadrata di ordine  $n$ . Gli elementi diagonali formano la **diagonale principale**. Durante lo studio, prenderemo solo matrici che appartengono all'insieme dei numeri reali, che è un **campo**, una struttura algebrica che abbiamo già visto. L'insieme delle

matrici quadrate di ordine  $n$  ad elemento nel campo  $K$ , si denota con  $M_n(K)$ . Le matrici di taglia  $1 \cdot n$  sono dette **matrici riga**, mentre quelle  $n \cdot 1$ , **matrici colonna**. Definiamo, ora, alcune operazioni che possiamo fare con le matrici. Se hanno la stessa taglia, possiamo effettuare la **somma di matrici**. È relativamente semplice, infatti basta sommare gli indici corrispondenti e creare una nuova matrice somma.

$$\bullet \text{ ES} = \begin{pmatrix} 1 & 0 & 2 \\ 3 & -1 & 4 \end{pmatrix} + \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1+0 & 0+1 & 2-1 \\ 3+2 & -1+0 & 4+3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 5 & -1 & 7 \end{pmatrix}$$

Un'altra operazione importante è la **moltiplicazione per uno scalare**. Spesso, potrebbe essere utile moltiplicare una matrice per un numero qualsiasi. Basterà, ancora una volta, moltiplicare quel numero per ogni elemento della matrice e trasferire tutto in una nuova matrice risultante.

$$\bullet \text{ ES} = 5 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 5 \cdot 1 & 5 \cdot 2 \\ 5 \cdot 3 & 0 \\ 5 \cdot (-1) & 5 \cdot 1 \end{pmatrix} = \begin{pmatrix} 5 & 10 \\ 15 & 0 \\ -5 & 5 \end{pmatrix}$$

La terza operazione che definiamo è il **prodotto riga per colonna**. Qui non è necessario che le matrici abbiano la stessa taglia, ma il numero di colonne di un'ipotetica matrice  $A$ , deve avere lo stesso numero di righe di un'ipotetica matrice  $B$ . Se  $A$  ha taglia  $n \cdot p$ , allora  $B$  dovrà per forza essere  $p \cdot m$ . Il risultato sarà una nuova matrice risultante, che avrà le stesse colonne di  $A$  e le stesse righe di  $B$ .

$$\bullet \text{ ES} = A \cdot B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \end{pmatrix} \cdot \begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ -6 & 3 \end{pmatrix}$$

Possiamo definire diversi tipi di matrici:

- **matrice diagonale**: è una matrice quadrata in cui gli elementi sono tutti nulli ad esclusione di quelli posti sulla diagonale principale. Questo tipo di matrice ha anche una variante, detta **matrice antidiagonale**, dove gli elementi sono tutti posti sull'antidiagonale.
- **matrice identica**: spesso indicata con  $Id_n$ , è una matrice diagonale che ha tutti 1 sulla diagonale principale.
- **matrice nulla**: una matrice di dimensione qualsiasi con tutti gli elementi nulli.
- **matrice triangolare**: possiamo distinguere la **matrice triangolare superiore**, i cui elementi sotto la diagonale principale sono tutti nulli e la **matrice triangolare inferiore**, i cui elementi sopra la diagonale principale sono tutti nulli.

**inferiore**, i cui elementi nulli sono al di sopra della diagonale principale.

- **matrice a scala**: una qualsiasi matrice è detta a scala se il primo elemento diverso da 0 nella riga  $i$ -esima, è più a destra del primo elemento diverso da zero della riga precedente. Il primo elemento non nullo di ogni riga è detto **pivot**. Ogni matrice può essere ridotta a scala e ne esistono vari metodi. Li vedremo successivamente.
- **matrice simmetrica**: una matrice quadrata si dice simmetrica se i suoi elementi sono simmetrici rispetto alla diagonale principale.

Prima abbiamo definito una matrice a scala. Com'è fatta? Più o meno così:

$$\bullet \quad A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Come abbiamo già detto, una qualsiasi matrice può essere ridotta a scala e, per farlo, utilizzeremo l'**algoritmo di eliminazione gaussiana**. Entriamo un po' più nel dettaglio. Consideriamo una matrice a componenti reali, quindi  $A \in \mathbb{R}^{m,n}$  e indichiamo con  $R_1, R_2, \dots, R_m$  le sue righe. Per ridurla a scala, ci rifacciamo alle cosiddette **mosse di Gauss**, che sono sostanzialmente tre:

- scambiare due righe
- moltiplicare una riga della matrice per uno scalare non nullo
- sostituire una riga della matrice con quella ottenuta sommando ad essa un multiplo di un'altra riga.

L'algoritmo di Gauss ha dei passi da seguire, considerando una qualsiasi matrice  $A$  con  $m$  righe ed  $n$  colonne:

1. Sia  $C_k$ , con  $1 \leq k \leq n$ , la prima colonna a partire da sinistra che contiene almeno un termine  $a$  non nullo. In questo caso, possono presentarsi due eventualità. Se  $a$  non è un elemento di  $R_1$ , scambiamo la riga che contiene  $a$  con  $R_1$ . Altrimenti, proseguiamo.
2. Siamo di fronte all'eventualità che  $a$  è un elemento di  $R_1$ , quindi dobbiamo annullare tutti gli elementi della  $k$ -esima colonna al di sotto di  $a$ . Sostituiamo ogni riga  $R_i$  con  $R_i + \lambda R_1$ . Lo scalare viene scelto in modo che possa annullare la riga.
3. Nel caso la matrice risultante risulti a scala, allora abbiamo finito, altrimenti, ricominciamo da capo.

Questa definizione può sembrare complicata, per questo vedremo un pratico esempio.

- **ES** = Prendiamo in considerazione una matrice, non a scala, ma che vogliamo ridurla.

$$\circ \begin{pmatrix} -2 & 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & -1 & -1 \\ 0 & 1 & 1 & 0 & 0 \\ -3 & 0 & 1 & -1 & 0 \end{pmatrix}$$

- Ad occhio, vediamo già una riga completamente nulla e, sapendo che al di sotto della riga nulla non può esserci una riga non nulla, possiamo effettuare uno scambio,  $R_2 \Leftrightarrow R_5$ .

$$\begin{pmatrix} -2 & 0 & 3 & 1 & 0 \\ -3 & 0 & 1 & -1 & 0 \\ 1 & 0 & 1 & -1 & -1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- Vediamo come il  $-3$  non vada bene, dato che l'elemento al di sotto del pivot  $-2$  deve essere nullo. Non avendo altre carte veloci a disposizione, andiamo a moltiplicare la riga per uno scalare.  $R_2 = R_2 + \lambda R_1$ . In parole povere, devo trovare un numero che, moltiplicato per  $-2$ , mi annulli il  $-3$  sommando. In questo caso, il numero designato è  $-\frac{3}{2}$ . Quindi  $-3 + (\frac{3}{2} \cdot 2) = 0$ . Dovremo poi, andare a moltiplicare ogni numero della riga.

Otterremo una cosa del genere.

$$\begin{pmatrix} -2 & 0 & 3 & 1 & 0 \\ 0 & 0 & -\frac{7}{2} & -\frac{5}{2} & 0 \\ 1 & 0 & 1 & -1 & -1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- Notiamo come la seconda riga vada bene, ma la terza no. Ci tocca annullare 1. Facciamo una cosa analoga, andando ad individuare uno scalare che possa annullare 1.  $R_3 = R_3 + \lambda R_1$ . Il numero scelto è  $\frac{1}{2}$ . Otterremo

questa matrice.

$$\begin{pmatrix} -2 & 0 & 3 & 1 & 0 \\ 0 & 0 & -\frac{7}{2} & -\frac{5}{2} & 0 \\ 0 & 0 & \frac{5}{2} & -\frac{1}{2} & -1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- Adesso, notiamo come  $R_4$  possa andare benissimo sotto  $R_1$ , quindi conviene, in questo caso, scambiare.  $R_2 \leftrightarrow R_4$ .

$$\begin{pmatrix} -2 & 0 & 3 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & -\frac{7}{2} & -\frac{5}{2} & 0 \\ 0 & 0 & \frac{5}{2} & -\frac{1}{2} & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- L'ultima cosa da fare è, adesso, annullare  $\frac{5}{2}$ , per poter avere una matrice a scala. Troviamo un numero che, moltiplicato per  $-\frac{7}{2}$ , annulli il  $\frac{5}{2}$ . Il numero designato è  $\frac{5}{7}$ .  $R_4 = R_4 + \lambda R_3$ .

$$\begin{pmatrix} -2 & 0 & 3 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & -\frac{7}{2} & -\frac{5}{2} & 0 \\ 0 & 0 & 0 & -3 & -\frac{7}{2} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- La matrice, ora, è correttamente ridotta a scala.

Di particolare importanza all'interno dell'algebra delle matrici è il determinante. Il determinante, indicato con  $\det(A)$ , è un numero associato solo ed esclusivamente a matrici quadrate, che ne esprime alcune proprietà algebriche e geometriche. In base all'ordine della matrice, abbiamo diversi modi per calcolarlo. In una matrice  $2 \cdot 2$ , il metodo è relativamente quello più semplice. Basta, infatti, moltiplicare gli elementi della diagonale e quelli dell'antidiagonale e poi sottrarli.

- ES** =  $\det(A) = \begin{pmatrix} 1 & 3 \\ 4 & 5 \end{pmatrix} = (1 \cdot 5) - (3 \cdot 4) = 5 - 12 = -7$

Quando ci troviamo, di fronte, ad una matrice  $3 \times 3$ , possiamo applicare la regola di Sarrus. È un po' più complesso, infatti bisogna sommare i prodotti della diagonale, più i due triangoli paralleli costruiti su di essa. Poi sommiamo i prodotti dell'antidiagonale e dei triangoli paralleli

costruiti su di essa. Calcoliamo la differenza tra i due risultati e troviamo il determinante. Sembra complicato, ma è più semplice del previsto.

- **ES** =  $\det(A) = \begin{pmatrix} 2 & -1 & 4 \\ 1 & 2 & 0 \\ 3 & 5 & 1 \end{pmatrix}$

- Procediamo per gradi. In questa matrice individuiamo la diagonale e i due triangoli paralleli ad essa. In rosso è segnata la diagonale, in verde e blu i triangoli.

$$\begin{pmatrix} 2 & -1 & 4 \\ 1 & 2 & 0 \\ 3 & 5 & 1 \end{pmatrix}$$

Facendo il calcolo, dovremo fare  $(2 \cdot 2 \cdot 1) + (4 \cdot 5 \cdot 1) + (-1 \cdot 0 \cdot 3) = 24$ .

- Rifacciamo il processo con l'antidiagonale, individuandone anche i triangoli paralleli.

$$\begin{pmatrix} 2 & -1 & 4 \\ 1 & 2 & 0 \\ 3 & 5 & 1 \end{pmatrix}$$

Rifacendo gli stessi calcoli,  $(4 \cdot 2 \cdot 3) + (-1 \cdot 1 \cdot 1) + (5 \cdot 0 \cdot 2) = 23$ .

- Sottraiamo  $24 - 23 = 1$ . Allora  $\det(A) = 1$ .

Ovviamente, non sempre la nostra matrice sarà di ordine 2 o 3 e potremo comunque voler calcolare il suo determinante. In questo caso, ci viene in aiuto il **teorema di Laplace** che, attraverso sviluppi ricorsivi, detti **sviluppi di Laplace**, tra righe e colonne, permette di calcolare il determinante. Considerata una matrice quadrata di ordine  $n$ , denotiamo con  $A_{ij}$  la matrice che si ottiene eliminando la riga  $i$  e la colonna  $j$  della matrice  $A$  e con  $\det(A_{ij})$  il suo determinante. Fissato un qualsiasi elemento  $a_{ij}$  della matrice, chiamiamo **complemento algebrico** il numero  $(-1)^{i+j} \cdot \det(A_{ij})$ . Il determinante di questa matrice non sarà altro che la somma dei prodotti degli elementi della riga per i rispettivi complementi algebrici. Lo sviluppo può avvenire sia per righe che per colonne, possiamo scegliere arbitrariamente una riga o una colonna. Generalmente, però, conviene scegliere la riga e la colonna con più zeri, in modo da risparmiare notevolmente i calcoli. Anche qui, vedremo un esempio.

- **ES** =  $\det(A) = \begin{pmatrix} 1 & 0 & 5 \\ 2 & -1 & 0 \\ 7 & -2 & 0 \end{pmatrix}$

- Ad un primo sguardo, ci conviene scegliere la terza colonna, che ha due zeri, quindi dovremo calcolare un unico complemento algebrico.

$$a_{13} = (-1)^{1+3} \cdot \det \begin{pmatrix} 2 & -1 \\ 7 & -1 \end{pmatrix} = 1 \cdot [2 \cdot (-1) - (-1) \cdot 7] = 1 \cdot 3 = 3$$

- Non ci resta che moltiplicare il complemento algebrico per il nostro  $a_{13}$ , quindi  $3 \cdot 5 = 15$ , allora  $\det(A) = 15$ .

Il determinante gode di alcune proprietà. Se siamo di fronte a due matrici dello stesso ordine, in cui è possibile fare il prodotto riga per colonna, il **teorema di Binet** dice che:

- **T.H.** =  $\det(AB) = \det(A) \cdot \det(B)$ , cioè il determinante del prodotto è uguale al prodotto dei determinanti.

Data una matrice invertibile, il determinante della matrice inversa è il reciproco del determinante della matrice di partenza, cioè  $\det(A^{-1}) = \frac{1}{\det(A)}$ . Una matrice quadrata e la sua trasposta hanno lo stesso determinante.

Prima di andare avanti, dobbiamo definire alcuni concetti. Sia  $A$  una matrice qualsiasi di ordine almeno 1. Si dicono **sottomatrici** di  $A$  tutte quelle matrici estratte da  $A$  eliminando un numero arbitrario di righe e/o colonne. Si definisce **minore** della matrice  $A$ , il determinante di una sottomatrice quadrata di  $A$ . L'ordine della sottomatrice è detto **ordine del minore**.

- **ES** =  $A = \begin{pmatrix} 2 & 1 & 4 \\ -1 & 0 & -2 \\ 3 & 6 & 5 \\ -4 & 7 & -3 \end{pmatrix}$

Da questa matrice, possiamo estrarre un minore di ordine 3.

- $\det \begin{pmatrix} -1 & 0 & -2 \\ 3 & 6 & 5 \\ -4 & 7 & -3 \end{pmatrix} = -37$

Ma anche un minore di ordine 2.

- $\det \begin{pmatrix} 3 & 6 \\ -4 & 7 \end{pmatrix} = 45$

Data una matrice  $A$ , quadrata o rettangolare, estraiamo una sottomatrice quadrata di ordine  $p$  e chiamiamola  $A'$ . Si definisce **minore orlato** il determinante di ogni sottomatrice quadrata di  $A$  di ordine  $p + 1$ , ottenuta dalla sottomatrice  $A'$  aggiungendo una riga e una colonna di  $A$ . Anche qui, sembra complicato, ma facciamo un pratico esempio.

- **ES** =  $A = \begin{pmatrix} 2 & 1 & -1 & 3 \\ 1 & 2 & 1 & 0 \\ 5 & 4 & 7 & -2 \end{pmatrix}$

Estraiamo una sottomatrice di ordine  $p = 2$ .

- $A' = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$

Detto ciò, costruiamo due sottomatrici quadrate di  $A$  che si ottengono da  $A'$  aggiungendo una riga e una colonna.

- $\begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 1 \\ 5 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 5 & 4 & -2 \end{pmatrix}$

I determinanti di queste sottomatrici, ossia 24 e  $-24$ , sono detti minori orlati  $A'$ .

Una matrice quadrata  $A$  di ordine  $n$  è detta **matrice invertibile** se esiste una matrice quadrata dello stesso ordine della matrice  $A$ , solitamente indicare con  $A^{-1}$  tale che il prodotto riga per colonna tra le due matrici restituisca la matrice identica di ordine  $n$ .  $A^{-1}$  è detta matrice inversa. Una matrice è invertibile se e solo se il suo determinante è diverso da zero. Per calcolare la matrice inversa, ci rifacciamo ai concetti di minore complementare e complemento algebrico, che per semplicità chiameremo **cofattore**. Sarebbe inutile dilungarsi in spiegazioni, quindi andiamo a commentare passo passo un esempio.

- **ES** =  $A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 3 \\ 1 & 4 & 2 \end{pmatrix}$

Risparmiamoci i calcoli sul determinante, lo sappiamo già fare, usando Sarrus o Laplace, si ottiene  $\det(A) = -5 \neq 0$ . Va bene, la matrice è invertibile, quindi possiamo proseguire a calcolare l'inversa. Il secondo punto è quello di calcolare la matrice dei cofattori, cioè sostituire ogni elemento della matrice di partenza, col suo complemento algebrico.

- $Cof(a_{11}) = (-1)^{1+1} \cdot \det\left(\begin{pmatrix} -1 & 3 \\ 4 & 1 \end{pmatrix}\right) = 1 \cdot (-14) = -14$
- $Cof(a_{12}) = (-1)^{1+2} \cdot \det\left(\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}\right) = -1 \cdot (1) = -1$
- $Cof(a_{13}) = (-1)^{1+3} \cdot \det\left(\begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix}\right) = 1 \cdot (9) = 9$
- $Cof(a_{21}) = (-1)^{2+1} \cdot \det\left(\begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}\right) = -1 \cdot (-4) = 4$

$$Cof(a_{22}) = (-1)^{2+2} \cdot \det\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = 1 \cdot (1) = 1$$

$$Cof(a_{23}) = (-1)^{2+3} \cdot \det\begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix} = -1 \cdot (4) = -4$$

$$Cof(a_{31}) = (-1)^{3+1} \cdot \det\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix} = 1 \cdot (1) = 1$$

$$Cof(a_{32}) = (-1)^{3+2} \cdot \det\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = -1 \cdot (1) = -1$$

$$Cof(a_{33}) = (-1)^{3+3} \cdot \det\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} = 1 \cdot (-1) = -1$$

Effettuato questo passaggio, andiamo a formare una nuova matrice sostituendo ogni elemento di  $A$  col suo cofattore. Chiamiamo la nuova matrice  $A^C$ :

$$\circ A^C = \begin{pmatrix} -14 & -1 & 9 \\ 4 & 1 & -4 \\ 1 & -1 & -1 \end{pmatrix}$$

Fatto ciò, la trasponiamo, cioè scambiamo righe e colonne, creando un'ulteriore matrice, chiamata  $A^{CT}$ :

$$\circ A^{CT} = \begin{pmatrix} -14 & 4 & 1 \\ -1 & 1 & -1 \\ 9 & 4 & -1 \end{pmatrix}$$

Come ultimo passaggio, andiamo a moltiplicare questa matrice ottenuta per il reciproco del determinante:

$$\circ A^{CT} \cdot \frac{1}{\det(A)} = \begin{pmatrix} -14 & 4 & 1 \\ -1 & 1 & -1 \\ 9 & 4 & -1 \end{pmatrix} \cdot -\frac{1}{5}$$

Andremo ad ottenere una nuova matrice risultante, che sarà la nostra inversa:

$$\circ A^{-1} = \begin{pmatrix} \frac{14}{5} & -\frac{4}{5} & -\frac{1}{5} \\ \frac{1}{5} & -\frac{1}{5} & \frac{1}{5} \\ -\frac{9}{5} & \frac{4}{5} & \frac{1}{5} \end{pmatrix}$$

Calcolata l'inversa, sappiamo che andando a moltiplicarla per la matrice iniziale, il risultato sarà la matrice identica.

Passiamo, adesso, a definire il concetto di **rango** di una matrice. Il rango è una proprietà fondamentale nello studio delle applicazioni lineari. Il rango, spesso indicato con  $\rho(A)$  è un numero intero positivo associato ad una matrice  $A$ . Esistono varie definizioni, analoghe tra loro. Il rango può essere:

- massimo numero di righe o colonne linearmente indipendenti di  $A$ ;
- dimensione massima dell'immagine dell'applicazione lineare;
- l'ordine massimo dei minori non nulli che si possono estrarre da  $A$ ;
- il numero di pivot dopo aver ridotto a scala la matrice attraverso l'eliminazione gaussiana;

Prima di definire un possibile metodo per calcolare il rango di una matrice, facciamo alcune osservazioni. Una matrice rettangolare  $A$  con  $m$  righe ed  $n$  colonne ha il rango compreso tra 0 e il minimo tra il numero di righe e colonne della matrice, quindi  $0 \leq \rho(A) \leq \min(m, n)$ . L'unica matrice con rango 0 è la matrice nulla. Nel caso in cui il rango coincida col minimo tra  $m$  ed  $n$ , diremo che la matrice ha **rango massimo**. Abbiamo detto che uno dei metodi per calcolare il rango della matrice, può essere l'eliminazione gaussiana. Riducendo a scala la matrice, il rango è uguale al numero dei pivot. Abbiamo già visto questo metodo e ne introduciamo uno più semplice e diretto che sfrutta il **teorema degli orlati**. Sia  $A$  una matrice con  $m$  righe ed  $n$  colonne e sia  $p \leq \min(m, n)$ . Il rango di  $A$  è uguale a  $p$  se e solo se esiste un minore non nullo di  $A$  di ordine  $p$ , e tutti i minori orlati di ordine  $p + 1$  sono nulli. Al pratico, è ancora più semplice, quindi vediamo immediatamente un esempio.

$$\bullet \text{ ES} = A = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 1 & -1 & 3 \\ 1 & 1 & 0 & 1 \\ -2 & 1 & 3 & -5 \end{pmatrix}$$

Per prima cosa, notiamo che è una matrice non nulla di ordine 4, quindi il rango sarà  $1 \leq \rho(A) \leq 4$ . Consideriamo una sottomatrice di ordine 2:

$$\circ \det \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -3 \neq 0$$

Il rango, quindi, non 1. Orliamo questa matrice con altre sottomatrici di ordine 3:

$$\circ \det \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & -1 \\ 1 & 1 & 0 \end{pmatrix} = 0$$

$$\det \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix} = 0$$

$$\det \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & -1 \\ -2 & 1 & 3 \end{pmatrix} = 0$$

$$\det \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 3 \\ -2 & 1 & 5 \end{pmatrix} = 0$$

Tutte e quattro le sottomatrici di ordine 3, ottenute orlando quella precedente di ordine 2, hanno determinante nullo. Quindi  $\rho(A) = 2$ .

Nel caso non avessimo trovato un determinante nullo, avremo dovuto continuare ad orlare una delle sottomatrici ottenendo matrici quadrate di ordine 4. Il processo si reitera fin quando è possibile orlare, cioè se la matrice di partenza aveva 4 righe, il rango non poteva essere 5, massimo 4. Per calcolare il rango, un metodo vale l'altro, ma quello degli orlati è il più diretto.

Abbiamo, ora, fatto un ampio excursus sulle matrici. Tutte queste definizioni ci servono per capire al meglio i metodi di risoluzione dei sistemi lineari. Prima di andare avanti, esistono varie tecniche di soluzione, ma ne vedremo solo una nel dettaglio, che è anche la più diretta. Un **sistema lineare** è un insieme finito di equazioni di primo grado. Un sistema lineare con  $m$  equazioni ed  $n$  incognite, si presenta generalmente in questa forma:

$$\bullet \quad \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{array} \right.$$

Gli scalari  $a_{ij}$  prendono il nome di **coefficienti** del sistema, mentre  $b_m$  si dicono **termini noti**. Si dice soluzione del sistema (\*) ogni  $n$ -upla di scalari  $(x_1, x_2, \dots, x_n)$  che soddisfa tutte le sue equazioni. Se un sistema lineare ammette almeno una soluzione, si dice **compatibile**, in caso contrario è **impossibile**. Se due o più sistemi hanno le stesse soluzioni, si dicono **equivalenti**. Se i termini noti sono tutti nulli, il sistema è detto **omogeneo**. Tutti i sistemi omogenei sono compatibili, infatti ammettono una **soluzione banale**. Alcuni metodi risolutivi dei sistemi lineari lavorano su alcune matrici associate al sistema. Una di queste è la **matrice dei coefficienti**, che si presenta nella forma:

$$\bullet \quad A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Nella forma completa, la matrice invece, assume questa forma:

$$\bullet \quad (A|b) = \left( \begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right)$$

Infine, abbiamo la matrice delle incognite:

$$\bullet \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Quindi, un sistema lineare ha la propria **forma matriciale**, scritta come  $Ax = b$ .

Esistono vari metodi di soluzione dei sistemi lineari. Esiste il **metodo di sostituzione** e il **metodo di Gauss-Jordan**, ma prima ci concentreremo sul **metodo di Cramer**, solo per i sistemi quadrati, vale a dire quelli in cui il numero di equazioni è uguale al numero delle incognite. Dato un sistema lineare di  $n \geq 1$  equazioni in  $n$  incognite e sia  $A$  la matrice incompleta ad esso associata e  $A_i$ , con  $i \in 1, 2, \dots, n$  le matrici ottenute sostituendo l' $i$ -esima colonna di  $A$  con la colonna dei termini noti del sistema. Se il determinante di  $A$  è diverso da zero, il sistema ammette un'unica soluzione  $(x_1, x_2, \dots, x_n)$  data da:

$$\bullet \quad x_1 = \frac{\det(A_1)}{\det(A)}, \quad x_2 = \frac{\det(A_2)}{\det(A)}, \dots, \quad x_n = \frac{\det(A_n)}{\det(A)}$$

Sembra complicato, ma vediamo un esempio pratico.

$$\bullet \quad \text{ES} = \begin{cases} 2x_1 + 6x_2 + 4x_3 = 1 \\ x_1 + 3x_2 + x_3 = 2 \\ -x_1 + x_2 + 2x_3 = 1 \end{cases}$$

Scriviamo prima la matrice incompleta:

$$\circ \quad A = \begin{pmatrix} 2 & 6 & 4 \\ 1 & 3 & -1 \\ -1 & 1 & 2 \end{pmatrix}$$

Senza soffermarci ulteriormente, notiamo che  $\det(A) = 24$ . Secondo Cramer, sappiamo che il sistema ammette un'unica soluzione e, quindi, dobbiamo calcolarci, in questo caso, i determinanti delle matrici  $A_1, A_2, A_3$ , sostituendo prima, seconda e terza colonna di  $A$  con la colonna dei termini noti:

$$\circ \ det(A_1) = \det \begin{pmatrix} 1 & 6 & 4 \\ 2 & 3 & -1 \\ 1 & 1 & 2 \end{pmatrix} = -27$$

$$det(A_2) = \det \begin{pmatrix} 2 & 1 & 4 \\ 1 & 2 & -1 \\ -1 & 1 & 2 \end{pmatrix} = 21$$

$$det(A_3) = \det \begin{pmatrix} 2 & 6 & 1 \\ 1 & 3 & 2 \\ -1 & 1 & 1 \end{pmatrix} = -12$$

Quindi, la soluzione del sistema sarà:

$$\circ \quad \begin{cases} x_1 = -\frac{27}{24} = -\frac{9}{8} \\ x_2 = \frac{21}{24} = \frac{7}{8} \\ x_3 = -\frac{12}{24} = -\frac{1}{2} \end{cases}$$



# Spazi Vettoriali

↗ Area	<a href="#">Studio</a>
↗ Project	<a href="#">Matematica Discreta</a>
☑ Done	
Σ Due Status	Done!
Σ Current Task	

Uno spazio vettoriale è una struttura algebrica definita a partire da un insieme di vettori, da un campo di scalari e da due operazioni binarie che devono soddisfare determinate proprietà. Ora andiamo subito ad approfondire, ma ci basti sapere che gli spazi vettoriali sono la struttura principale dell'algebra lineare, fondamentali per le sue applicazioni. Per definire uno spazio vettoriale, ci servono quattro ingredienti principali:

- un campo, solitamente indicato con  $\mathbb{K}$ , detto **campo di scalari**.  $\mathbb{K}$  coincide con l'insieme dei reali.
- un insieme  $V$ , chiamato **spazio di vettori**, i cui elementi vengono indicati in grassetto.
- un'operazione binaria interna, indicata con  $+$ , detta **somma tra vettori**, cioè  $(v, w) \rightarrow v + w$ .
- un'operazione binaria esterna, indicata con  $\cdot$ , detta **prodotto di un vettore per uno scalare**, cioè  $(\lambda, v) \rightarrow \lambda \cdot v$ .

Diremo che  $(V, +, \cdot)$  è uno spazio vettoriale  $F$  sul campo  $\mathbb{K}$  se l'insieme  $V$ , munito delle operazioni  $+$  e  $\cdot$  è una struttura algebrica che soddisfa le seguenti proprietà.

- la sottostruttura  $(V, +)$  deve essere un gruppo commutativo, cioè  $+$  deve godere della proprietà associativa, in  $V$  deve esserci l'elemento neutro rispetto a  $+$  e ogni elemento di  $V$  deve ammettere l'inverso rispetto a  $+$ . Inoltre  $+$  deve godere della proprietà commutativa.
- l'operazione  $\cdot$  deve essere omogenea, cioè il suo effetto su insieme di elementi deve essere lo stesso indipendentemente dalla dimensione o dalla scala degli

elementi.

Sembra complicato, per questo vediamo un esempio.

- **ES** =  $R^3$  può essere considerato uno spazio vettoriale di tutte le triple  $(x, y, z)$  di numeri reali con operazioni di somma e moltiplicazione scalare. Ma perché  $R^3$  è uno spazio vettoriale? Innanzitutto vediamo come viene rispettata l'associatività della somma, infatti  $(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$ . Viene rispettata anche la commutatività della somma, infatti  $x_1 + x_2 = x_2 + x_1$ . Esiste l'elemento neutro, il vettore  $(0, 0, 0)$ . Esiste anche il vettore inverso, ossia  $(-x, -y, -z)$ . Notiamo come vale anche la distributività del prodotto scalare rispetto alla somma, infatti notiamo subito come  $a \cdot x_1 + x_2 = a \cdot x_1 + a \cdot x_2$ . Verificate queste proprietà, concludiamo che  $R^3$  è uno spazio vettoriale.

Un altro concetto importante è un sottoinsieme di uno spazio vettoriale, detto **sottospazio vettoriale**. Per definirlo, consideriamo uno spazio vettoriale  $F$  su un campo  $\mathbb{K}$ . Si dice che il sottoinsieme non vuoto  $S$  di  $F$ , è un sottospazio vettoriale se è uno spazio vettoriale su rispetto alle stesse operazioni di somma tra vettori e di prodotto di un vettore per uno scalare definite in  $F$ . Ogni spazio vettoriale contiene almeno i **sottospazi banali**, ossia stesso e il sottospazio nullo  $\{0\}$ . Ogni sottospazio, con  $S \neq F$  è detto **sottospazio proprio**. Per verificare che un insieme sia effettivamente un sottospazio vettoriale, dovremo verificarne alcune proprietà e, per fare ciò, ci viene incontro il **teorema di caratterizzazione**.

- **T.H.** = un sottoinsieme non vuoto di  $S$  di uno spazio vettoriale  $F$  su un campo  $\mathbb{K}$  è un sottospazio vettoriale di se e solo se è chiuso rispetto alle due operazioni in  $F$ , cioè per ogni  $s_1, s_2 \in S$  risulta che  $s_1 + s_2 \in S$  e per ogni  $s \in S, \lambda \in \mathbb{K}$   $\lambda \cdot s \in S$ .

Facciamo un altro esempio.

- **ES** = prendendo come esempio sempre  $R^2$ , supponiamo sia composto dai vettori  $(1, 0)$  e  $(0, 1)$ . Un possibile sottospazio vettoriale generato potrebbero essere tutti i vettori espressi come combinazioni lineari di  $(1, 0)$  e  $(0, 1)$ , poiché rispettano le proprietà appena descritte.

Abbiamo introdotto un nuovo termine. Cos'è una **combinazione lineare**? Si tratta generalmente di un'espressione in cui compaiono somme di vettori e moltiplicazioni di vettori per uno scalare. Abbiamo uno spazio vettoriale  $F$  in un campo  $\mathbb{K}$ , con  $n$  vettori  $v_1, v_2, \dots, v_n$ . Una combinazione lineare potrebbe essere:

- $a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ ;

Diremo che i vettori  $v_1, v_2, \dots, v_n$  sono **linearmente indipendenti** tra di loro se, imponendo  $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0$ . Vale a dire se l'unica combinazione lineare dei vettori che risulti uguale al vettore nullo è quella in cui gli scalari sono tutti nulli. Ovviamente, i vettori saranno **linearmente dipendenti** se esiste una combinazione lineare dei vettori con scalari non tutti nulli che risulti uguale al vettore nullo. Per fissare meglio il concetto, basta leggere l'espressione di prima come un sistema lineare omogeneo, scrivendolo nella forma matriciale del tipo:

- $Ax = 0$  con  $x = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$

Sappiamo che un sistema lineare omogeneo è sempre compatibile, infatti  $(0, 0, \dots, 0)$  è sempre una soluzione. Quindi, affinché i vettori siano linearmente indipendenti, la soluzione banale deve essere l'unica ammessa dal sistema.

Introduciamo, adesso un altro metodo di risoluzione dei sistemi lineari, il **teorema di Rouché-Capelli**.

- **T.H.** = indicando con  $A$  la matrice incompleta dei coefficienti e  $b$  quella dei termini noti, il teorema stabilisce che se:
  - $\rho(A) < \rho(A|b)$ , allora il sistema è impossibile.
  - $\rho(A) = \rho(A|b)$ , allora il sistema è compatibile, ossia ammette una o infinite soluzioni

Inoltre, se indichiamo con  $n$  il numero di incognite, risulta che:

- $\rho(A) = \rho(A|b) = n$ , allora c'è una sola soluzione
- $\rho(A) = \rho(A|b) < n$ , allora il sistema ammette  $\infty^{n-\rho(A)}$

Applicando questo teorema ai vettori, esso ci garantisce che, se il rango della matrice costruita con i vettori è uguale al numero di vettori, allora essi saranno linearmente indipendenti. Vediamo un pratico esempio:

- **ES** = prendiamo un insieme di vettori:

- $v_1 = (1, 0, 1, -1), v_2 = (2, -1, 0, 3), v_3 = (-2, 5, 2, 1)$

Vogliamo stabilire se questi vettori sono linearmente indipendenti, così li scriviamo nella loro forma matriciale:

$$\circ A = \begin{pmatrix} 1 & 2 & -2 \\ 0 & -1 & 5 \\ 1 & 0 & 2 \\ -1 & 3 & 1 \end{pmatrix}$$

Sappiamo già calcolare il rango, scegliendo uno dei metodi già studiati, stabiliamo che  $\rho(A) = 3$ . I vettori sono 3, quindi concludiamo che sono linearmente indipendenti.

Un altro concetto importante in tema di spazi vettoriali, è il **sistema generatore**, cioè un insieme di vettori che permette di ricostruire, attraverso combinazioni lineari, tutti i vettori dello spazio. Sia  $F$  uno spazio vettoriale su un campo  $\mathbb{K}$ . Diremo che un insieme di vettori  $v_1, v_2, \dots, v_n \subseteq F$  è un sistema di generatori di  $F$  se ogni elemento di  $F$  si può esprimere mediante una combinazione lineare. Osserviamo che, per ogni spazio vettoriale  $F$  non nullo, esiste un numero infinito di sistemi di generatori. Sembra complicato, ma vediamo ora un pratico esempio su come stabilire se un insieme di vettori costituisce un sistema di generatori.

- **ES** = consideriamo il seguente insieme di vettori in  $\mathbb{R}^3$ :

$$\circ \{(1, 0, 1), (0, 0, 3), (1, 2, 1), (1, -1, 0)\}$$

Per definizione, diciamo che tali vettori generano  $\mathbb{R}^3$  se e solo se per ogni  $w \in \mathbb{R}^3$ , esistono quattro scalari  $a_1, a_2, a_3, a_4$  tali che:

$$\circ a_1(1, 0, 1) + a_2(0, 0, 3) + a_3(1, 2, 1) + a_4(1, -1, 0) = (w_1, w_2, w_3)$$

Svolgendo i calcoli, ci troveremo di fronte ad una cosa del genere:

$$\circ (a_1 + a_3 + a_4, 2a_3 - a_4, a_1 + 3a_2 + a_3) = (w_1, w_2, w_3)$$

Possiamo scrivere questo come un sistema lineare, quindi:

$$\circ \begin{cases} a_1 + a_3 + a_4 = w_1 \\ 2a_3 - a_4 = w_2 \\ a_1 + 3a_2 + a_3 = w_3 \end{cases}$$

Scriviamo la matrice completa  $(A|b)$  e, se  $\rho(A) = \rho(A|b)$ , i vettori saranno un sistema di generatori in  $\mathbb{R}^3$ :

$$\circ (A|b) = \left( \begin{array}{cccc|c} 1 & 0 & 1 & 1 & w_1 \\ 0 & 0 & 2 & -1 & w_2 \\ 1 & 3 & 1 & 0 & w_3 \end{array} \right)$$

Usiamo uno dei metodi conosciuti per ottenere il rango e noteremo che  $\rho(A) = \rho(A|b) = 3$ , quindi i vettori costituiscono un sistema di generatori in  $\mathbb{R}^3$ .

Un altro concetto che affronteremo adesso è quello di **base** di uno spazio vettoriale. Dato uno spazio vettoriale  $F$  su un campo  $\mathbb{K}$ , diciamo che un insieme di vettori  $v_1, v_2, \dots, v_n$  di è una base se è un sistema di generatori e se i vettori sono tra loro linearmente indipendenti. Osserviamo che un qualsiasi spazio vettoriale, definito su un campo , non nullo ammette infinite basi. Inoltre, due basi definite sullo stesso spazio vettoriale hanno lo stesso numero di elementi, quindi la stessa cardinalità. Non serve realmente vedere un esempio, dato che sappiamo sia stabilire se un insieme di vettori costituisce un sistema di generatori. E, ovviamente, una volta ottenuto il rango, se sarà uguale al numero di vettori, allora essi saranno anche linearmente indipendenti. Basta verificare queste due condizioni, se vere, allora quell'insieme di vettori costituisce una base dello spazio vettoriale . Un caso particolare di base è la **base canonica**, generalmente definita su alcuni spazi vettoriali notevoli che si studiano, come  $R_n[x]$ , che è lo spazio dei polinomi, oppure  $Mat(m, n, R)$ , lo spazio delle matrici. Una base canonica di  $R^n$  è costituita da  $n$  vettori, solitamente indicati con  $e_1, e_2, \dots, e_n$ , ciascuno dei quali ha una sola componente nulla. La cardinalità di una qualsiasi base di uno spazio vettoriale, cioè il numero di suoi elementi, è detta **dimensione** di uno spazio vettoriale, quindi  $\dim(F) = |B|$ .

Immaginiamo di avere due spazi vettoriali  $V$  e  $W$ , definiti su un campo , e sia una funzione da in , quindi  $F : V \rightarrow W$ . prende il nome di **applicazione lineare** se soddisfa alcune condizioni:

- **additività**: per ogni  $v_1, v_2 \in V$ , l'immagine della somma è uguale alla somma delle immagini, quindi  $F(v_1 + v_2) = F(v_1) + F(v_2)$ .
- **omogeneità**: per ogni  $v \in V$  e per ogni  $\lambda \in \mathbb{K}$ , l'immagine del prodotto di  $v$  per lo scalare  $\lambda$  è uguale al prodotto dello scalare per l'immagine di  $v$ , quindi  $F(\lambda \cdot v) = \lambda \cdot F(v)$ .

Per semplicità, riassumeremo queste condizioni, chiamandole **condizioni di linearità**. Vediamo un esempio.

- **ES** = consideriamo l'applicazione  $F : \mathbb{R} \rightarrow \mathbb{R}$  definita da  $F(x) = 4x$ . Dobbiamo verificare le condizioni di linearità. L'applicazione gode della proprietà additiva, poiché  $F(x + y) = 4(x + y) = 4x + 4y = F(x) + F(y)$ . Inoltre, notiamo anche che è omogenea, dato che  $F(\lambda \cdot x) = 4 \cdot \lambda \cdot x = \lambda \cdot 4 \cdot x = \lambda \cdot F(x)$ .

Quindi  $F$  è un applicazione lineare. Possiamo osservare che è una verifica abbastanza meccanica che, in base allo spazio, richiede la conoscenza di determinate operazioni per verificare la linearità. Possiamo definire l'applicazione

lineare  $F : V \rightarrow W$  come un **omomorfismo** tra  $V$  e  $W$ . Esistono, ovviamente, vari tipi di omomorfismo. Li abbiamo già definiti, ma li ripetiamo.

- **monomorfismo**: detto anche omomorfismo iniettivo, si chiama così se elementi distinti di  $V$  mediante  $F$  hanno immagini distinte, in simboli  $\forall v_1, v_2 \in V, v_1 \neq v_2 \Rightarrow F(v_1) \neq F(v_2)$ .
- **epimorfismo**: detto anche omomorfismo suriettivo, si chiama così se ogni elemento del codominio  $W$  è l'immagine di un elemento del dominio  $V$ , in simboli  $\forall w \in W \exists v \in V$  tale che  $F(v) = w$ .
- **isomorfismo**: detto anche omomorfismo biettivo, cioè per ogni vettore  $w \in W$  esiste un unico elemento del dominio che ha per immagine  $w$ , in simboli  $\forall w \in W !\exists v \in V$  tale che  $F(v) = w$ .
- **endomorfismo**: detto anche operatore lineare, è un omomorfismo di uno spazio vettoriale in sé, cioè quando dominio e codominio coincidono, in simboli  $F : V \rightarrow V$ .

Sia  $F : V \rightarrow W$  un'applicazione lineare. Chiamiamo **nucleo** di  $F$ , indicandolo con  $Ker(f)$ , l'insieme degli elementi del dominio  $V$  che hanno come immagine mediante  $F$  lo zero di  $W$ .

- $Ker(f) := \{v \in V : F(v) = 0_w\}$

Definire il nucleo, in ambito di applicazioni lineare, è fondamentale, poiché ci dice quali elementi dello spazio di partenza hanno come immagine lo zero dello spazio di arrivo. Un altro caposaldo in un'applicazione lineare, è l'**immagine**. Data la definizione precedente, indichiamo con  $Im(f)$  il sottoinsieme del codominio che ha per elementi tutti e soli i vettori di  $W$  che sono immagine, mediante  $F$ , degli elementi di  $V$ .

- $Im(f) := \{w \in W | \exists v \in V \rightarrow F(v) = w\}$

È importante definire il concetto di **matrice associata ad un'applicazione lineare**, che rappresenta la trasformazione lineare cui è riferita rispetto a due fissate basi degli spazi vettoriali di partenza e di arrivo. Consideriamo sempre un'applicazione lineare del tipo  $F : V \rightarrow W$  e siano  $B_v = \{v_1, v_2, \dots, v_n\}$  e  $B_w = \{w_1, w_2, \dots, w_n\}$  le rispettive basi associate. Per costruire la matrice dobbiamo determinare l'immagine rispetto all'applicazione  $F$  di ogni vettore  $v$ , quindi le varie  $F(v_1), F(v_2), \dots, F(v_n)$ . I vettori ottenuti saranno elementi di  $W$  e possono essere scritti come combinazione lineare di  $B_w$ , quindi  $F(v_1) = \{a_{11}w_1 + a_{21}w_2 + \dots + a_{m1}w_m\}$ . Otterremo la matrice associata all'applicazione lineare

che ha per  $j$ -esima colonna il vettore delle coordinate dell'immagine  $F(v)$  rispetto alla base di  $W$  e sarà del tipo:

$$\bullet \quad A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Un'applicazione lineare ha basi infinite associate a dominio e codominio, quindi automaticamente anche infinite matrici associate. Inoltre, il numero di righe è sempre uguale alla dimensione dello spazio vettoriale di arrivo e il numero di colonne dello spazio vettoriale di partenza. Se la matrice è quadrata, allora ci troviamo di fronte ad un endomorfismo, avendo le stesse dimensioni degli spazi vettoriali. Vediamo un esempio.

- **ES** = sia  $F : R^3 \rightarrow R^3$  un'applicazione lineare con  $F(x, y, z) = (x + y, z)$  e siano  $B_{R^3} = \{(1, 0, 1), (1, 0, 0), (1, 1, 1)\}$  e  $B_{R^2} = \{(0, 1), (1, 1)\}$  le basi rispettive. Allora, cominciamo calcolando le immagini mediante  $F$  dei vettori  $B_{R^3}$
- $F(1, 0, 1) = \{(1 + 0, 1) = (1, 1)\}$   
 $F(1, 0, 0) = \{(1 + 0, 0) = (1, 0)\}$   
 $F(1, 1, 1) = \{(1 + 1, 1) = (2, 1)\}$

Adesso, scriviamo i vettori ottenuti come combinazioni lineari dei vettori di  $B_{R^2}$ .

- $F(1, 0, 1) = (1, 1) = 0 \cdot (0, 1) + 1 \cdot (1, 1)$   
 $F(1, 0, 0) = (1, 0) = -1 \cdot (0, 1) + 1 \cdot (1, 1)$   
 $F(1, 1, 1) = (2, 1) = 0 \cdot (0, 1) + 1 \cdot (1, 1)$

La matrice associata a quell'applicazione lineare avrà tre righe, come i vettori dello spazio di partenza, e due colonne, come quelli di arrivo e sarà:

$$\circ \quad A_F = \begin{pmatrix} 0 & -1 & -1 \\ 1 & 1 & 2 \end{pmatrix}$$

In questo capitolo andremo a riprendere un concetto familiare all'algebra delle matrici, ma che senza le nozioni acquisite in questo, non saremo riusciti a capire nel precedente. Prima di farlo, andiamo a definire due concetti molto importanti. Partiamo col dire che ci concentreremo solo ed esclusivamente sulle matrici quadrate. Sia  $A$  una matrice quadrata di ordine  $n$  su un campo  $\mathbb{K}$ . Si dice che lo scalare  $\lambda_0 \in \mathbb{K}$  è un **autovalore** della matrice  $A$  se esiste un vettore colonna non nullo  $v$  tale che  $Av = \lambda_0 v$ . Il vettore  $v$  è detto **autovettore** relativo all'autovalore  $\lambda_0$ .

Da questa espressione segue automaticamente  $Av - \lambda_0 v = 0$ , quindi  $(A - \lambda_0 \cdot Id_n)v = 0$ , dove  $Id_n$  è la matrice identità avente lo stesso ordine della matrice  $A$ . Osserviamo che l'espressione di prima è la forma matriciale di un sistema lineare omogeneo. Sappiamo che un sistema lineare omogeneo ammette soluzione diversa da quella banale se e solo se la matrice incompleta associata ha determinante uguale a zero. Quindi segue che  $\det(A - \lambda_0 \cdot Id_n) = 0$ . L'espressione viene detta **polinomio caratteristico**. Deduciamo che gli autovalori sono gli zeri del polinomio caratteristico. Una volta trovati, andiamo a calcolare gli autovettori corrispondenti ad ogni autovalore. La procedura è leggermente più complessa. Chiamando  $\lambda_1, \lambda_2, \dots, \lambda_n$  gli autovalori distinti di  $A$ , per ogni autovalore dobbiamo calcolare lo spazio degli autovettori associati ad essi e, per farlo, ci serviamo di un sistema lineare omogeneo.

- $(A - \lambda_i \cdot Id_n)v = 0$ ;

Da qui possiamo estrarne una base  $B$  per l'insieme delle soluzioni. Gli autovettori saranno i vettori non nulli che appartengono al sottospazio generato dai vettori di  $B$ . Sembra piuttosto complicato, anche perché non abbiamo ancora le nozioni adeguate. Ma, possiamo vedere un esempio pratico per calcolarli.

- **ES** = consideriamo la matrice:

$$\circ \quad A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

La prima cosa da fare è calcolare il polinomio caratteristico  $p_A(\lambda) = \det(A - \lambda \cdot Id_3)$ :

$$\circ \quad \det\left[\begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right]$$

Risparmiamo un po' di calcoli e troviamo  $\det(A) = -\lambda^3 + 7\lambda^2 - 14\lambda + 8$ . Ora, dobbiamo trovare gli zeri. Essendo un'equazione di terzo grado, ci tocca scomporre il polinomio con Ruffini. Risparmiamo anche qui i calcoli, non essendo di competenza di questo corso e scopriamo che sono  $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 4$ . Questi sono gli autovalori della matrice. Ora, calcoliamo gli autovettori corrispondenti. Partiamo da  $\lambda_1$  e dobbiamo ottenere un sistema lineare in forma estesa, impostiamo la matrice in questo modo:  $(A - Id_3)v = 0$ , ma sostituendo  $v$  con il vettore colonna delle incognite e 0 col vettore colonna nullo. Verrà una cosa di questo tipo:

$$\circ \left[ \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Svolgendo il prodotto tra matrici otterremo questa matrice:

$$\circ \begin{pmatrix} x+y \\ x+2y+z \\ y+z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Ora, il tutto viene messo a sistema:

$$\circ \begin{cases} x+y=0 \\ x+2y+z=0 \\ y+z=0 \end{cases}$$

Banalmente, andiamo a risolvere il sistema usando il metodo di sostituzione e otterremo una soluzione del tipo  $(-y, y, -y)$  che scritto in forma di combinazione lineare scopriremo gli autovettori. Ci risparmiamo i calcoli anche per gli altri autovalori e li scriveremo tutti insieme:

$$\circ B_{V\lambda 1} = (-1, 1, -1); \\ B_{V\lambda 2} = (-1, 0, -1); \\ B_{V\lambda 3} = (1, 2, 1);$$

Per ogni autovalore di una matrice, è possibile calcolare la sua **molteplicità algebrica** e la **molteplicità geometrica**. Cominciamo ad avvicinarci alla **diagonalizzabilità**. Sia  $A$  una matrice quadrata di ordine  $n$  e sia  $\lambda_0$  un suo autovalore. Si dice molteplicità algebrica dell'autovalore  $\lambda_0$  e si indica con  $m_a(\lambda_0)$ , il numero che esprime quante volte l'autovalore  $\lambda_0$  annulla il polinomio caratteristico. In questo caso, possiamo rifarci all'esempio precedente.

- **ES** = abbiamo gli autovalori  $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 4$ . Procediamo per gradi, cominciando dalla molteplicità algebrica di  $\lambda_1$ . Per annullare il polinomio, dividiamo l'originale per  $(\lambda - 1)^1$ , ottenendo una cosa del genere:

$$\circ \frac{-\lambda^3 + 7\lambda^2 - 14\lambda + 8}{(\lambda - 1)^1}$$

Facendo questa scomposizione, otteniamo un polinomio che ha 1 grado inferiore a quello originale, ossia  $-\lambda^2 + 6\lambda - 8$ . Vale a dire che 1 annulla il polinomio una sola volta e, quindi  $m_a(\lambda_1) = 1$ . Così facendo,  $m_a(\lambda_2) = 2$  e  $m_a(\lambda_3) = 1$ . Di conseguenza, mantenendo le stesse condizioni di prima, diremo che la molteplicità geometrica dell'autovalore  $\lambda_0$ , indicata con  $m_g(\lambda_0)$ , è la dimensione dell'autospazio relativo a  $\lambda_0$ , cioè il numero di elementi di una qualsiasi base

dell'autospazio relativo a  $\lambda_0$ . Sembra complicato, ma per calcolarlo basta applicare la formula  $n - \rho(A - \lambda_0 \cdot Id_n)$ , dove  $n$  indica l'ordine della matrice. Partiamo col primo autovalore:

$$\circ \quad 3 - \rho \left[ \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{pmatrix} - 1 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right]$$

Essendo 1, la matrice identità resta invariata, quindi andiamo a fare semplicemente  $A - Id_n$ . Otteniamo la matrice:

$$\circ \quad \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Verifichiamo immediatamente che  $\rho = 2$ ,  $3 - 2 = 1$ , quindi  $m_g(\lambda_1) = 1$ . Di conseguenza  $m_g(\lambda_2) = 2$  e  $m_g(\lambda_3) = 1$ .

La molteplicità geometrica di un autovalore associato a una matrice quadrata di ordine  $n$  è minore o al più uguale alla molteplicità algebrica dello stesso, ed è almeno 1. Sia  $A$  una matrice quadrata di ordine  $n$  a coefficienti su un campo  $\mathbb{K}$ . Si dice che  $A$  è una **matrice diagonalizzabile** se è simile ad una matrice diagonale  $D$  di ordine  $n$ . Intendiamo affermare che  $A$  è diagonalizzabile se e solo se esiste una matrice invertibile  $P$  tale che  $PD = AP$ . P sarà detta **matrice diagonalizzante**. Ci sono alcune condizioni sufficienti e necessarie affinché una matrice sia diagonalizzabile:

1. il numero di autovalori di  $A$ , contati con le loro molteplicità è pari all'ordine della matrice.
2. la molteplicità geometrica di ciascun autovalore coincide con la relativa molteplicità algebrica.

Un caso particolare prevede che una matrice simmetrica, cioè se essa coincide con la sua trasposta, allora sarà automaticamente diagonalizzabile. Inoltre, se l'ordine della matrice coincide col numero di autovalori, allora la matrice è diagonalizzabile.

- **ES** =  $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 2 & 4 \end{pmatrix}$

Calcoliamo il polinomio caratteristico con la formula  $p_{A(\lambda)} = \det(A - \lambda \cdot Id_3) = -\lambda^3 + 7\lambda^2 - 16\lambda + 12$ . Troviamo la molteplicità algebrica  $m_{a(\lambda_1)} = 2$  e  $m_{a(\lambda_2)} = 1$ . La matrice è di ordine 3, quindi è soddisfatta la prima condizione. Andiamo a verificare le molteplicità geometriche. Usando la formula  $m_g(\lambda) =$

$n - \rho(A - \lambda \cdot Id_n)$ . Risparmiandoci dei calcoli che sappiamo già fare, troviamo che  $m_g(\lambda_1) = 1$ . La molteplicità algebrica e quella geometrica non coincidono, possiamo anche fermarci qui, la matrice non è diagonalizzabile

Ma se lo fosse stata?

- **ES** =  $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 0 \\ 1 & -2 & 1 \end{pmatrix}$

Supponiamo per certo che sia diagonalizzabile. La matrice diagonale  $D$  ha gli elementi della diagonale uguali agli autovalori di  $A$ , quindi è:

- $D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

Ora, dobbiamo trovare la matrice  $P$ , la matrice diagonalizzante. Sappiamo che la matrice ha due autovalori, quindi dobbiamo determinare una base  $V_\lambda$  per ogni autovalore  $\lambda_1 = 0$  e  $\lambda_2 = 2$ . Abbiamo visto che, per determinare una base, dobbiamo trovare l'insieme delle soluzioni del sistema lineare omogeneo.

- $(A - \lambda \cdot Id_n)x = 0;$

Cominciamo dal primo autovalore. Vale , quindi si annulla anche la matrice identica:

- $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 0 \\ 1 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Impostiamo il seguente sistema lineare:

- $$\begin{cases} x + 2y + z = 0 \\ 2y = 0 \\ x - 2y + z = 0 \end{cases}$$

Usando il metodo di sostituzione, troviamo rapidamente  $(x, y, z) = a(-1, 0, 1)$ , che sarà la prima colonna della matrice diagonalizzante. Dobbiamo fare la stessa cosa con  $\lambda_2$  e ci troveremo, questa volta, due vettori  $(2, 1, 0)$  e  $(1, 0, 1)$ . Impostata la nuova matrice, otterremo facilmente la diagonalizzante:

- $P = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

Possiamo verificare se abbiamo eseguito bene i calcoli verificando se  $PD = AP$ .