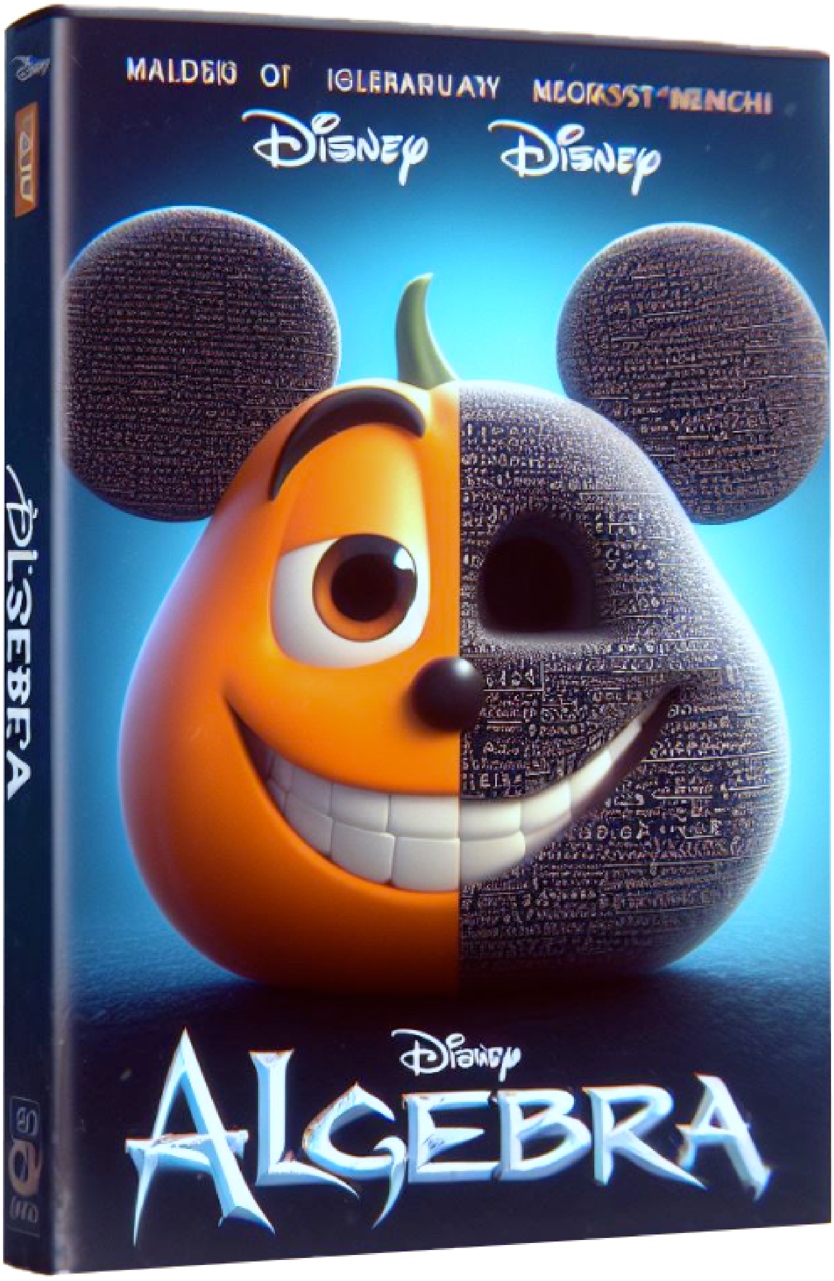
Algebra

Marco Casu



Contents

1 Insiemi e Relazioni

Sappiamo già che un insieme non è altro di una collezione di oggetti distinti.

$$A = \{1, 2, 3, 4, 5\}$$

Ricapitoliamo le proprietà basiche degli insiemi :

- **Intersezione** - $A \cap B \rightarrow \{x | x \in A \wedge x \in B\}$
- **Unione** - $A \cup B \rightarrow \{x | x \in A \vee x \in B\}$
- **Sottoinsieme** - $A \subseteq B \rightarrow \{x \in A \implies x \in B\}$
- **Insieme complementare** - $A^c_{\text{in B}} \rightarrow \{x \in B | x \notin A\}$

1.1 Proprietà fondamentali degli insiemi

Elenchiamo le già note proprietà degli insiemi :

- **Associativa** - $(A \cap B) \cap C = (C \cap B) \cap A$ oppure $(A \cup B) \cup C = (C \cup B) \cup A$
- **De Morgan** - Se $A, B \subseteq C$ allora $(A \cap B)^c = A^c \cup B^c$ oppure $(A \cup B)^c = A^c \cap B^c$
- **Distributiva** - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ oppure $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Un insieme particolare associato ad un dato insieme A è **l'insieme delle parti** di A, è l'insieme di tutti i possibili sotto-insiemi di A e si indica con :

$$\mathcal{P}(A) = \{B | B \subseteq A\} \tag{1}$$

Introduciamo adesso il concetto di **prodotto cartesiano** su due insiemi A e B, esso non è altro che l'insieme di tutte le coppie ordinate dove il primo elemento appartiene ad A ed il secondo elemento a B :

$$A \times B = \{(a, b) | a \in A, b \in B\} \tag{2}$$

1.2 Le Relazioni

Una relazione ρ da un insieme A ad un insieme B, è un sotto-insieme del prodotto cartesiano $A \times B$.

$$\rho \subseteq A \times B, \text{ se } (a, b) \in \rho \text{ si scrive } a\rho b \tag{3}$$

Il dominio di tale relazione ρ risulta essere :

$$\mathcal{D}(\rho) = \{a \in A | \exists b \in B \text{ per il quale risulti } a\rho b\} \tag{4}$$

La sua immagine :

$$\Im(\rho) = \{b \in B | \exists a \in A \text{ per il quale risulti } a\rho b\} \tag{5}$$

Per una relazione ρ, se il suo dominio risulta essere tutto A, e $\forall a \in A \exists$ un unico $b \in B | a\rho b$, tale ρ è anche una **funzione**.

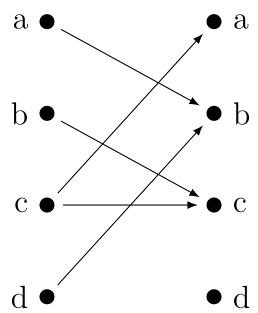
Esempio di relazione :

sia $A = \{a, b, c, d\}$, è definita la relazione $\rho \subseteq A \times A = \{(a, b), (b, c), (c, c), (c, a), (d, b)\}$.

Abbiamo due modi per poter visualizzare una relazione, un formato tabellare, ed un formato con nodi e collegamenti fra gli elementi della relazione. Per la relazione ρ appena enunciata si ha la seguente rappresentazione tabellare dove si inserisce un 1 nel punto in cui le due coordinate sono in relazione fra loro :

d	0	0	0	0
c	0	1	1	0
b	1	0	0	1
a	0	0	1	0
	a	b	c	d

Vediamone adesso una rappresentazione con nodi e collegamenti :



Essendo le relazioni degli insiemi, possiamo considerare le operazioni di unione ed intersezione anche per le relazioni. Esista per ogni relazione, anche la sua **relazione inversa**, se ρ è definita da A a B, esisterà ρ^{-1} definita da B a A.

$$\rho^{-1} = \{(b, a) \in B \times A | a\rho b\} \text{ quindi } a\rho b \implies b\rho^{-1}a \tag{6}$$

Se la relazione ρ è una funzione, non è detto che la sua relazione inversa sia una funzione anch'essa, prendiamo ad esempio la relazione $\rho \subset \mathbb{R} \times \mathbb{R} = \{(x, x^2)\forall a \in \mathbb{R}\}$, che non è altro che la funzione di una variabile reale $f(x) = x^2$. Tale funzione, per $x = -a$ ed $x = a$, ha sempre $f(x) = a^2$, per due valori appartenti al dominio ha la stessa immagine, la sua funzione inversa avrebbe quindi un punto che mappa due immagini.

Una relazione nota su insieme A è la **relazione identità**, definita : $\Delta_A = \{(a, a) \in A \times A\}$.

1.3 Relazioni di Equivalenza

Una relazione ρ definita su un insieme A, quindi $\rho \subseteq A \times A$, è detta **relazione di equivalenza** se soddisfa i seguenti requisiti :

- ρ è **riflessiva**, ossia è vero che : $a\rho a \forall a \in A$
- ρ è **simmetrica**, ossia è vero che se esiste $a\rho a'$ allora esiste $a'\rho a$
- ρ è **transitiva**, se esistono $a\rho a'$ e $a'\rho a''$, allora esiste $a\rho a''$

Un esempio di relazione di equivalenza è la relazione di *avere la stessa età* su un insieme di studenti, difatti soddisfa tutti e 3 i requisiti :

- è **riflessiva** perchè ognuno ha la stessa età di se stesso.
- è **simmetrica** perchè se tizio ha la stessa età di caio, caio ha la stessa età di tizio.
- è **transitiva** perchè se tizio ha la stessa età di caio e caio ha la stessa età di sempronio, tizio ha la stessa età di sempronio.

Un esempio di relazione **non** di equivalenza è la relazione di *genitorialità*, ad esempio non è simmetrica, perchè se tizio è padre di caio, caio non è assolutamente padre di tizio.

1.4 Le Classi di Equivalenza

Sia ρ una relazione di equivalenza definita su A, si definisce **classe di equivalenza** di un elemento $a \in A$, e si denota con $[a]$, l'insieme di tutti gli elementi di A che sono equivalenti (ossia in relazione di equivalenza) ad a, ossia

$$[a] = \{b \in A | b\rho a\} \tag{7}$$

Ad esempio, su una relazione di *avere la stessa età*, in ogni classe di equivalenza ci sono tutte le persone che hanno la stessa età : ogni classe può essere quindi un etichetta con il numero corrispondente all'età.
Esempio esteso :
Si prenda in considerazione il seguente insieme di persone :

$$A = \{\text{Valentino,Marco,Luca,Alessandro,Davide}\}$$

Ognuno ha i seguenti anni :

- Valentino - 20
- Marco - 19
- Luca - 20
- Alessandro - 19
- Davide - 19

La relazione di *avere la stessa età* su A è definita come :
$\rho = \{(Valentino, Luca), (Luca, Luca), (Marco, Alessandro), (Alessandro, Davide)...ecc\}$
La classe di equivalenza $[Marco] = \{Marco, Alessandro, Davide\}$ definisce tutti gli elementi in relazione con $Marco$, e rappresenta tutte le persone di età uguale a 19.

Sia A un insieme sulla quale è definita una relazione di equivalenza, l'insieme $^A/_a$ è detto **insieme quoziente**, ed è l'insieme che contiene tutte le classi di equivalenza della relazione definita su A.

$$^A/_a = \{[a], a \in A\} \tag{8}$$

Vediamo adesso un **importante proprietà** delle classi di equivalenza :

Teorema 1

$$[a] = [b] \iff a\rho b \tag{9}$$

Dimostrazione 1 *Ovviamente $b \in [b]$ perchè $b\rho b$, essendo*
$[a] = [b] \implies b \in [a] \implies b\rho a \implies a\rho b$*, Analogamente, se $a\rho b$, se esiste*
$c \in [a] \implies c\rho a \implies c\rho b \implies c \in [b] \implies [a] \subseteq [b]$.
se esiste $c \in [b] \implies c\rho b \implies c\rho a \implies c \in [a] \implies [b] \subseteq [a]$. Essendo $[b] \subseteq [a]$ e $[a] \subseteq [b]$, necessariamente $[a] = [b]$.

■

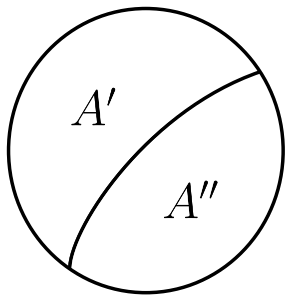
1.4.1 Le Partizioni

Dicesi **partizione** di un insieme A una *collezione di parti o sotto-insiemi* A_α non vuoti di A tali che **l'unione** di tutti i sotto-insiemi sia A, ossia, tali collezioni *ricoprono* A.

$$\bigcup_\alpha A_\alpha = A \tag{10}$$

Ciò significa che $A_\alpha \cap A_\beta \neq \varnothing \implies A_\alpha = A_\beta$, in un linguaggio meno formale, tutte le partizioni di un insieme A, non condividono nessun elemento di A. Nell'immagine seguente, A' e A'' sono partizioni di A.

$A =$



Proposizione 1 *Sia ρ una relazione di equivalenza su A, le classi di equivalenza di ρ sono partizioni di A.*

Dimostrazione:
Ricoprono totalmente A, essendo $a\rho a \forall a \in A$, ogni a appartiene alla sua classe di equivalenza. Inoltre le classi di equivalenza, o coincidono o sono disgiunte.

Proposizione 2 *Ogni partizione di un insieme A determina su A una relazione di equivalenza, per la quale i sotto insiemi della partizione sono le classi di equivalenza.*

Dimostrazione:
Se indichiamo con B_α i sotto-insiemi della partizione A_α su A, è ovvio che :

$$a\rho b \implies \exists B_\alpha | a, b \in B_\alpha \tag{11}$$

Una relazione di equivalenza definisce a sua volta delle classi di equivalenza, che definiscono a loro volta delle partizioni.

1.5 Relazioni di Ordine Parziale

Introduciamo adesso un'altro gruppo di relazioni, ma prima necessitiamo della definizione di **relazione antisimmetrica** :

Sia ρ una relazione, essa si dice **antisimmetrica** se è vero che $a\rho b$ e $b\rho a \implies a = b$ (12)

Detto ciò, possiamo definire una *relazione di ordine* parziale se essa è :

- Riflessiva
- Transitiva
- Antisimmetrica

Esempio 1 - Sia X un insieme, e sia $\mathcal{P}(X)$ l'insieme delle sue parti, definiamo la relazione sugli elementi di $\mathcal{P}(X)$ nel seguente modo $\rho = \{\{A, B\}$ con $A, B \in \mathcal{P}(X)$ se $A \subseteq B\}$, quindi $A\rho B \iff A \subseteq B$, è chiaro che tale relazione soddisfa i 3 requisiti, è quindi di ordine parziale.

Esempio 2 - Prendiamo come relazione la divisibilità in $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$, siano $a, b \in \mathbb{N}^*$ vale che $a\rho b \iff a|b$, dove $a|b$ significa *a divide b*, ossia che $\exists x \in \mathbb{N}^*$ tale che $b = a \cdot x$. Tale relazione è di ordine parziale dato che è riflessiva ($a = 1 \cdot a$ quindi $a\rho a$), è transitiva (dato che se a è divisibile per b e b è divisibile per c, è ovvio che a sia divisibile per c), e risulta essere anche antisimmetrica, dato che :

$$\begin{cases} a\rho b \\ b\rho a \end{cases} \implies \begin{cases} b = ax \\ a = by \end{cases} \implies a = (ax)y \implies xy = 1 \tag{13}$$

Quando si ha una relazione di ordine parziale, gli elementi di tale relazione godono della proprietà di poter essere rappresentati graficamente in un determinato modo, ma prima di enunciare tale rappresentazione, necessitiamo di una definizione.

Teorema 2 *Sia ρ una relazione d'ordine parziale su un insieme A, presi $a, b \in A$, diciamo che a* ***è coperto*** *da b e scriveremo*

$$a \preccurlyeq b \tag{14}$$

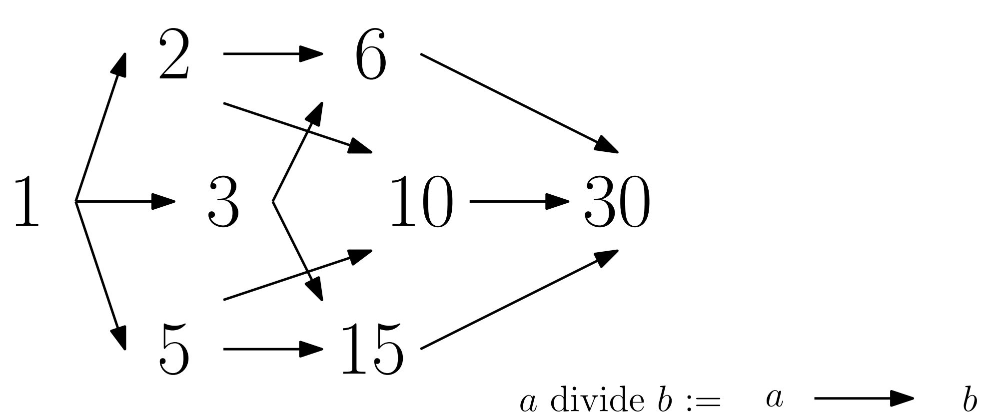
se $a\rho b$ e non esiste nessun elemento c tale che $a\rho c$ e $c\rho b$.

Ad esempio, prendiamo l'insieme $A = \{1, 2, 3, 5, 6.10, 15, 30\}$, ossia dei numeri naturali che dividono 30. Risulta chiaro come :

- $2! \preccurlyeq 30$ 30 non è il primo valore che si fa dividere da 2, ci sono valori prima di 30 per il quale 2 è divisore.
- $2! \preccurlyeq 3$ dato che 2 e 3 non sono nemmeno in relazione.
- $2 \preccurlyeq 6$ perchè 6 è il primo numero che 2 può dividere.

Stabilito ciò, possiamo *rappresentare graficamente* una relazione di ordine parziale su un insieme finito tramite il **diagramma di Hasse**, disegnando tutti gli elementi dell'insieme, collegandoli con una fraccia ogni dove un elemento *copre* un altro.

preso $A = \{1, 2, 3, 5, 6.10, 15, 30\}$ e la relazione di divisibilità prima enunciata, si ha



1.6 I Numeri Naturali

Dalle scuole elementari siamo abituati a lavorare e fare operazioni con i numeri naturali, in questa sezione ne daremo una definizione assiomatica in termini di *fondamenti della matematica.* È importante in questo momento non considerare assolutamente il concetto di numeri naturali che ci è ben chiaro, e cercare di leggere il seguente paragrafo da un punto di vista puramente logico, dando nulla per scontato.

1.6.1 La Terna di Peano

Introduciamo prima quella che è un'astrazione dei numeri naturali, ossia la **terna di Peano**.

$$(\mathbb{N}, \sigma, 0) \tag{15}$$

Si indica in questo caso con $\mathbb{N}$ un insieme di elementi, non i numeri naturali alla quale siamo abituati, con σ invece si indica una funzione $\sigma : \mathbb{N} \to \mathbb{N}$, e dato ogni elemento $n \in \mathbb{N}$, l'elemento $\sigma(n)$ si dice *successivo* di n. Su tale terna, sono definiti 3 fondamentali assiomi :

- $\mathbb{N}_1$ - σ è una funzione iniettiva.
- $\mathbb{N}_2$ - $0 \notin \Im(\sigma)$, 0 non è contenuto nell'immagine di σ.
- $\mathbb{N}_3$ (*Principio di induzione matematica*) - Se $U \subseteq \mathbb{N}$, ed è vero che :
  - $0 \in U$
  - $k \in U \implies \sigma(k) \in U$

  Allora $U = \mathbb{N}$

  Dimostrazione
  Considero $U = \{0\} \cup \{n | \exists n' \text{ tale che } \sigma(n') = n\}$ quindi $k \in U \implies \exists k' | k = \sigma(k')$ allora risulta ovvio che $\sigma(k) = \sigma(\sigma(k')) \in U \implies U = \mathbb{N}$.

1.6.2 Definizione Formale

Dati tali assiomi adesso procediamo nel riconnetterci con l'insieme dei numeri naturali da noi conosciuti, enunciandone le proprietà elementari secondo la terna di Peano.
Sia $(\mathbb{N}, \sigma, 0)$ una terna di Peano, presi $n, m \in \mathbb{N}$, dirò che $n \leq m \iff m = \sigma(\sigma(\sigma(...n)))$, ossia che n è minore o uguale di m se m è uguale a σ applicato su n un certo numero di volte.

Proposizione - Questo stabilisce una relazione di ordine totale.

Adesso definiamo le operazioni elementari che conosciamo sui numeri naturali, ossia di somma e prodotto.
Definiamo la **somma** come operazione su un insieme $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, ossia che associa ad ogni coppia di elementi di $\mathbb{N}$, un elemento di $\mathbb{N}$.

$$n, m \in \mathbb{N} \text{ si definisce somma } n \times m \to n + m \tag{16}$$

La somma è definita in tal modo :

- (i) $0 + b = b$

- (ii) $\sigma(a) + b = \sigma(a + b)$

  Osservazione - $\sigma(0) + b = \sigma(0 + b) = \sigma(b)$, Se poniamo $\sigma(0) = 1$, allora vediamo che $\sigma(b) = b + 1$.

Definamo adesso il **prodotto**, sempre come un operazione $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ avente le seguenti proprietà :

- (i) $0 \cdot b = 0 \forall b \in \mathbb{N}$

- (ii) $\sigma(a) \cdot b = a \cdot b + b$

  Si può dire che gli assiomi di Peano caratterizzano i numeri naturali. Quello che si deve accettare senza dimostrazione, è l'esistenza di un insieme $\mathbb{N}$ *verificante gli assiomi di Peano.*

2 I Numeri Interi

Nell'insieme $\mathbb{N}$, non ci è permesso risolvere $x + 1 = 0$. In questo capitolo partiremo dai numeri naturali per costruirne un estensione in grado di rappresentare gli interi. Partendo dal prodotto cartesiano $\mathbb{N} \times \mathbb{N}$, costruiamo una relazione del tipo :

$$(n, m) \sim (n', m') \iff n + m' = m + n' \tag{17}$$

In linguaggio meno formale, una coppia $(0, a)$ è in relazione con tutte le coppie n, m, per cui $n - m = -a$, ed una coppia $(a, 0)$ è in relazione con tutte le coppie n, m, per cui $n - m = a$. *Esempio :*

$$\begin{array}{l} (5,6) \sim (0,1) \iff 5+1=6+0 \\ (8,2) \sim (6,0) \iff 8+0=2+6 \end{array}$$

Si nota facilmente come tale relazione sia di equivalenza, possiamo quindi definire delle classi di equivalenza che ripartiscono l'insieme $\mathbb{N} \times \mathbb{N}$ in classi $[(n, m)]$. Scegliamo come *rappresentanti* delle classi di equivalenza gli elementi che prevedono uno dei due elementi uguale a *zero*, ogni classe sarà rappresentabile con uno dei seguenti rappresentanti distinti :

$$\begin{array}{l} (0,0) \\ (1,0),(2,0),(3,0)...,(n,0)... \\ (0,1),(0,2),(0,3)...,(0,n)... \end{array}$$

Abbiamo detto che ogni classe $[(a, 0)]$ contiene tutti gli elementi (n, m) per cui $n - m = a$, ad esempio si noti come :

$$[(5,0)] = \{(10,5),(35,30),(1434,1429)...\}$$

Analogamente :

$$[(0,3)] = \{(5,8),(1,4),(22,25)...\}$$

Poniamo per **definizione** :

$$\mathbb{Z} = {}^{\mathbb{N} \times \mathbb{N}}/_{\sim} \tag{18}$$

Ossia l'insieme $\mathbb{Z}$ è l'insieme quoziente[1] di $\mathbb{N} \times \mathbb{N}$ sulla relazione $\sim$ precedentemente definita. Possiamo inoltre decomporre $\mathbb{Z}$ nei seguenti sotto-insiemi :

$$\mathbb{Z} = \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^-$$

Dove (com'è di facile intuizione) si ha :

$$\begin{aligned}
&\mathbb{Z}^+ = \{[(n,0)] | n \in \mathbb{N}\backslash\{0\}\} \\
&0 = [(0,0)] \\
&\mathbb{Z}^- = \{[(0,n)] | n \in \mathbb{N}\backslash\{0\}\}
\end{aligned}$$

Gli elementi di $\mathbb{Z}^+$ saranno denominati **interi positivi** mentre quelli di $\mathbb{Z}^-$ **interi negativi**, l'insieme $\mathbb{Z}$ è un *estensione* di $\mathbb{N}$, dato che contiene al suo interno $\mathbb{Z}^+ \cup \{0\}$ che è identificabile come $\mathbb{N}$ tramite l'applicazione iniettiva da $\mathbb{N}$ in $\mathbb{Z}$ che associa ad ogni naturale n la classe $[(n,0)]$. Definiamo adesso su $\mathbb{Z}$ le operazioni elementari di somma e prodotto :

Somma :

$$[(n,m)] + [(n',m')] = [(n+n', m+m')]$$

Esempio 1 :

$$[(5,0)] + [(0,9)] = [(5,9)] = [(0,4)]$$

Prodotto :

$$[(n,m)] \cdot [(n',m')] = [(n \cdot n' + m \cdot m', n' \cdot m + n \cdot m')]$$

Esempio 2 :

$$[(7,0)] \cdot [(0,2)] = [(7 \cdot 0 + 0 \cdot 2, 0 \cdot 0 + 7 \cdot 2)] = [(0,14)]$$

Da ora in poi indicheremo gli elementi di $\mathbb{Z}$ in tal modo :

$$[(n,0)] = n \qquad [(0,0)] = 0 \qquad [(0,n)] = -n$$

Riprendendo gli esempi di prima, è chiaro come adesso siano definite le operazioni elementari che siamo abituati ad utilizzare fin dalle elementari.

$$\begin{aligned}
&\textit{Esempio 1} \ \to 5 + (-9) = -4 \\
&\textit{Esempio 2} \ \to 7 \cdot (-2) = -14
\end{aligned}$$

Osservazioni :

$$[(n,0)] + [(0,n)] = [(n+0, 0+n)] = [(n,n)] \sim [(0,0)] \implies n + (-n) = 0$$

In $\mathbb{Z}$ ci sono due importanti elementi, $[(0,0)] = 0$ e $[(1,0)] = 1$, dati tali elementi e le operazioni precedentemente definite, diciamo che $\mathbb{Z}$ è una **struttura algebrica**.

[1] l'insieme di tutte le classi di equivalenza.

2.1 Divisibilità in $\mathbb{Z}$

Teorema Fondamentale : Presi due numeri $a, b \in \mathbb{Z}$, con $b \neq 0$, esistono e sono unici due numeri $q, r \in \mathbb{Z}$ tale che :

$$a = bq + r \text{ dove } 0 \leq r < |b|$$

Dove a è detto *dividendo*, b è detto *divisore*, q è detto *quoziente* ed r è detto *resto*.

Dimostrazione :
(*Esistenza*) Consideriamo un numero intero $b \geq 1$ e l'insieme $S = \{a - bx \geq 0, x \in \mathbb{Z}\}$, si ha che $S \neq \emptyset$ perchè, ponendo ad esempio $x = -|a|$, si verifica $a + b|a| \geq 0$. Per *principio del buon ordinamento*, essendo S sottoinsieme di $\mathbb{N}$, S ha un minimo, che denoteremo r. Quindi $r \in S \implies r = a - bq$ con $q \in \mathbb{Z}$. Segue che $a = bq + r$, e tale coppia q, r è unica dato che r essendo un minimo, è unico. Si dimostra facilmente $0 \leq r < |b|$, sicuramente $0 \leq r$ dato che $r \in S$, poniamo per assurdo che $r \geq |b|$, quindi $r - b \geq 0$. Dato che prima si è scritto $r = a - bq$, ora abbiamo $r - b = a - bq - b$, che possiamo riscrivere come $a - b(q + 1)$, che rientra nella forma $a - bx$ definita inizialmente nell'insieme S. Ciò vuol dire che $r - b \in S$, ovviamente $r > r - b$, ma r è il minimo di S quindi è **assurdo** che $r - b$ sia in S, per questo $r < |b|$. $\blacksquare$

Definizione : presi $a, b \in \mathbb{Z}$ si dice che a *divide* b, e si scrive $a|b$, se esiste $c \in \mathbb{Z}$ tale che $b = ac$.
Osservazioni :

- 1) ogni $a \in \mathbb{Z}$ ha sempre i divisori *ovvi*, ossia ± 1 e $\pm a$.
- 2) $\forall a \in \mathbb{Z}, a|0$.
- 3) $0|a \iff a = 0$
- 4) $a|1 \iff a = \pm 1$
- 5.1) se $a|b$ e $a|c$, allora $\forall x, \forall y, a|bx + cy$, si dimostra facilmente :

$$\begin{cases} a|b \implies b = at \\ a|c \implies c = as \end{cases} \implies bx + cy = atx + asy = a(tx + sy) \implies a|bx + cy \tag{19}$$

- 5.2) se $\forall x, \forall y, a|bx + cy$, allora $a|b$ e $a|c$.

2.2 Il Massimo Comun Divisore

Definizione : Siano $a, b \neq 0, 0 \in \mathbb{Z}$, $d \geq 1 \in \mathbb{Z}$ si dice **massimo comun divisore** di (a, b) se:

- i) $d|a$ e $d|b$
- ii) se $d'|a$ e $d'|b$ allora $d'|d$

Il massimo comun divisore esiste $\forall a, b \neq 0, 0 \in \mathbb{Z}$ ed è *unico*.
Dimostrazione :
(*Esistenza*) Vogliamo dimostrare che $MCD(a, b)$ esiste. Sia $S = \{ax + by > 0, \forall x, y \in \mathbb{Z}\} \subseteq \mathbb{N} \backslash \{0\}$ un insieme, ovviamente non vuoto, essendo

sotto-insieme dei numeri naturali vale il principio del buon ordinamento, quindi esiste un minimo in S, che denotiamo $d = ax_0 + by_0$. Vogliamo provare che $MCD(a, b) = d$, per la (5.2) basta dimostrare che $d|ax + by\ \forall x, y$, prendo $ax + by$ e lo divido per d, vale ovviamente :
$ax + by = d \cdot q + r$ con $0 \leq r < |d|$. Ci basta ora dimostrare che $r = 0$. Supponiamo per *assurdo* che $r > 0$, ciò vorrebbe dire che, essendo $d = ax_0 + by_0$, ho che :

$$ax + by = (ax_0 + by_0) \cdot q + r \implies r = a(x - x_0q) + b(y - y_0q) \tag{20}$$

Essendo di tale forma, vuol dire che essendo maggiore di 0,$r \in S$. Si giunge ad una contraddizione, dato che r è strettamente minore di d, ma abbiamo definito d come il minimo di s, quindi è impossibile che $r > 0$. Essendo $r = 0$, si ha che $d|ax + by$, quindi $d|a$ e $d|b$, d è il massimo comun divisore. ■

Abbiamo visto che tale d può essere scritto nella forma $d = ax_0 + by_0$ per due coefficenti x_0, y_0. Tale forma è detta **identità di Bézout**, e *non è unica*. Vediamo alcune proposizioni:

- 1) se $a \neq 0$ e $a|b$, allora $MCD(a, b) = |a|$
- 2) $MCD(a, \pm a) = a$
- 3) $MCD(a, 0) = a$
- 4) $MCD(\pm 1, a) = 1$
- 5) Siano $a, b, c \in \mathbb{Z}$ tutti diversi da 0, vale che $MCD(ab, ac) = |a| \cdot MCD(b, c)$
- 6) $MCD(a, b) = d \implies MCD(\frac{a}{d}, \frac{b}{d}) = 1$

Definizione : Siano $a, b \neq 0$, se $MCD(a, b) = 1$, allora a e b si dicono *co-primi*. Se due numeri sono co-primi, allora $\exists r, s \in \mathbb{Z}$ t.c. $ar + bs = 1$.
Lemma di Euclide : se $a|bc$ e $MCD(a, b) = 1$ allora $a|c$.
***Dimostrazione* :**
Abbiamo per ipotesi che $ar + bs = 1$, allora $c = c \cdot 1 = c \cdot (ar + bs)$, e per ipotesi essendo $a|bc$ vuol dire che $bc = ax$ per qualche x. allora $c = a(cr) + a(xs) = a(cr + xs) \implies a|c$. ■

Vediamo un importante *lemma*, sappiamo che se $a, b \in \mathbb{Z}$ con $b \neq 0$, si ha che $a = bq + r$ con $0 \leq r < |b|$. Si ha che $MCD(a, b) = MCD(b, r)$.
***Dimostrazione* :**
Sia $d = MCD(a, b)$ e $d' = MCD(b, r)$. In generale, se $a|b$ e $b|a \implies a = \pm b$. Per tale osservazione, dobbiamo dimostrare che $d|d'$ e $d'|d$.

- Sappiamo che $d|a$ e $d|b$, quindi $d|a - bq \implies d|r$, essendo che $d|r$ e $d|b$, si ha che $d|d'$ perchè $d' = MCD(b, r)$.
- Sappiamo che $d'|d$ e $d'|r$, quindi $d'|bq + r \implies d'|a$, essendo che $d'|a$ e $d'|b$, si ha che $d'|d$ perchè $d = MCD(a, b)$.

■

2.2.1 L'Algoritmo Euclideo

Vediamo ora l'algoritmo per trovare il massimo comun divisore di due numeri a, b, per cui vale la condizione $a \geq b > 0$. Vediamo come si fa passo per passo.

- Passo 1) divido a per b, ed ottengo $a = bq_1 + r_1$. Se $r_1 \neq 0$, continuo.
- Passo 2) divido b per r_1, ed ottengo $b = r_1q_2 + r_2$. Se $r_2 \neq 0$, continuo.
- Passo 3) divido r_1 per r_2, ed ottengo $r_1 = r_2q_3 + r_3$. Se $r_3 \neq 0$, continuo.

Osservazione : Procedendo in tal modo, definiamo una successione di interi strettamente decrescente :

$$b > r_1 > r_2 > r_3...$$

Quindi, ad un certo punto, otterremo un resto pari a 0 :

- Passo n) divido r_{n-2} per r_{n-1}, ed ottengo $r_{n-2} = r_{n-2}q_n + r_n$. Se $r_n \neq 0$, continuo.
- Passo $n+1$) divido r_{n-1} per r_n, ed ottengo $r_{n-1} = r_nq_{n+1} + r_{n+1}$. A questo punto ho che $r_{n+1} = 0$

Ho trovato finalmente che $r_{n+1} = 0$, per lemma di Euclide, si ricordi che : $MCD(r_{n-1}, r_n) = MCD(r_n, r_{n+1}) \implies MCD(r_{n-1}, r_n) = MCD(r_n, 0) \implies MCD(r_{n-1}, r_n) = r_n$.
A questo punto risulta chiaro che :

$$MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2)..., = MCD(r_n, 0) = r_n \tag{21}$$

Quindi, $MCD(a, b)$ è uguale all'ultimo resto non nullo.

2.3 Equazioni Diofantee

Un *equazione diofantea* è un equazione della forma :

$$ax + by = c \text{ con } a, b, c \in \mathbb{Z}$$

Dove si vogliono trovare delle soluzioni intere, ossia con $x, y \in \mathbb{Z}$. Tale equazione, ha soluzione intera **se e solo se** il massimo comun divisore fra a e b divide c.

$$\text{con } a, b, c \in \mathbb{Z},\ \exists x, y \in \mathbb{Z} \text{ tale che } ax + by = c \iff MCD(a, b)|c$$

2.3.1 Risoluzione

Vediamo adesso passo-passo come si risolve un equazione di questo tipo:

- 1) Bisogna prima verificare che l'equazione sia risolvibile, si calcoli quindi $MCD(a, b) = d$, se esso divide c, l'equazione ammette soluzione.
- 2) Usare l'algoritmo euclideo2.2.1 per trovare un'identità di Bézout per d, esprimendolo nella forma $d = ax_0 + by_0$, utilizzeremo proprio tali coefficenti (x_0, y_0).
- 3) Moltiplicare (x_0, y_0) per $\frac{c}{d}$, ottenendo $(\tilde{x}, \tilde{y})$=$(\frac{c}{d} \cdot x_0, \frac{c}{d} \cdot y_0)$.
- 4) Per qualsiasi $k \in \mathbb{Z}$, le soluzioni dell'equazione diofantea sono della forma :

$$(\tilde{x} + k \cdot \frac{b}{d}, \tilde{y} - k \cdot \frac{a}{d})$$

Vediamo un *Esempio* di risoluzione, sia :

$$2x + 5y = 3$$

- Uso l'algoritmo di Euclide per trovare $MCD(5,2)$: $(1)5 = 2 \cdot 2 + 1$ $(2)2 = 2 \cdot 1 + 0$. Trovo quindi $MCD(5,2) = 1$.
- Tramite tale algoritmo, identifico anche la combinazione lineare $1 = (-2) \cdot 2 + (1) \cdot 5$.
- Moltiplico $(-2, 1)$ per 3, ottenendo $(-6, 3)$.
- Tutte le soluzioni sono : $(-6 + (k \cdot 5), 3 - (k \cdot 2))$, difatti, per $k = 1$ ho : $2(-6 + 5) + 5(3 - 2) = 3$.

2.4 Il Minimo Comune Multiplo

Il *minimo comune multiplo* fra due numeri a, b, che si indica con $mcm(a, b)$, è quel valore $h \geq 0$ tale che, $a|h$ e $b|h$, e se esiste h' tale che $a|h'$ e $b|h'$, allora $h|h'$. Ne seguono le seguenti osservazioni:

- 1) $mcm(a, 0) = 0$
- 2) $mcm(a, 1) = a$
- 3) $mcm(a.b) = 0 \implies a = o \vee b = 0$

Corollario : Se $a, b \in \mathbb{Z}$ e $a, b \neq 0$, allora $|ab| = MCD(a, b) \cdot mcm(a, b)$, quindi $mcm(a, b) = \dfrac{|ab|}{MCD(a, b)}$.

2.5 I Numeri Primi

Un intero $p \geq 2$ è detto *primo* se i suoi divisori sono esclusivamente ± 1 e $\pm p$. Quindi, segue la seguente osservazione : Se $p|xy$ e $p \nmid x \implies p|y$, è chiaro che p è primo se e solo se, se p divide un prodotto : $p|xy$, $x \neq \pm 1 \implies y = \pm 1$. La generalizzazione di elemento primo è la seguente :

Un elemento p di un anello 3.3 $(\mathbb{Z}, +, \cdot)$ è detto **irriducibile** se:

$$p = xy, x \notin \mathcal{U}(\mathbb{Z}) \implies y \in \mathcal{U}(\mathbb{Z})$$

Un qualsiasi dominio di integrità può presentare elementi primi o irriducibili, se $a \in (A, +, \cdot)$ è primo, allora a è irriducibile (primo $\implies$ irriducibile). non è però vero il contrario, in generale, se un elemento è irriducibile, non è per forza primo (irriducibile $\not\Rightarrow$ primo). Nei numeri interi $\mathbb{Z}$, gli elementi irriducibili sono i numeri primi.

2.5.1 Teorema Fondamentale dell'Aritmetica

Se $n \geq 2$, $n \in \mathbb{N}$, tale n è un prodotto di numeri primi (può essere fattorizzato in numeri primi). Inoltre, tale fattorizzazione ha scrittura :

$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} ..., \cdot p_s^{h_s} \text{ con } h_i \geq 1 \text{ e } s \geq 1$$

Dove $p_1, p_2..., p_s$ sono s primi distinti, e tale scrittura è **unica** a meno dell'ordine dei fattori. Consegue che, preso un qualunque intero z diverso da zero e diverso da ± 1, ha scrittura :

$$z = \pm p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} ..., \cdot p_s^{h_s} \text{ con } h_i \geq 1 \text{ e } p_i \text{ irriducibili} > 1$$

Vediamo una proprietà, sia :

$$a = p_1^{h_1} \cdot p_2^{h_2} ..., \cdot p_s^{h_s}, \qquad b = p_1^{k_1} \cdot p_2^{k_2} ..., \cdot p_s^{k_s}$$

Ammettendo esponenti $h_i = 0$, è possibile scrivere le fattorizzazioni di due interi diversi con gli stessi identici primi distinti, "costringengo" ad essere presenti nella fattorizzazione anche primi che in realtà non apparirebbero, ma grazie ad esponente nullo diventano $p_i^0 = 1$. Date tali fattorizzazioni, si ha che :

$$MCD(a, b) = p_1^{m_1} \cdot p_2^{m_2} ..., \cdot p_s^{m_s}$$

$$mcm(a, b) = p_1^{M_1} \cdot p_2^{M_2} ..., \cdot p_s^{M_s}$$

Dove, per ogni i, tali esponenti sono : $m_i = \min\{h_i, k_i\}$ e $M_i = \max\{h_i, k_i\}$.
Proposizione : Esistono *infiniti* numeri primi. *Dimostrazione* : Supponiamo che i numeri primi siano in un numero finito : $p_1, p_2, p_3..., p_N$. Prendiamo adesso il numero $a = p_1 \cdot p_2 \cdot p_3... \cdot p_N + 1$. Tale numero è un intero positivo maggiore di 1, quindi, per il teorema fondamentale dell'aritmetica, deve per forza avere una fattorizzazione in numeri primi. Tuttavia, se esso viene diviso per ogni primo p_i dà come resto 1, questo è assurdo e ci assicura che i numeri primi sono necessariamente infiniti.
Corollario : $\forall p$ primo, $\nexists \sqrt{p} \in \mathbb{Q}$.

3 Strutture Algebriche Notevoli

Vediamo prima una definizione :

> Sia X un insieme, un **operazione binaria** in X è un *applicazione* $* : X \times X \to X$, ossia che ad ogni elemento del prodotto cartesiano $X \times X$ associa un elemento di X.

Ad esempio, l'operazione somma + nei numeri naturali è un operazione binaria. $(\mathbb{Z}, +)$ è un insieme con un'operazione binaria definita su di esso. Vediamo adesso alcune strutture algebriche notevoli e largamente studiate.

3.1 Definizione di Semigruppo

Il **semigruppo** è un insieme S dotato di un operazione $*$ verificante i seguenti punti :

- **1.1** - $*$ è **associativa**, ossia $(s * s') * s'' = s * s' * s''$.
- **1.2** - $\exists e \in S | e * s = s = s * e \forall s \in S$ dove tale e è detto **elemento neutro**.

Se dovesse accadere che $\forall s, s' \in S | s * s' = s' * s$ si dice che il semigruppo $S, *$ è anche **commutativo**.
Esempio 1 : Sia $S = \{f : X \to X\}$ l'insieme delle funzioni definite su un insieme X, l'operazione $\circ$ detta composizione è associativa, presenta l'elemento neutro (la funzione identità), ma non è commutativa, dato che $f \circ g \neq g \circ f$, quindi $(S, \circ)$ è un semigruppo non commutativo.

3.2 Definizione di Gruppo

Il **gruppo** è un insieme S dotato di un operazione $*$ verificante i punti del semigruppo, ma avendo una condizione aggiunta necessaria :

- **2.1** - $*$ è **associativa**, ossia $(s * s') * s'' = s * s' * s''$.
- **2.2** - $\exists e \in S | e * s = s = s * e \forall s \in S$ dove tale e è detto **elemento neutro**.
- **2.3** - $\forall s \in S \exists s' | s * s' = e = s' * s$ dove s' è detto **inverso** di s.

Esempio 1 : $(\mathbb{N}, +)$ non è un gruppo, ma $(\mathbb{Z}, +)$ si, dato che $\forall x \in \mathbb{Z} \exists -x | x + (-x) = 0$, ovviamente 0 è l'elemento neutro.
Esempio 2 : Sia X un insieme, l'insieme $S = \{f : X \to X \text{ biettiva}\}$ ossia di tutte le funzioni biettive su X, con l'operazione $\circ$ di composizione, è un gruppo, dato che $\forall f \in S \exists f^{-1} | f \circ f^{-1} = d_x$, dove d_x è la funzione identità (l'elemento neutro).

È importante notare che per definizione, l'elemento neutro e, se esiste è unico. La **dimostrazione** è semplice : sia $\tilde{e}$ un'altro elemento neutro su $(S, *)$. dato che $\forall s \in S | s * \tilde{e} = s = \tilde{e} * s \implies \tilde{e} * e = e = e * \tilde{e}$, ma dato che anche e è elemento neutro, $e * \tilde{e} = \tilde{e} = \tilde{e} * e$.

$$\begin{cases} e * \tilde{e} = \tilde{e} = \tilde{e} * e \\ \tilde{e} * e = e = e * \tilde{e} \end{cases} \implies \tilde{e} = e \textbf{ L'elemento neutro è unico.} \tag{22}$$

3.2.1 Il Gruppo Simmetrico S_n

Sia X un insieme ,abbiamo chiamato il gruppo di tutte le sue corrispondenze biunivoche $f : X \to X$ con il simbolo $(S(X), \circ)$, nel caso in cui X sia finito, con cardinalità $|X| = n$, si indicherà con S_n, e prende il nome di **gruppo simmetrico di grado** n. Tale gruppo non è commutativo, data l'operazione di composizione $\circ$. È facile notare come ogni elemento σ di S_n sia una permutazione di $X = \{1, 2, 3, 4..., n\}$, quindi la cardinalità sarà $|S_n| = n!$.

3.3 Definizione di Anello

L'anello $(A, \odot, *)$ è un insieme dotato di 2 operazioni con le seguenti proprietà :

- **3.1** - $(A, \odot)$ è un **gruppo commutativo**, dove O_A è l'elemento neutro.
- **3.2** - L'operazione $*$ è **associativa**.
- **3.3** - Riguardo le due operazioni, valgono le proprietà **distributive** :

$$(a \odot a') * b = (a * b) \odot (a' * b) \tag{23}$$

Per essere un anello, non è necessario che l'operazione $*$ sia commutativa, nel caso dovesse esserlo, l'anello si dice commutativo.
Un anello si dice **unitario** se $\exists u \in A | a * u = a = u * a \forall a \in A$, ossia, se è definito l'elemento neutro sull'operazione $*$.
Un anello commutativo, è detto **privo di divisori dello zero** se :

$$a * b = O_A \implies a = O_A \lor b = O_A \tag{24}$$

Dove si ricordi che O_A è l'elemento neutro definito su $(A, \odot)$.
Se un anello commutativo è privo di divisori dello zero, ed è unitario, si dice **dominio di integrità**.
L'insieme dei numeri interi $(\mathbb{Z}, +, \cdot, 0)$ è un *anello commutativo unitario* con unità 1, privo di divisori dello 0, detto quindi *dominio di integrità.*

Proprietà dell'anello

- **(1)** $\forall a \in A, a \cdot 0 = 0$ ciò si dimostra facilmente, infatti $a \cdot 0 = a \cdot 0 + 0$, ma essendo che $a \cdot 0 = a \cdot (0 + 0)$ si ha $a \cdot 0 + 0 = a \cdot (0 + 0)$, aggiungo ad entrambi i membri $-a \cdot 0$ ed ottengo $-a \cdot 0 + a \cdot 0 + 0 = -a \cdot 0 + a \cdot 0 + a \cdot 0 \implies 0 + 0 = a \cdot 0 + 0 \implies a \cdot 0 = 0.$ ■
- **(2)** $a \cdot (-b) = -(-ab) = (-a) \cdot b$
- **(3)** $(-a) \cdot (-b) = ab$
- **(4)** $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$

In ogni anello unitario (non necessariamente commutativo) $(A, +, \cdot)$ si definisce
$\mathcal{U}(A) = \{a \in A | \exists a' | a \cdot a' = 1 = a' \cdot a\}$, ossia l'insieme degli elementi invertibili di A, ad esempio, nei numeri interi si ha $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$. Si nota facilmente che l'insieme degli elementi invertibili è un gruppo. Vediamo ora un importante proprietà :

$$a, b \in \mathcal{U}(A) \implies a \cdot b \in \mathcal{U}(A)$$

Ossia, il prodotto di due elementi invertibili, è anche esso un elemento invertibile.
Dimostrazione:
Siano a' l'inverso moltiplicativo di a e b' l'inverso moltiplicativo di b, quindi $a, b, a', b' \in \mathcal{U}(A)$.
Ciò vuol dire che $a' \cdot b'$ è l'inverso moltiplicativo di $a \cdot b$, dato che
$(a' \cdot b') \cdot (a \cdot b) = b' \cdot (a' \cdot a) \cdot b = b' \cdot 1 \cdot b = b' \cdot b = 1$, è quindi dimostrato che essendo $a'b'$ l'inverso di ab, essi sono invertibili, per cui fanno parte di $\mathcal{U}(A)$. ■

Notazioni semplificate

Da questo punto in poi useremo le seguenti notazioni semplificate :

- **Gruppo** - $(S, \cdot, 1)$ dove "S" è l'insieme, "$\cdot$" l'operazione, ed "1" l'elemento neutro.
- **Gruppo Commutativo** - $(S, +, 0)$ dove "S" è l'insieme, "+" l'operazione, e "0" l'elemento neutro.
- **Anello** - $(A, +, \cdot, 0)$ dove "S" è l'insieme, "+" la prima operazione, per cui $(A, +)$ risulta un gruppo commutativo, "$\cdot$" la seconda operazione, e "0" l'elemento neutro. Se unitario, si usa "1" come simbolo per l'unità.

3.4 Definizione di Campo

Abbiamo visto che l'insieme degli invertibili di un anello è uguale a tutti quegli elementi, che moltiplicati per un altro elemento dell'insieme, detto *inverso*, sono uguali all'elemento neutro rispetto l'operazione di prodotto. Infatti in un anello, l'inverso esiste per tutti gli elementi rispetto l'operazione di somma (essendo un gruppo), ma non del prodotto.
Da qui possiamo dare la definizione di **campo**, che si denota con $\mathbb{K}, +, \cdot$, e non è altro che un *anello commutativo unitario* per cui vale la seguente proprietà :

$$\forall k \in \mathbb{K}, k \neq 0, \exists k' | k \cdot k' = 1 \text{ dove 1 è l'elemento neutro rispetto all'operazione "}\cdot\text{", e 0 è l'elemento neutro rispetto all'operazione "+".}$$

Quindi un campo, è un anello commutativo unitario per cui esiste l'inverso di ogni elemento rispetto l'operazione di prodotto, difatti vale che $\mathcal{U}(\mathbb{K}) = \mathbb{K} \backslash \{0\}$. Due noti esempi di campo che conosciamo sono il campo dei numeri razionali $\mathbb{Q}$ ed il campo dei numeri reali $\mathbb{R}$.

4 L'Anello $\mathbb{Z}_n$

L'insieme dei numeri interi $\mathbb{Z}$ è il più semplice e chiaro esempio di anello. Vediamo adesso un anello commutativo unitario, **con divisori dello zero**, che non sia quindi dominio di integrità. Definiamo prima di tutto una relazione :

$$a \sim_n b \iff a - b \text{ è divisibile per } n \tag{25}$$

L'insieme $\mathbb{Z}_n \equiv {}^{\mathbb{Z}}/_{\sim_n}$ non è altro che l'insieme quoziente di tale relazione sui numeri interi. Ossia l'insieme delle sue classi di equivalenza. $\mathbb{Z}_n = \{[0], [1], [2]..., [n-1]\}$. Notiamo come la cardinalità di tale insieme sia proprio n, e che :

$$\begin{gathered}
[-1] = [n-1] \text{ perchè } n-1 \sim_n 1 \iff n-1-(-1) = n \\
[0] = [n] \text{ perchè } n \sim_n 0 \iff n-0 = n \\
[1] = [n+1] \text{ perchè } n+1 \sim_n 1 \iff n+1-1 = n \\
[10] = [n+10] \text{ perchè } n+10 \sim_n 10 \iff n+10-10 = n
\end{gathered}$$

Su tale insieme sono definiti somma e prodotto (ben posti):

$$\begin{gathered}
[k] + [h] = [k+h] \\
[k] \cdot [h] = [k \cdot h]
\end{gathered}$$

Ha un elemento neutro per la somma [0], ed uno per il prodotto [1]. L'anello è commutativo ed unitario, però possiede *divisori dello zero*, se prendo ad esempio $\mathbb{Z}_{12}$, nonostante $[3] \neq [4] \neq [0]$, risulta che $[3] \cdot [4] = [12] = [0]$ perchè $12 \sim_{12} 0 \iff 12 - 0 = 12$ e 12 è divisibile per 12. *Osservazione:* Se non si è in un dominio di integrità non è possibile semplificare un equazione, si prenda $\mathbb{Z}_{10}$, sicuramente $[8] = [2][4]$ e $[8] = [28] = [7][4]$, quindi $[7][4] = [2][4]$, semplificando il $[4]$ otterrei $[7] = [2]$ che non è vero.

Notazione : Al posto di $\mathbb{Z}_n$ scriveremo $\pmod n$, e se $a = b \pmod n$, potremmo anche scrivere $a \equiv b \pmod n$.

4.1 Equazioni in $\mathbb{Z}_n$: Congruenze Lineari

In questo paragrafo ci occuperemo di esplicare come si risolve un equazione detta *congruenza lineare*, del tipo :

$$ax \equiv b \pmod n$$

Ossia, trovare un x_0 tale che $ax_0 \equiv b$ in $\mathbb{Z}_n$.
Proposizione : La congruenza lineare $ax \equiv b \pmod n$ ammette soluzioni **se e solo se** $MCD(a, n)|b$. La *Dimostrazione* è semplice, dato che risolvore una congruenza lineare equivale a risolvere un equazione diofantea2.3 del tipo:

$$ax + ny = b$$

Proposizione : Se x_0 è una soluzione di $ax \equiv b \pmod n$, *tutte* le soluzioni di tale congruenza saranno del tipo :

$$x_0 + h \cdot \frac{n}{MCD(a, n)} \text{ con } h \in \mathbb{Z}$$

Ma tale generalizzazione identifica infinite soluzioni congruenti fra loro, le soluzioni diverse $\pmod n$ sono quindi esattamente $d = MCD(a, n)$.
Come accennato precedentemente, per risolvere una congruenza lineare $ax \equiv b \pmod n$, basta risolvere $ax + ny = b$, trovando : $(x_0 + h \cdot \frac{n}{MCD(a,n)}, y_0 + h \cdot \frac{a}{MCD(a,n)})$, e considerando la prima coordinata della coppia.

4.2 La funzione di Eulero

Il *Teorema di Eulero*, enucia che, se n è un intero positivo, ed a è co-primo rispetto ad n, allora è vero che :

$$a^{\varphi(n)} \equiv 1 \pmod n$$

Dove φ è la **funzione di Eulero**, che associa ad ogni n, il numero di tutti gli interi positivi minori di n, che sono co-primi con n (dimostrazione 13.1.1). Ad *esempio* :

- $\varphi(20) = 8$ perchè i co-primi con 20 minori di esso sono : $1, 3, 7, 9, 11, 13, 17, 19$.
- $\varphi(6) = 2$ perchè i co-primi con 6 minori di esso sono : $1, 5$.

Ci occuperemo di capire come calcolare $\varphi(n)$ per ogni intero n della quale si conosca la *fattorizzazione.*

Proposizione : Sia $n = p_1^{h_1} \cdot p_2^{h_2} ... \cdot p_k^{h_k}$ la fattorizzazione in numeri primi di n, dove $\forall i \in \{1, 2..., k\}$, p_i è un numero primo distinto, risulta :

$$\varphi(n) = \varphi(p_1^{h_1}) \cdot \varphi(p_2^{h_2})..., \cdot\varphi(p_k^{h_k})$$

Con tale risultato, non rimane che calcolare il valore di φ sulle potenze dei numeri primi.

Proposizione : Se p è un numero primo, allora :

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

Tale risultato risulta quasi scontato, tutti i numeri co-primi con un numero primo, sono tutti i numeri minori di tale numero, dato che esso non condivide divisori con nessuno. Parlando di potenze, non sono co-primi con p^h, solo i multipli di p, che sono del tipo : $p \cdot i$. Ora per ogni n della quale si conosca la fattorizzazione, siamo in grado di calcolare la sua funzione di Eulero :

- $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3)\varphi(3^2) = (2^3 - 2^2)(3^2 - 3) = (4)(6) = 24$
- $\varphi(8) = \varphi(2^3) = (2^3 - 2^2) = 4$

4.2.1 Gli Invertibili di $\mathbb{Z}_n$

Ricordiamo che $\mathbb{Z}_n$ ha la struttura di un anello commutativo con unità3.3, ha quindi un insieme di elementi invertibili. Vogliamo determinare la cardinalità di tale insieme $\mathcal{U}(\mathbb{Z}_n)$.

Proposizione : In $\mathbb{Z}_n$, gli unici elementi *invertibili* sono quelle classi a tali che $MCD(a, n) = 1$.
Ossia, tutti gli elementi co-primi con n, ed equivale a risolvere la congruenza :

$$ax \equiv 1 \pmod{n}$$

Tale congruenza ammette un unica soluzione, se e solo se $MCD(a, n) = 1$. Gli invertibili, sono esattamente $\varphi(n)$, quindi, se p è primo, tutti gli elementi di $\mathbb{Z}_p$ escluso lo 0 sono co-primi con p, quindi, ogni classe non nulla è invertibile : $|\mathcal{U}(\mathbb{Z}_p)| = \varphi(p) = p - 1$.
Ricordando che un campo è un anello commutativo con unità, per cui ogni elemento non nullo è invertibile, si arriva al seguente risultato :

Se p è un numero primo, allora l'anello $\mathbb{Z}_p$ è un *campo*.

4.2.2 Il Teorema di Eulero

Se $n \geq 2$, $a \in \mathbb{Z}$ e $MCD(a, n) = 1$, allora :

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

4.3 Sistemi di Congruenze e Teorema Cinese del Resto

Osserviamo il seguente *sistema* :

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ ... \\ a_s x \equiv b_s \pmod{n_s} \end{cases} \tag{26}$$

Si vuole trovare una soluzione intera che sia soluzione di tutte le equazioni del sistema. Il sistema per avere soluzione, deve avere ognuna delle sue equazioni risolvibili, quindi

$\forall i, j, i \neq j \implies MCD(a_i, n_i)|b_i$. Prima di vedere la soluzione di tale sistema, si consideri un altro sistema della forma :

$$\begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ ... \\ x \equiv c_s \pmod{r_s} \end{cases} \quad i \neq j \implies MCD(r_i, r_j) = 1 \tag{27}$$

Dove ogni argomento del modulo, è coprimo con tutti gli altri. Tale sistema si dice di tipo *cinese.* Il *teorema cinese del resto* enuncia che, un sistema di questo tipo ammette soluzione ed è **unica** in $(\text{mod } r_1 \cdot r_2 ... \cdot r_s)$.

Dimostrazione(e risoluzione) : Consideriamo il prodotto di tutti gli argomenti dei moduli, ossia $R = r_1 \cdot r_2 ... \cdot r_s$, e, per ogni k-esima equazione del sistema, si consideri $R_k = \dfrac{R}{r_k}$. Risulta ovvio che, essendo R un prodotto di numeri co-primi, $MCD(R_k, r_k) = 1$, quindi ogni congruenza lineare $R_k x \equiv c_k \pmod{r_k}$ ammette una soluzione unica (si ricordi che le soluzioni distinte di una congruenza lineare $ax \equiv b \pmod{n}$ sono in numero $MCD(a, n)$).
Consideriamo adesso, per ogni k-esima equazione del sistema, la sua soluzione $\tilde{x}_k$, che si trova risolvendo l'equazione diofantea (derivante dall'identità di Bézout) $R_k t_k + r_k g_k = 1$, una volta trovato il coefficente t_k, la soluzione è $\tilde{x}_k = t_k c_k$. Una volta trovate le soluzioni di ogni equazione, la soluzione generale del sistema sarà :

$$\tilde{x} = \sum_{i=1}^{s} \tilde{x}_i R_i$$

Quindi, $\forall i, \tilde{x} = c_i \pmod{r_i}$.

Torniamo adesso al caso generale, in cui si ha un sistema del tipo :

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ ... \\ a_s x \equiv b_s \pmod{n_s} \end{cases} \tag{28}$$

Se sono vere alcune supposizioni, ossia:

- Ogni equazione del sistema ammette soluzione, $\forall i, j | i \neq j \implies MCD(a_i, n_i)|b_i$.
- Gli argomenti dei moduli sono tutti co-primi fra loro, $\forall i, j | i \neq j \implies MCD(n_i, n_j) = 1$

Possiamo dividere ogni elemento di ogni equazione del sistema per il corrispettivo massimo comun divisore fra a_i e n_i:

$$d_i = MCD(a_i, n_i) \begin{cases} \frac{a_1}{d_1} x \equiv \frac{b_1}{d_1} \pmod{\frac{n_1}{d_1}} \\ \frac{a_2}{d_2} x \equiv \frac{b_2}{d_2} \pmod{\frac{n_2}{d_2}} \\ ... \\ \frac{a_s}{d_s} x \equiv \frac{b_s}{d_s} \pmod{\frac{n_s}{d_s}} \end{cases} \tag{29}$$

Adesso, si ha che $MCD(\frac{a_i}{d_i}, \frac{n_i}{d_i}) = 1$, quindi $\frac{a_i}{d_i}$ è *invertibile* in (mod $\frac{n_i}{d_i}$). Per ogni equazione del sistema, moltiplico tutto per l'inverso di $\frac{a_i}{d_i}$, ottenendo $x \equiv c_i \pmod{\frac{n_i}{d_i}}$, ottenendo un sistema di tipo cinese, per la quale conosciamo il metodo risolutivo :

$$d_i = MCD(a_i, n_i) \begin{cases} x \equiv c_1 \pmod{\frac{n_1}{d_1}} \\ x \equiv c_2 \pmod{\frac{n_2}{d_2}} \\ ... \\ x \equiv c_s \pmod{\frac{n_s}{d_s}} \end{cases} \tag{30}$$

4.3.1 Seconda Formulazione del Teorema Cinese del Resto

In questa specifica sezione, si farà riferimento ad argomenti trattati nel capitolo 7, si invita quindi il lettore, a soffermarsi su questa sezione esclusivamente dopo aver trattato il capitolo sulla *Teoria degli Anelli.*

Appunto sulla notazione : con $[a]_n$ si definisce la classe di equivalenza di a in $\mathbb{Z}_n$.

Vediamo adesso una definizione differente del teorema cinese del resto, si prenda come esempio un sistema con due sole equazioni :

$$\begin{cases} x \equiv a \pmod r \\ x \equiv b \pmod s \end{cases} \quad MCD(r, s) = 1 \tag{31}$$

Consideriamo adesso *l'applicazione* $F : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ definita nel seguente modo :

$$[x]_{rs} \to ([x]_r, [x]_s) \tag{32}$$

Ossia che ad ogni classe di equivalenza in $\mathbb{Z}_{rs}$, assegna la coppia delle due classi di equivalenza dello stesso intero, ma rispettivamente $\mathbb{Z}_r$ e $\mathbb{Z}_s$.
Ebbene, tale applicazione è ben definita, e vale che :

$$x \equiv x' \pmod{rs} \implies \begin{cases} x \equiv x' \pmod r \\ x \equiv x' \pmod s \end{cases} \tag{33}$$

Ossia, sia l'equazione a sinistra che il sistema a destra hanno la stessa identica soluzione.

Tale applicazione F è un **isomorfismo** di anelli.

Teorema :
Dato il seguente sistema di tipo cinese :

$$\begin{cases} x \equiv a \pmod r \\ x \equiv b \pmod s \end{cases} \quad MCD(r, s) = 1 \tag{34}$$

e date le seguenti condizioni :

- (1) L'applicazione $F : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ è biettiva
- (2) $MCD(r, s) = 1$

- (3) Il sistema ha un'unica soluzione $\text{mod}(r \cdot s)$

Vale che :

$$(1) \iff (2) \iff (3)$$

Ossia che se una qualsiasi delle 3 condizioni è vera, anche le altre sono vere, si implicano a vicenda in maniera circolare.
Dimostrazione :
$\boxed{(2) \implies (1)}$ - Abbiamo come ipotesi le condizioni (2) e (3), supponiamo per assurdo che $MCD(r,s) = d > 1$, sia $mcm(r,s) = h$, per il teorema fondamentale dell'aritmetica, $MCD(r,s) \cdot mcm(r,s) = dh = rs$, quindi $h = \dfrac{rs}{d}$, è chiaro che $h \geq 1$, e che $h < rs$, quindi sicuramente $[h]_{rs} \neq [0]_{rs}$. d'altra parte però, $r|h$ e $s|h$, quindi $[h]_r = [0]_r$ e $[h]_s = [0]_s$, ma se consideriamo l'applicazione F, si ha che :

$$\begin{cases} F([0]_{rs}) = ([0]_r, [0]_s) \\ [0]_r = [h]_r \wedge [0]_s = [h]_s \implies ([0]_r, [0]_s) = ([h]_r, [h]_s) = F([h]_{rs}) \end{cases}$$

Ma abbiamo detto che $[h]_{rs} \neq [0]_{rs}$, quindi F non può essere iniettiva, ma ciò va contro la tesi iniziale, quindi necessariamente $MCD(r,s) = 1$.
$\boxed{(3) \implies (1)}$ - Per ipotesi, $\exists! x | x \equiv a \text{ mod}(r) \wedge x \equiv b \text{ mod}(s)$, quindi, è anche vero che per tale x vale : $x \equiv a \text{ mod}(rs) \wedge x \equiv b \text{ mod}(rs)$, se prendo allora $[x]_{rs}$ ho che $F([x]_{rs}) = ([x]_r, [x]_s) = ([a]_r, [b]_s)$, quindi F è suriettiva. Essendo per l'ipotesi (3) che la soluzione è unica, F è anche iniettiva. Inoltre come ulteriore rafforzante per la nostra tesi, si ha che $|\mathbb{Z}_r \times \mathbb{Z}_s| = |\mathbb{Z}_{rs}|$, Essendo la cardinalità degli insiemi la stessa, se l'applicazione F è iniettiva, è anche necessariamente suriettiva, quindi biettiva. ■
Conclusione - Tale teorema enuncia che avvolte la risoluzione di un'equazione congruenziale è equivalente alla risoluzione di un sistema, e viceversa, ad esempio, la soluzione dei due problemi è equivalente :

$$8x \equiv 3 \text{ mod}(385) \iff \begin{cases} 8x \equiv 3 \text{ mod}(5) \\ 8x \equiv 3 \text{ mod}(7) \\ 8x \equiv 3 \text{ mod}(11) \end{cases} \tag{35}$$

4.4 Piccolo Teorema di Fermat

Sia p un numero primo, vale che : $\forall a \in \mathbb{Z},\ a^p \equiv a \pmod{p}$

Dimostrazione : Si dimostra per induzione.

- Caso Base $a = 0$ - $0^p = 0$
- Passo Induttivo - Per ipotesi, $a^p \equiv a \pmod{p}$, prendiamo $a + 1$, si ha :

$$(a+1)^p = a^p + 1 \tag{36}$$

Ma $a^p \equiv a$ quindi $a^p + 1 \equiv a + 1 \implies (a+1)^p \equiv a^p + 1 \pmod{p}$. ■

5 I Numeri Razionali

Abbiamo definito i numeri naturali, che servono per la definizione degli interi, che useremo a loro volta per definire i **numeri razionali**. Prima però, dobbiamo stabilire una *relazione* su $\mathbb{Z} \times \mathbb{Z} \backslash \{0\}$, ossia sul prodotto cartesiano fra gli interi, e gli interi escluso l'elemento neutro rispetto la somma. Definiamo la relazione ρ in tal modo :

$$(a, b)\rho(c, d) \iff a \cdot d = b \cdot c \tag{37}$$

Ad esempio, $(2, 1)\rho(4, 2)$ perchè $2 \cdot 2 = 4 \cdot 1$, oppure $(3, 2)\rho(6, 4)$ perchè $3 \cdot 4 = 6 \cdot 2$. Definiamo l'insieme dei razionali come l'insieme quoziente del prodotto cartesiano fra gli interi, e gli interi escluso l'elemento neutro rispetto la somma, rispetto la relazione appena definita.

$$\mathbb{Q} = \{{}^{\mathbb{Z} \times \mathbb{Z} \backslash \{0\}}/_{\rho}\}$$

Ossia l'insieme di tutte le classi di equivalenza. Denotiamo poi $0 := [(0, 1)]$ e $1 := [(1, 1)]$. Come abbiamo visto prima, $(2, 1)\rho(4, 2)$, quindi $[(2, 1)] = [(4, 2)]$. Come abbiamo detto in precedenza, $\mathbb{Q}$ è un campo. Definiamo quindi due operazioni, ossia la somma ed il prodotto.

- somma : $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$
- prodotto : $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$

Tali operazioni fra classi di equivalenza sono *ben poste*, ossia non dipendono dalla scelta dei rappresentanti delle classi. Difatti se $[(a, b)] = [(c, d)]$ e $[(a', b')] = [(c', d')]$, si avrà che $[(a, b)] + [(a', b')] = [(c, d)] + [(c', d')]$, ossia che $(ab' + ba', bb')\rho(cd' + dc', dd') \implies (ab' + ba') \cdot dd' = bb' \cdot (cd' + dc')$.

Abbiamo quindi due operazioni con definiti elementi neutri, uno per la somma $0 := [(0, 1)]$ ed uno per il prodotto $1 := [(1, 1)]$, è un anello commutativo unitario, ed inoltre è un campo, dato che presi qualsiasi $[(a, b)]$ con $a \neq 0$ allora $[(a, b)] \cdot [(b, a)] = 1$, questo è di facile verifica dato che $[(a, b)] \cdot [(b, a)] = [(ab, ba)] = [(1, 1)] = 1$ dato che $(ab, ba)\rho(1, 1) \iff ab \cdot 1 = ba \cdot 1$, ed essendo il prodotto definito su $\mathbb{Z}$ commutativo, ciò risulta vero.

L'insieme $\mathbb{Z}$ si identifica come sotto-insieme di $\mathbb{Q}$, dato che c'è un'applicazione iniettiva φ che associa ad ogni intero, la sua classe in $\mathbb{Q}$. Per ogni intero a, si ha $\varphi(a) = [(a, 1)]$. Inoltre, è compatibile con le operazioni di somma e prodotto, dato che:

$$\varphi(a + b) = \varphi(a) + \varphi(b) = [(a, 1)] + [(b, 1)] = [(a \cdot 1 + b \cdot 1, 1 \cdot 1)] = [(a + b, 1)]$$

Si dice che $\mathbb{Z}$ è sotto-insieme di $\mathbb{Q}$, di fatti $\mathbb{Z}$ è in biezione con $\{[(a, 1)] | a \in \mathbb{Z}\}$. L'inverso di $[(a, b)]$ è $[(b, a)]$. Possiamo usare una **notazione semplificata** e denotare ogni elemento:

$$[(a, b)] := \frac{a}{b}$$

Qui risultano chiare note tutte le proprietà e le operazioni fatte sui razionali che svolgiamo fin dalle elementari.

$[(3, 2)] + [(9, 4)] = [(3 \cdot 4 + 2 \cdot 9, 2 \cdot 4)]$ in notazione semplificata risulta $\frac{3}{2} + \frac{9}{4} = \frac{3 \cdot 4 + 2 \cdot 9}{2 \cdot 4} = \frac{12 + 18}{8} = \frac{30}{8} = \frac{15}{4}$ dato che $[(30, 8)] = [(15, 4)] \iff (30, 8)\rho(15, 4) \iff 30 \cdot 4 = 15 \cdot 8$

6 Il Campo dei Numeri Complessi

Un equazione del tipo $3x = 5$ non ha soluzione in $\mathbb{Z}$, si è appunto creata una sua estension $\mathbb{Q}$ che ammette la soluzione $x = \frac{5}{3}$. Un equazione del tipo $x^2 = 2$ non ha soluzione nei numeri razionali, ma la ha in quella dei numeri reali, ossia $x = \sqrt{2}$. Vediamo l'equazione $x^2 + 1 = 0$, è un equazione di secondo grado che non ammette nessuna soluzione reale, di fatto non esistono numeri reali, il quale quadrato equivale a -1. Esiste un estensione di $\mathbb{R}$, definita nel seguente modo.

6.1 Definizione

I **numeri complessi** sono una struttura di questo tipo : si consideri $\mathbb{R}^2 = \{(x, y)|x, y \in \mathbb{R}\}$, ossia tutte le coppie ordinate di numeri reali, ed introduciamo due operazioni :

- **Somma** - $(x, y) + (x', y') = (x + x', y + y')$
- **Prdototto** - $(x, y) \cdot (x', y') = (xx' - yy', xy' + yx')$

Si noti come l'elemento neutro additivo è $(0, 0)$ e l'elemento neutro moltiplicativo $(1, 0)$. Ogni elemento ha un inverso, presa la coppia $(x, y) \neq (0, 0)$ si ha :

$$(x, y)^{-1} = (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}) \tag{38}$$

Dimostrazione :

$$(x, y) \cdot (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}) = (x \cdot \frac{x}{x^2 + y^2} - y \cdot \frac{-y}{x^2 + y^2}, x \cdot \frac{-y}{x^2 + y^2} + y \cdot \frac{x}{x^2 + y^2}) = \tag{39}$$

$$= (\frac{x^2 + y^2}{x^2 + y^2}, \frac{-xy + xy}{x^2 + y^2}) = (1, 0) \quad \blacksquare \tag{40}$$

$(R^2, +, \cdot)$ è un **campo** noto come *campo dei numeri complessi* ed è denotato con $\mathbb{C}$. Esiste un applicazione iniettiva φ da $\mathbb{R}$ a $\mathbb{C}$ che associa $\varphi : x \to (x, 0)$. R è un *sotto-campo* di $\mathbb{C}$, dato che l'applicazione *conserva* le operazioni, i complessi sono quindi un estensione dei reali.

$$\varphi(x \cdot_{\mathbb{R}} x') = \varphi(x) \cdot_{\mathbb{C}} \varphi(x') \tag{41}$$

$$\varphi(x +_{\mathbb{R}} x') = \varphi(x) +_{\mathbb{C}} \varphi(x') \tag{42}$$

L'equazione iniziale $x^2 + 1 = 0$, che possiamo riscrivere $x^2 + (1, 0) = (0, 0)$, ammette soluzione in $\mathbb{C}$, ed è proprio $x = (0, 1)$, difatti :

$$(0, 1)^2 + (1, 0) = (0, 0) \implies (0, 1)(0, 1) + (1, 0) = (0, 0) \implies (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) + (1, 0) = (0, 0) \implies (-1, 0) + (1, 0) = (0, 0) \implies (-1 + 1, 0) = (0, 0) \implies (0, 0) = (0, 0)\checkmark$$

Denoteremo $(a, 0) \equiv a$ per ogni $a \in \mathbb{R}$. Notiamo come qualsiasi numero complesso della forma (a, b) può essere riscritto come $(a, 0) + (0, b)$, ma $(0, b) = (0, 1)(b, 0)$, quindi posso rappresentare ogni numero come $(a, 0) + (0, 1)(b, 0)$, ossia la somma di un reale con un altro reale moltiplicato per $(0, 1)$. Tale numero viene denotato con i, ed è detta **unità immaginaria**, possiamo quindi rappresentare ogni numero complesso nella seguente forma : $(a, b) \equiv a + ib$, con $i^2 = -1$.

6.2 Teorema Fondamentale dell'Algebra

Ogni equazione algebrica con coefficenti complessi (quindi in particolare reali) di grado n, ammette precisamente n soluzioni in $\mathbb{C}$ (contando le moltiplicità). Si dice che $\mathbb{C}$ è **algebricamente chiuso**.

7 Elementi di Teoria degli Anelli

7.1 Isomorfismi e Omomorfismi tra Anelli

Abbiamo visto precedentemente la definizione assiomatica di *Anello*, presentiamo ora un altra importante definizione :

Definizione 1 *Un* ***isomorfismo*** φ *tra due anelli* $(R, +_R, \cdot_R)$ *e* $(R', +_{R'}, \cdot_{R'})$ *è una corrispondenza biunivoca tra* R *e* R' *che conserva le operazioni, tale che*

$$\varphi(a +_R b) = \varphi(a) +_{R'} \varphi(b) \ \forall a, b \in R$$

$$\varphi(a \cdot_R b) = \varphi(a) \cdot_{R'} \varphi(b) \ \forall a, b \in R$$

Se i due anelli sono *isomorfi*, si scrive $R \backsimeq R'$. La relazione di isomorfismo è una relazione di equivalenza, e qualunque proprietà algebrica che vale in R, vale anche in R', e viceversa, godendo delle stesse proprietà, dal punti di vista algebrico sono *indistinguibili*, si considerano quindi uguali due anelli isomorfi.

Spesso fra due anelli, esiste un applicazione che ne conservi le operazioni, ma che non è biunivoca. Si da la seguente definizione:

Definizione 2 *Dati due anelli* $(R, +_R, \cdot_R)$ *e* $(R', +_{R'}, \cdot_{R'})$*, si chiama* ***omomorfismo*** *di* R *in* R' *ogni corrispondenza (non necessariamente biunivoca)* φ *da* R *ad* R' *tale che :*

$$\varphi(r_1 +_R r_2) = \varphi(r_1) +_{R'} \varphi(r_2) \ \forall r_1, r_2 \in R$$

$$\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_{R'} \varphi(r_2) \ \forall r_1, r_2 \in R$$

Se φ è un isomorfismo di due anelli $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$, ovviamente l'unità viene mappata nell'unità : $\varphi(1_A) = 1_B$, la dimostrazione è semplice :

$$\begin{cases} \varphi(1_A) = \varphi(1_A \cdot_A 1_A) = \varphi(1_A) \cdot_B \varphi(1_A) \\ 1_B = (\varphi(1_A))^{-1} \cdot_B \varphi(1_A) = (\varphi(1_A))^{-1} \cdot_B \varphi(1_A) \cdot_B \varphi(1_A) \end{cases} \implies 1_B = 1_B \cdot_B \varphi(1_A) = \varphi(1_A)$$

7.1.1 Nucleo di un omomorfismo

Inoltre si definisce un **nucleo** di omomorfismo φ tra R e R', il sotto-insieme di R costituito da tutti gli elementi che hanno come immagine l'elemento neutro rispetto la somma (lo zero) di R', indicato con $0_{R'}$. Tale nucleo si indica con :

$$Ker\varphi = \{r \in R | \varphi(r) = 0_{R'}\} \tag{43}$$

Esempio :
Prendiamo l'ismorfismo $\varphi : \mathbb{Q} \to \mathbb{Q}$ definito come $\varphi(a) = a + (-2)$, avremo che $Ker\varphi = \{2\}$.

$Ker\varphi$ gode di un importante *proprietà*, moltiplicando un qualunque $a \in Ker\varphi$ per un qualunque $b \in R$, il risultato sarà sempre un elemento di $Ker\varphi$:

$$\text{siano } k \in Ker\varphi \text{ e } r \in R \text{ vale che } \varphi(k \cdot r) = \varphi(k) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0 \tag{44}$$

7.1.2 Ideale di un Anello

Definiamo adesso cos'è un **ideale** :
Un *ideale destro* di un anello R, è un sotto-gruppo additivo I di R, tale che, $\forall a \in I$ e $\forall r \in R$, risulta che $ar \in I$.
Un *ideale sinistro* di un anello R, è un sotto-gruppo additivo I di R, tale che, $\forall a \in I$ e $\forall r \in R$, vale che $r \cdot a \in I$.
Se un ideale è sia sinistro che destro si dice *bilatero*, e si denota nel seguente modo :

$$I \trianglelefteq R \tag{45}$$

Per come l'abbiamo definito prima, è ovvio che il nucleo di un omomorfismo tra due anelli $Ker\varphi$ sia un ideale bilatero. Ogni anello R possiede due ideali detti *banali*, ossia $\{0\}$ e R.

$\{0\}$ è un ideale I di R perchè $\forall a \in R$, essendo 0 l'unico elemento di I, è ovvio che $a \cdot 0 = 0 \cdot a = 0 \in I$.

7.2 Prodotto Diretto di Anelli

Siano $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$ due anelli commutativi unitari, vale che, il risultato del loro prodotto cartesiano, detto **prodotto diretto di anelli**, ha una *naturale struttura* di anello, e preserva le operazioni in tal modo :

$$\begin{gathered}\text{Siano } a, a' \in A \text{ e } b, b' \in B \\ \text{somma : } (a,b) + (a',b') = (a +_A a', b +_B b') \\ \text{prodotto : } (a,b) \cdot (a',b') = (a \cdot_A a', b \cdot_B b')\end{gathered}$$

Quindi $(A \times B, +, \cdot)$ è un anello. L'elemento neutro è $0_{A \wedge B} = (0_A, 0_B)$, ossia la coppia dei due elementi neutri rispettivamente per A e B.

8 Teoria dei Gruppi

In questo capitolo ci occuperemo di studiare le proprietà dei gruppi, ricordiamo la definizione, $(G, *)$ è un gruppo se $*$ è un operazione binaria tale che :

1. $*$ è associativa.
2. $\exists e | g * e = g = e * g$
3. $\forall g \in G\ \exists g' | g * g' = e = g' * g$

Abbiamo già visto che l'elemento neutro e è **unico** e si identifica con 1 oppure 1_G, l'inverso di un elemento g, si denota con g^{-1}.

8.1 Omomorfismo tra Gruppi

Siano $(G, *)$ e $(G', \cdot)$ due gruppi, un applicazione φ tra G e G' si dice **omomorfismo** se :

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b) \text{ con } a, b \in G$$

Ossia se *conserva* l'operazione. Prima abbiamo parlato di gruppo simmetrico, esso stabilisce sempre un omomorfismo iniettivo *canonico* $\varphi : (X, *) \to (S(X), \circ)$. Se un omomorfismo è anche biunivoco, si dice **isomorofismo**.

8.2 Sottogruppi

Definizione : Sia $(G, *)$ un gruppo, e sia $S \subseteq G$, tale che $1_G \in S$, diremo che S è un *sottogruppo* di G, e scriveremo $S \leq (G, *)$ se l'operazione di G :

$$* : S \times S \to S$$

è ben definita su S, e risulta essere chiuso rispetto a $*$, inoltre $\forall s \in S \exists s^{-1} \in S$.

Proposizione : In definitiva, $S \subseteq G$ è un sottogruppo se

- $\forall s_1, s_2 \in S, s_1 * s_2 \in S$
- $\forall s \in S, \exists s^{-1} \in S$

da tali due affermazioni ne consegue che $1_G \in S$. Detto ciò, possiamo implicare dalle 3 affermazioni precedenti un *criterio*, che, se valido, conferma che S sia un sottogruppo :

$$(3)\ \forall s_1, s_2 \in S, s_1 * s_2^{-1} \in S$$

Dimostrazione : Se S è un sottogruppo, $1_G \in S$, quindi $1_G = s * s^{-1} \in S$, per la (3), prendendo $s_1 = 1_G$ ed $s_2 = s$, si ha che $1_G * s^{-1} = s^{-1} \in S$, infine, presi $s_1 = a$ ed $s_2 = b^{-1}$, si ha che $a * (b^{-1})^{-1} = a * b \in S$. Quindi (3) è condizione necessaria e sufficente per dimostrare che S è un sottogruppo di G. ■

Proposizione : L'immagine di un omomorfismo φ, ossia $Im(\varphi) = \{\varphi(g), \forall g \in G\}$, è un *sottogruppo.*
Dimostrazione : Siano $y_1, y_2 \in Im(\varphi)$, ciò implica che $y_1 * y_2^{-1} \in Im(\varphi)$, per ipotesi, $\exists g_1, g_2 | y_1 = \varphi(g_1) \wedge y_2 = \varphi(g_2)$. Si ha che $y_1 * y_2^{-1} = \varphi(g_1) * \varphi(g_2)^{-1}$, essendo φ un omomorfismo, tale scrittura è equivalente a $\varphi(g_1) * \varphi(g_2^{-1}) = \varphi(g_1 * g_2^{-1})$, quindi in definitiva $y_1 * y_2^{-1} = \varphi(g_1 * g_2^{-1})$. ■

Ogni omomorfismo è un sottogruppo.

Ogni gruppo ha sempre due *sottogruppi banali*, ossia il gruppo identità $(1_G, *)$ ed il gruppo stesso.

8.2.1 Esempi di Sottogruppi

Esempio 1 Si consideri il gruppo $(\mathbb{R} \backslash \{0\}, \cdot)$ ho che $(\mathbb{R}^{>0}, \cdot)$ è un suo sottogruppo, se prendo due qualsiasi $a, b \in \mathbb{R}^{>0}$, ho che $a \cdot b^{-1} \in \mathbb{R}^{>0}$.

Esempio 2 Si consideri $(\mathbb{Z}, +)$, e considero l'insieme $n\mathbb{Z} = \{nh, h \in \mathbb{Z}\}$, ossia tutti i multipli di n, si ha che $(n\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$, infatti, presi due qualsiasi $nh_1, nh_2 \in n\mathbb{Z}$ ho che $nh_1 + nh_2^{-1} = nh_1 - nh_2 = n(h_1 - h_2) \in n\mathbb{Z}$.

Esempio 3 Considero il gruppo $(\mathbb{Z}_n, +)$, prendo un intero d tale che d divide n, ossia $n = kd$ per qualche k. Considero adesso l'insieme :

$$H_d := \{[d], [2d], [3d], [4d]..., [(k-1)d], [n]\}$$

Tale insieme H_d rispetto a $+$ è un sottogruppo di $(\mathbb{Z}_n, +)$, dato che presi due qualsiasi a, b, ho che $[ad] - [bd] = [ad - bd] = [(a-b)d] \in H_d$.

8.3 I Sottogruppi di $\mathbb{Z}$ e $\mathbb{Z}_n$

In questo paragrafo enunceremo e dimostreremo due proposizioni piuttosto importanti, che descrivono la totalità dei sottogruppi di due gruppi a noi molto noti.

Proposizione 1 : Se H è un sottogruppo di $(\mathbb{Z}, +)$, allora $\exists n | n\mathbb{Z} = H$.
Dimostrazione 1 : Per ipotesi $H \leq (\mathbb{Z}, +)$, quindi $H \cap \mathbb{N} \neq \emptyset$, perché se $a \in H$, allora anche $-a \in H$, quindi H contiene elementi positivi. Per principio del buon ordinamento, H ha un minimo (positivo), sia esso n. Siccome H è un gruppo, ogni multiplo di n è in H, vale a dire che $n\mathbb{Z} \subset H$.
Affermiamo che ogni elemento di H sia divisibile per n, questo perchè, per qualsiasi $a \in H$ si ha $a = qn + r$, ricordando che $0 \leq r < n$, ma n è il minimo positivo, quindi $r = 0$, allora ogni elemento è divisibile per n, ne concludiamo che $H \subset n\mathbb{Z}$.

$$\begin{cases} H \subset n\mathbb{Z} \\ n\mathbb{Z} \subset H \end{cases} \implies n\mathbb{Z} = H$$

■

tutti i sottogruppi di $\mathbb{Z}$ sono del tipo $n\mathbb{Z}$.

Proposizione 2 : Se H è un sottogruppo di $(\mathbb{Z}_n, +)$, allora $\exists d$ tale che d divide n, ossia $n = kd$, quindi $H = H_d := \{[d], [2d], [3d], [4d]..., [(k-1)d], [n]\}$.
Dimostrazione 2 : Consideriamo l'insieme $H' = \{a \in \mathbb{Z} | [a] \in H\}$, ovviamente, $[0] = [n] \in H$, quindi $0 \in H'$. Anche $n \in H'$, risulta chiaro che $H' \neq \emptyset$ ed è un sottogruppo di $\mathbb{Z}$. Siano $a, b \in H'$, essendo un sottogruppo, $a + b^{-1} = a - b \in H'$, ne consegue che $[a - b] \in H \iff a - b \in H'$, sapendo che $H' \leq (\mathbb{Z}, +)$, per la *proposizione 1* appena vista, $\exists d | d\mathbb{Z} = H'$, avendo già visto che $n \in H'$, sappiamo ora che n è un multiplo di d, quindi è chiara la struttura dell'insieme $H' = \{d, 2d, 3d, 4d..., n\}$, avendo detto all'inizio che $H' = \{a \in \mathbb{Z} | [a] \in H\}$, è ovvio che $H = H_d$. ■

tutti i sottogruppi di $\mathbb{Z}_n$ sono del tipo H_d.

Ad esempio, i sottogruppi di $(\mathbb{Z}_{12}, +)$ sono :

$$\{[0]\}, \mathbb{Z}_{12}, H_2, H_3, H_4, H_6$$

Essendo $n = kd$, la cardinalità di H_d è k. Se un gruppo ha cardinalità finita, la sua cardinalità identifica il suo **ordine**. Per i gruppi finiti, è possibile considerare la *tabella moltiplicativa* :

*	1	g_1	g_2	g_3	...	g_n
1	1+1					
g_1				$g_3 + g_1$		
g_2						
g_3			$g_2 + g_3$			
...						
g_n						$g_n + g_n$

8.4 Gruppo Ciclico e Classi Laterali

8.4.1 Gruppo Generato

Prima di parlare dell'argomento di tale paragrafo, introduciamo una notazione :

Sia $(G, *)$ un gruppo, preso $g \in G$ e $t \in \mathbb{Z}$, si ha la seguente notazione :

$$g^t = \begin{cases} 1_G \text{ se } t = 0 \\ g * g * g ... * g \text{ per } t\text{-volte se } t > 0 \\ g^{-1} * g^{-1} * g^{-1} ... * g^{-1} \text{ per } t\text{-volte se } t < 0 \end{cases}$$

Ne segue :

- $g^s * g^t = g^{s+t}$
- $g^{-t} = (g^{-1})^t = (g^t)^{-1}$

L'insieme $\{g^t, t \in \mathbb{Z}\}$ è un sotto-gruppo di G, dato che presi g^{t_1} e g^{t_2}, si ha che:

$$g^{t_1} * (g^{t_2})^{-1} = g^{t_1} * g^{-t_2} = g^{t_1 - t_2} \in \{g^t, t \in \mathbb{Z}\}$$

Questo sottogruppo ha simbolo $\langle g \rangle$ ed è denominato sottogruppo **generato** da g.

Definizione : Sia $(G, *)$ un gruppo ed $H \leq (G, *)$, H è detto sottogruppo **ciclico** se $\exists h \in H | H =< h >$, ed in generale, $(G, *)$ è un gruppo **ciclico** se $\exists g \in G | G =< g >$, ossia è generato da un suo elemento. Se $(G, *)$ è ciclico, allora è **commutativo**, dato che $g^s + g^t = g^{s+t} = g^t + g^s$.
Esempio : $(\mathbb{Z}, +)$ è un gruppo ciclico perché è generato dal numero 1, infatti, $\mathbb{Z} = \langle 1 \rangle$ (vale anche per -1), dato che $\forall k \in \mathbb{Z}$ è vero che $k = 1^k = 1 + 1 + 1 ... + 1$ k-volte.
Anche $(\mathbb{Z}_n, +)$ è ciclico, dato che $\mathbb{Z}_n = \langle [1] \rangle$.

8.4.2 Classi Laterali Destre e Sinistre

Introduciamo adesso quelle che sono le *classi laterali* di un sottogruppo.
Sia H un sottogruppo di $(G, *)$, dove G non è necessariamente finito, l'insieme H ha una **classe laterale sinistra** associata ad ogni $a \in G$, ed è l'insieme $aH = \{a * h, h \in H\}$, analogamente, la **classe laterale destra** associata ad ogni $a \in G$, è l'insieme $Ha = \{h * a, h \in H\}$. Se $(G, *)$ è commutativo, allora $aH = Ha$, altrimenti, non è generalmente vero.
Esempio : consideriamo il gruppo simmetrico S_3, ed il suo sottogruppo $H = \left\{1, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}$, prendo $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, avrò che :

$$aH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \qquad Ha = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Seguono 3 importanti **proposizioni** :

- (1) $a, b \in G$, $aH = bH \iff a^{-1} * b \in H$
- (2) $a, b \in G \implies aH = bH$ oppure $aH \cap bH = \emptyset$
- (3) $\forall x \in G \exists a \in G | x \in aH$

Osservando le proposizioni (1),(2) e (3), risulta chiaro che, tutte le classi laterali sinistre forniscono una *partizione* di G, che denotiamo con $\mathcal{L}_S$.
Tale partizione $\mathcal{L}_S$, definisce anche una relazione di equivalenza :

$$a\rho_S b \iff \exists g \in G | a \in gH \wedge b \in gH$$

Osservazione : $a\rho_S b \iff a^{-1} * b \in gH$.
Esiste la partizione analoga $\mathcal{L}_D$, con le classi laterali destre, che definisce la relazione :

$$a\rho_D b \iff a * b^{-1} \in Hg$$

In generale, $\rho_S \neq \rho_D$. Se G è finito, **l'indice** di H in G è il numero di classi laterali sinistre, che è uguale al numero di classi laterali destre.

8.4.3 Teorema di Lagrange

Sia $(G, *)$ un gruppo finito, e H un suo sottogruppo, vale che la cardinalità dell'insieme H *divide* la cardinalità dell'insieme G, l'ordine di H è un divisore dell'ordine di G.

$$|G| = i \cdot |H|$$

Dimostrazione : Sia H un sottogruppo di $(G, *)$ osserviamo che, esiste una mappa biettiva φ fra H ed una classe laterale sinistra $\varphi : H \to aH \ \forall a$, tale mappa è definita come : $h \to a * h$, quindi, la cardinalità di H è uguale alla cardinalità di aH.
Consideriamo adesso $\{a_1H, a_2H, a_3H..., a_iH\}$, ossia l'insieme di tutte le classi laterali distinte. Essendo che le classi definiscono una partizione, e sono fra loro tutte disgiunte, risulta chiaro che la somma delle loro cardinalità da la cardinalità di G :

$$|G| = \sum_{j=1}^{i} |a_jH| \tag{46}$$

Inoltre, è anche ovvio che le partizioni ricoprono totalmente G :

$$G = \bigcup_{j=1}^{i} (a_jH) \tag{47}$$

Le classi laterali hanno tutte la stessa cardinalità, quindi se sono in numero i, e vale che, per un qualsiasi a, la cardinalità di H è uguale alla cardinalità di aH, è vero che $|G| = i \cdot |H|$. ■

Proposizione : $\rho_S = \rho_D \iff aH = Ha \ \forall a \in G$

Definizione : Se $\rho_S = \rho_D$, allora H è detto sottogruppo **normale** e si denota con $H \trianglelefteq G$.

Proposizione (Criterio importante): Sia $h \in H$, $\quad H \trianglelefteq G \iff a * h * (a^{-1}) \in H \ \forall a \in G$.

8.4.4 Nucleo di un Omomorfismo

Se φ è un omomorfismo, l'insieme $Ker\varphi = \{g \in G | \varphi(g) = 1_G\}$ è detto **nucleo** di φ ed è un sotto-gruppo di G, è di facile dimostrazione :

$$\varphi(g_1 \cdot g_2^{-1}) = \varphi(g_1) \cdot \varphi(g_2^{-1}) = \varphi(g_1) \cdot \varphi(g_2)^{-1} = 1_G \cdot 1_G = 1_G \in Ker\varphi \tag{48}$$

Proposizione : φ è iniettiva $\iff Ker\varphi = \{1_G\}$.
Dimostrazione : Inizianmo dimostrando $\boxed{\varphi \text{ è iniettiva } \implies Ker\varphi = \{1_G\}}$, L'ipotesi è che φ sia iniettiva, prendo un qualsiasi $g \in Ker\varphi$, ed ho che $\varphi(g) = 1_G = \varphi(1_G)$, ma dato che φ è iniettiva, ciò è vero se e solo se $g = 1_G$, quindi $Ker\varphi = \{1_G\}$. Adesso dimostriamo $\boxed{Ker\varphi = \{1_G\} \implies \varphi \text{ è iniettiva}}$, ho che $\varphi(g) = \varphi(g')$, ed inoltre $\varphi(g) \cdot \varphi(g')^{-1} = 1_G$, ed essendo che φ è un omomorfismo, ho $\varphi(g \cdot g'^{-1}) = 1_G$, per ipotesi
$g \cdot g'^{-1} \in Ker\varphi \implies g \cdot g'^{-1} = 1_G \implies$ per unicità inverso $\implies g = g' \implies \varphi$ è iniettiva. ■

8.5 Struttura dei Gruppi Ciclici

Abbiamo già dato la definizione di gruppo ciclico, ossia un gruppo G, per cui risulta che, preso $g \in G$, si ha che $G = \langle g \rangle$.

8.5.1 Ordine di g

Definizione : In un gruppo ciclico G per cui $G = \langle g \rangle$, sia n il numero naturale *più piccolo* tale che $g^n = 1$, si dice che g ha **ordine** n e si denota $o(g) = n$, se tale n non esiste, allora g ha ordine infinito.

$$o(g) = \min(n \geq 1 | g^n = 1) \tag{49}$$

Proposizione : Se $G = \langle g \rangle$ e $o(g) = n$, allora $G = \{1, g, g^2, g^3 ..., g^{n-1}\}$.
È chiaro che, l'ordine di un gruppo ciclico, ossia la sua cardinalità, è l'ordine del suo generatore.

Se un gruppo è ciclico, quindi $G = \langle g \rangle$, esso è generato o da un elemento di ordine finito, oppure da un elemento di ordine infinito, vediamo nel dettaglio i due casi :

Caso 1 $o(g) = \infty$: g è il generatore del gruppo G, definisco un applicazione $\varphi : \mathbb{Z} \to G$ definita come $\varphi : m \to g^m$, si ricordi che $\mathbb{Z} = \langle 1 \rangle$, tale applicazione, è un *omomorfismo* :

$$\varphi(m + n) = g^{m+n} \tag{50}$$

Risulta essere anche biettiva, è quindi un *isomorfismo*, essendo ovviamente iniettiva, $Ker\varphi = \{0\}$, ricordando com'è definito il nucleo :

$$Ker\varphi = \{m \in \mathbb{Z} | \varphi(m) = 1_G\} = \{m \in \mathbb{Z} | g^m = 1_G\}$$

Si noti che il più piccolo elemento di tale insieme è proprio $o(g)$, che però sappiamo per ipotesi essere infinito, quindi l'unico $m \in \mathbb{Z} | g^m = 1_G$ è esattamente $m = 0 \implies Ker\varphi = \{0\}$.
Osservazione : Se φ è un isomorfismo, allora stabilisce una corrispondenza biunivoca fra i sottogruppi di G.
Esiste un unico gruppo ciclico infinito (a meno di isomorfismi) ed è $(\mathbb{Z}, +)$.
Caso 2 $o(g) = n$: g è il generatore del gruppo G, definisco un applicazione $\varphi : \mathbb{Z}_n \to G$ definita come $\varphi : [m] \to g^m$, tale φ è ben definita ed è un omomorfismo :

$$\text{se } [m] \equiv [m'] \implies m' = m + nk \implies g^{m'} = g^{m+nk} = g^m * g^{nk} = g^m * (g^n)^k \tag{51}$$

Si ricordi che $g^n = 1_G$:

$$g^m * g^{nk} = g^m * 1_G^k = g^m \text{ abbiamo dimostrato che } [m] \equiv [m'] \implies g^m = g^{m'} \tag{52}$$

Inoltre essendo $G = \{1, g, g^2, g^3 ..., g^{n-1}\}$, ho che $\forall k \in \mathbb{Z}, k \to g^k$, φ è suriettiva. Essendo che $|G| = |\mathbb{Z}_n|$, φ è biettiva.

Fatta questa breve disquisizione possiamo enunciare un importante teorema, non prima però di una fondamentale *Osservazione* : Abbiamo visto che, $H \leq (\mathbb{Z}, +) \implies \exists n \in \mathbb{Z} | H = n\mathbb{Z}$, e che $H \leq (\mathbb{Z}_n, +) \implies H = H_d = \{[d], [2d] ..., [(k-1)d], [0]\}$ con $n = dk$. Si ricordi che un isomorfismo $\varphi : G \to G'$ definisce una corrispondenza biunivoca fra i sottogruppi di G e G'.

8.5.2 Teorema di Struttura dei Gruppi Ciclici

1. Se $H \leq G = \langle g \rangle$, allora H è ciclico.
2. Se $H \leq G = \langle g \rangle$ e $|G| = n = o(g)$, allora l'ordine di H divide n.
3. $\forall k$ tale che $n = k \cdot c$ per qualche c (per ogni k divisore di n), $\exists! H \leq G$ tale che $|H| = k \implies H = \langle g^{\frac{n}{k}} \rangle$

Se $G = \langle g \rangle$ e $o(g) = n$ allora esiste una corrispondenza biunivoca tra i divisori di n ed i sottogruppi di G.

$$\begin{gathered}\{\text{divisori di } n\} \to \text{ sottogruppi di } G \\ k \to \langle g^{\frac{n}{k}} \rangle\end{gathered}$$

Notare che $| \langle g^{\frac{n}{k}} \rangle | = k$. Se $h|k \wedge k|n$, allora $\langle g^{\frac{n}{h}} \rangle$ è un sottogruppo di $\langle g^{\frac{n}{k}} \rangle$. (Dimostrazione 13.1.3) Quindi, il teorema di struttura dei gruppi ciclici si ottiene dall'isomorfismo $\varphi : \mathbb{Z}_n \to G$. Essendo ogni gruppo ciclico riconducibile a $\mathbb{Z}_n$, si può dire che, un gruppo ciclico ha tanti sottogruppi quanti sono i divisori di n.

8.5.3 Proprietà dell'Ordine

Proposizione : In un gruppo $(G, \cdot)$ se $g^t = 1$ (assumendo che $o(g) < \infty$), allora $o(g)$ divide t. Ciò è di facile dimostrazione, se $o(g)$ divide t si ha $t = k \cdot o(g) + r$ con $r < o(g)$, si ha che $g^t = g^{ko(g)+r} = (g^{o(g)})^k \cdot g^r = g^r = 1 \iff r = 0$. ∎

Vediamo una **proprietà aritmetica** dell'ordine, se $o(g) < \infty$, allora :

$$o(g^s) = \frac{\text{mcm}(o(g), s)}{s} = d$$

Preso un omomorfismo $\varphi : G \to G'$, è lecito chiedersi se in qualche modo c'è un collegamento fra $o(g)$ e $o(\varphi(g))$. Si vedano le seguenti proposizioni :
Proposizione 1 : $o(\varphi(g))$ divide $o(g)$.
Dimostrazione 1 : $1 = g^{o(g)} \implies \varphi(1) = \varphi(g^{o(g)})$, essendo che φ è un omomorfismo, riscrivo quest'ultimo come $\varphi(g)^{o(g)}$, si ricordi che per qualsiasi omomorfismo, $\varphi(1) = 1$, quindi $\varphi(g^{o(g)}) = \varphi(g)^{o(g)} = 1$, per la definizione di ordine, per la definizione di ordine appena vista, $o(\varphi(g))|o(g)$. ∎
Proposizione 2 : Se φ è iniettiva, allora $o(\varphi(g)) = o(g)$.

Dimostrazione 2 : $G = \{1, g ..., g^{o(g)-1}\}$ presenta elementi a coppie distinti, essendo φ iniettiva, anche le loro immagini risultano a coppie distinte, per definizione di ordine, $o(\varphi(g)) \geq o(g)$, necessariamente $o(\varphi(g)) = o(g)$. ∎ Attenzione ! Questa specifica dimostrazione, l'ho copiata per come l'ho scritta dagli appunti presi in classe, non mi è chiara e credo di essermi perso qualcosa, chiunque disponga di una dimostrazione completa, è pregato di scrivermi in modo tale che io possa aggiornare e correggere questa sezione.

Teorema : Sia n primo, allora $(\mathcal{U}(\mathbb{Z}_n), \cdot)$ è isomorfo a $(\mathbb{Z}_{n-1}, +)$, ossia, esiste un $a \in \mathcal{U}(\mathbb{Z}_n)$ per cui $o(a) = n - 1$.
Per dimostrare tale teorema si necessita di alcune osservazioni e proposizioni :

Proposizione : Sia G un gruppo commutativo, se $a, b \in G$ di ordine $o(a) = n$ e $o(b) = m$, allora esiste $c \in G$ tale che $o(c) = \text{mcm}(o(a), o(b))$.
Dimostrazione della proposizione : Consideriamo l'elemento ab e calcoliamone l'ordine, osserviamo che $(ab)^{mn} = (a^n)^m \cdot (b^m)^n = 1 \implies o(ab)$ divide mn, tuttavia, non è detto che $o(ab) = mn$, infatti, si prenda il caso $a = x$ e $b = x^{-1}$, si ha che $ab = 1$, e $1 = o(1) < o(a) = o(b) = n$.
In generale, se $(ab)^t = 1$, allora $1 = (ab)^t = a^t b^t \implies a^t = b^{-t} \implies o(a^t) = o(b^{-t})$. Ciò suggerisce la seguente osservazione.

Osservazione 1 : Se $n = o(a)$ e $m = o(b)$ sono coprimi, allora $o(ab) = nm = mcm(n, m)$.
Dimostrazione dell'osservazione 1 : Per quanto visto sopra,
$a^{o(ab)} = b^{-o(ab)} \implies 1 = (a^{o(ab)})^n = (b^{-o(ab)})^n = b^{-n \cdot o(ab)} \implies o(b) = m$ divide $n \cdot o(ab)$, essendo m ed n coprimi, necessariamente m divide $o(ab)$, analogamente, si ha l'identità $1 = a^{m \cdot o(ab)}$, ed implica che n divide $o(ab)$, di conseguenza, nm divide $o(ab)$, che è ciò che si voleva dimostrare nell'osservazione 1. $\square$
Tornando alla proposizione, rimane da considerare il caso in cui n, m abbiano fattori comuni, ciò si riduce al caso precedente nel seguente modo :
Si fattorizza in primi :

$$\text{mcm}(n, m) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots \cdot p_k^{\alpha_k} \tag{53}$$

Ogni fattore $p_i^{\alpha_i}$ o divide n oppure divide m (si è visto nel capitolo 2.5.1), se G contiene un elemento g di ordine s, e d divide s, allora G contiene un elemento di ordine d, questo ci permette di costruire per ogni $j = 1, 2..., k$ un elemento c_j per cui $o(c_j) = p_j^{\alpha_j}$. Consideriamo il prodotto di tutti questi elementi : $c := c_1 \cdot c_2..., \cdot c_k$, si noti :

Osservazione 2 : $o(c) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots \cdot p_k^{\alpha_k} = \text{mcm}(n, m)$.
Dimostrazione dell'osservazione 2 : Facciamo induzione sul parametro k, ossia il numero di fattori :
caso base : $o(c_1 \cdot c_2..., \cdot c_j) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots \cdot p_j^{\alpha_j}$
ipotesi induttiva : $o(c_1 \cdot c_2..., \cdot c_{j+1}) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots \cdot p_{j+1}^{\alpha_{j+1}}$
Siccome $o(c_1 \cdot c_2..., \cdot c_j)$ e $o(c_{j+1})$ sono coprimi, posso applicare l'*osservazione 1* e trovare che $o((c_1 \cdot c_2..., \cdot c_j) \cdot o(c_{j+1})) = o(c_1 \cdot c_2..., \cdot c_j) \cdot o(c_{j+1})$ come volevasi dimostrare, quindi abbiamo dimostrato l'osservazione 2 e la proposizione. $\square$
Applichiamo adesso la proposizione per dimostrare il teorema.

Dimostrazione del teorema : Vogliamo vedere che $\exists a \in \mathcal{U}(\mathbb{Z}_n) | o(a) = n - 1$. Possiamo prendere un elemento di ordine massimo, dato che $\mathcal{U}(\mathbb{Z}_n)$ è finito, ogni elemento ha ordine finito, prendiamo allora $a \in \mathcal{U}(\mathbb{Z}_n)$ tale che $o(a) = m$, dove m è l'ordine massimo :
$\forall h \in G, o(h) \leq m = o(a)$. Chiaramente, $m \leq n - 1$, ma a priori non vale l'uguaglianza, notiamo la seguente osservazione :

Osservazione 3 : Ogni elemento $b \in \mathcal{U}(\mathbb{Z}_n)$ ha ordine che divide l'ordine massimo $m = o(a)$.

Dimostrazione dell'osservazione 3 : Si utilizza la *proposizione*, se esistesse b di ordine che non divide $m = o(a)$, allora, essendo $\mathcal{U}(\mathbb{Z}_n)$ commutativo, esisterebbe $c \in \mathcal{U}(\mathbb{Z}_n)$ di ordine $o(c) = \text{mcm}(o(a), o(b)) > o(a)$ (dato che $o(b)$ non divide $o(a)$). Tuttavia, era stato scelto a che ha ordine massimo, questo produce una contraddizione e dimostra l'osservazione 3. $\square$.
Dunque, $\forall b \in \mathcal{U}(\mathbb{Z}_n), b^m = 1$ dove $m = o(a)$, in altri termini, $b \in \mathcal{U}(\mathbb{Z}_n)$ non è altro che una soluzione del polinomio $x^m - 1 = 0$ a coefficenti nel campo $\mathbb{Z}_n$ (si è usato il termine campo perché n è primo, come si è visto nel capitolo 4.2.1), essendo un campo, per il teorema fondamentale dell'algebra 6.2, il polinomio $x^m - 1 = 0$ ha al più m soluzioni. Ne deduciamo che $m \geq |\mathcal{U}(\mathbb{Z}_n)| = n - 1$, e di conseguenza, che $m = n - 1$. $\blacksquare$

Faccio un osservazione, e noto che $\mathbb{Z}_6 = \langle [1] \rangle = \langle [5] \rangle$, infatti :

$$\langle [5] \rangle = \{[5], [5^2] = [10] \equiv [4], [5^3] = [15] \equiv [3]..., [5^6] = [30] \equiv [0]\} \tag{54}$$

Proposizione : Se G è generato da g ed è di ordine n, allora, G è anche generato da $\langle g^t \rangle$ se $\text{MCD}(n, t) = 1$.

Dimostrazione : $\langle g^t \rangle = G \iff o(g^t) = n \iff \text{MCD}(n, t) = 1$. $\blacksquare$ Quindi, i generatori di un gruppo ciclico di ordine n, sono precisamente tanti, quanti sono i numeri *coprimi* con n minori di n, che sono precisamente in numero $\varphi(n)$, dove φ è la funzione di Eulero 4.2.

8.5.4 *Esercizio* : Esempio di Studio dei Sottogruppi

Vediamo adesso, un *esempio* di studio dei sottogruppi di un gruppo ciclico, si consideri il gruppo :

$$\mathbb{Z}_{12} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [0], \}$$

Quali sono i suoi sottogruppi? Prima dobbiamo chiederci, quali sono i divisori di 12? Sono esattamente : 1,2,3,4,6 ed ovviamente 12. Per il teorema di struttura dei gruppi ciclici, per ogni divisore k è associato il sottogruppo $\left\langle g^{\frac{n}{k}} \right\rangle$, che in notazione additiva per $\mathbb{Z}_{12}$ sarebbe $\left\langle \frac{n}{k} \cdot [1] \right\rangle$ quindi avremo i sottogruppi :

- $k = 2 \implies \left\langle g^{12/2} \right\rangle \implies \langle g^6 \rangle \implies \langle [6] \rangle = \{[6], [12] \equiv [0]\}$
- $k = 3 \implies \left\langle g^{12/3} \right\rangle \implies \langle g^4 \rangle \implies \langle [4] \rangle = \{[4], [8], [12] \equiv [0]\}$
- $k = 4 \implies \left\langle g^{12/4} \right\rangle \implies \langle g^3 \rangle \implies \langle [3] \rangle = \{[3], [6], [9], [12] \equiv [0]\}$
- $k = 6 \implies \left\langle g^{12/6} \right\rangle \implies \langle g^2 \rangle \implies \langle [2] \rangle = \{[2], [4], [8], [10], [12] \equiv [0]\}$

Inoltre se $k|12$ e $h|k$, allora $\left\langle [\frac{12}{h}] \right\rangle$ è un sottogruppo di $\left\langle [\frac{12}{k}] \right\rangle$, ad esempio, 4|12 e 2|4, quindi $\langle [6] \rangle \leq \langle [3] \rangle$. Essere sotto-gruppi stabilisce una relazione di ordine parziale 1.5, che può essere rappresentata con il diagramma di *Hasse* :

$$\begin{tikzcd}
 & \langle [4] \rangle \arrow[r, dash] & \langle [2] \rangle \arrow[dr, dash] & \\
\langle [12] \rangle \arrow[ur, dash] \arrow[dr, dash] & & & \mathbb{Z}_{12} \\
 & \langle [6] \rangle \arrow[r, dash] \arrow[uur, dash] & \langle [3] \rangle \arrow[ur, dash] &
\end{tikzcd}$$

8.6 Gruppi Normali

Riprendendo la definizione di classi laterali 8.4.2, si ricordi che se H è un sottogruppo di G, è detto *normale*, e si denota con $H \trianglelefteq G$, se le sue classi laterali destre e sinistre sono equivalenti

$$Ha = aH$$

Proposizione : $H \trianglelefteq G \iff \rho_S = \rho_D$.

Proposizione : $H \trianglelefteq G \iff \forall a \in G, ah(a^{-1}) \in H$.
Dimostrazione : $H \trianglelefteq G \implies aH = Ha, \forall a \implies \forall h \in H, ah \in Ha \wedge ha \in aH \implies ah = h'a$ per qualche $h' \in H$ e $ha = ah''$ per qualche $h'' \in H$, ciò implica : $ah(a^{-1}) = h' \in H$, ne segue che $ah = h'a \implies aH \subseteq Ha$ ed analogamente $Ha \subseteq aH$. ■

Ricordando che l'indice di H è il numero delle classi laterali, si ha la seguente :

Proposizione : Se H è un sottogruppo di indice 2, allora è normale, dato che le sue classi laterali, essendo 2 sono : $G = H \cdot 1 \cup H \cdot a$ ed analogamente $G = 1 \cdot H \cup a \cdot H$, necessariamente, $G \backslash H = aH = Ha \implies H \trianglelefteq G$.

Proposizione : Sia $\varphi : G \to G'$ un omomorfismo di gruppi, allora il suo nucleo $Ker\varphi = \{g \in G | \varphi(g) = 1_G\}$ è un sottogruppo normale.
Dimostrazione : $ah(a^{-1})$ con $H \in Ker\varphi \implies \varphi(h) = 1_G$, devo dimostrare che $ah(a^{-1}) \in Ker\varphi, \forall h \in Ker\varphi$ e $\forall a \in G$, ho che :

$$\varphi(ah(a^{-1})) = \varphi(a)\varphi(h)\varphi(a^{-1}) = \varphi(a)\varphi(h)\varphi(a)^{-1} = \varphi(a)1_G\varphi(a)^{-1} = 1_G \quad ■ \tag{55}$$

Ogni omomorfismo (quindi **non** iniettivo), ha almeno un sottogruppo normale, ed esso è il suo nucleo, ossia $Ker\varphi$.

Proposizione : Sia $\varphi : A \to B$ un omomorfismo, allora $|Ker\varphi| = \dfrac{|A|}{|B|}$.

8.7 Il Gruppo degli Automorfismi

Sia G un gruppo, allora $\mathrm{Aut}(G)$, detto gruppo degli *automorfismi*, è definito nel seguente modo :

$$\mathrm{Aut}(G) = \{\varphi : G \to G \text{ isomorfismo }\}$$

Ossia il gruppo di tutti gli isomorfismi di G con se stesso, dove su esso è definita l'operazione di composizione.

8.7.1 Automorfismi Interni

Adesso, per ogni $x \in G$, definisco una funzione $\gamma_x : G \to G$ definita : $\gamma_x(g) = xgx^{-1}$, tale γ_x è un omomorfismo : $\gamma_x(ab) = xabx^{-1} = xax^{-1}xbx^{-1} = \gamma_x(a)\gamma_x(b)$, inoltre, tale funzione è *invertibile* : $(\gamma_x)^{-1} = \gamma_{x^{-1}}$. Prendo $a \in G$ e noto che :

$$a = x^{-1}xax^{-1}x = x^{-1}\gamma_x(a)x = \gamma_{x^{-1}}(\gamma_x(a)) \tag{56}$$

γ_x è biettiva, è quindi un isomorfismo, allora $\forall x \in G, \gamma_x \in \mathrm{Aut}(G)$. Osservo come si comporta l'operazione di composizione : $\gamma_x(\gamma_y(a)) = \gamma_x(yay^{-1}) = xyay^{-1}x^{-1} = \gamma_{xy}(a)$, ne deduche che :

$$\gamma_x \circ \gamma_y = \gamma_{xy}$$

Ciò mi suggerisce di considerare la mappa $\gamma : G \to \text{Aut}(G)$ definita : $\gamma(x) = \gamma_x$. Tale mappa è un omomorfismo, in generale, non si sa hanno informazioni sulla suriettività o inieittività di γ.

8.7.2 Centro del Gruppo

Ricordando la funzione γ, definisco adesso un altro insieme :

$$\text{Centro}(G) = Ker\gamma = \{x \in G | \gamma_x = e \text{ (elemento neutro) } \} = \{x \in G | xax^{-1} = a\}$$

Tale gruppo Centro(G), che sarebbe il nucleo dell'omomorfismo γ, contiene tutti gli elementi di G che **commutano**, ed è detto *centro* del gruppo.

Osservazione : Se G è commutativo, allora $G = \text{Centro}(G)$.

8.7.3 Gli Automorfismi di $\mathbb{Z}_n$

Dopo aver definito il gruppo degli automorfismi 8.7, è interessante trovare quali sono tutti gli automorfismi del gruppo $(\mathbb{Z}_n, +)$, che equivale a trovare tutti gli automorfismi per qualsiasi gruppo ciclico finito, prendiamo un qualsiasi automorfismo φ, e notiamo una cosa :

Osservazione : Essendo che un automorfismo (quindi isomorfismo) deve preservare l'unità, gli automorfismi di $\mathbb{Z}_n$ dipendono totalmente da $\varphi(1)$, quindi 1 dovrà essere mappato in uno degli elementi di $\mathbb{Z}_n$ che lo genera, sappiamo che gli elementi che possono fungere da unità in $\mathbb{Z}_n$ sono tutti gli $a \in \mathcal{U}(\mathbb{Z}_n)$.

A questo punto so che un automorfismo φ_a sarà del tipo $\varphi_a(k) = a \cdot k$ dove a sarebbe l'immagine dell'unità. Noto che $\varphi_a(\varphi_b(k)) = \varphi_a(bk) = abk \implies \varphi_a \circ \varphi_b = \varphi_{ab}$.

Considero la mappa $\phi : Aut(\mathbb{Z}_n) \to \mathcal{U}(\mathbb{Z}_n)$ tale che $\phi(\varphi_a) = a$. Tale mappa è suriettiva, in quanto per ogni $a \in \mathcal{U}(\mathbb{Z}_n)$ esiste φ_a tale che $\phi(\varphi_a) = a$. Essendo la cardinalità dei due insiemi identica, tale mappa è biettiva.

Noto che la mappa ϕ conserva le operazioni : $\phi(\varphi_a \circ \varphi_b) = \phi(\varphi_{ab}) = a \cdot b = \phi(\varphi_a) \cdot \phi(\varphi_b)$. Essendo un omomorfismo biettivo, ne segue che $Aut(\mathbb{Z}_n)$ è **isomorfo** a $\mathcal{U}(\mathbb{Z}_n)$.

8.8 Gruppo Quozioente per un Sottogruppo Normale

Sia $H \trianglelefteq G$ un sottogruppo normale, e considero $\mathcal{L}_S$ (essendo H normale, è analogo a $\mathcal{L}_D$), ossia l'insieme delle classi laterali associate ad H che partizionano G. Su questo insieme, considero un operazione $* : \mathcal{L}_S \times \mathcal{L}_S \to \mathcal{L}_S$ definita nel seguente modo :

$$Ha * Hb = H(a \cdot b)$$

Devo verificare che sia ben definita e che non dipenda dai rappresentanti delle classi di equivalenza, ossia che $Ha = Ha' \wedge Hb = Hb' \implies Hab = Ha'b'$.
Dimostrazione : per ipotesi, so che $a \cdot (a')^{-1} \in H$ e $b \cdot (b')^{-1} \in H$, per una proposizione già vista, so che $ab \cdot (a'b')^{-1} \in H$. chiamo $a \cdot (a')^{-1} = h_1$ e $b \cdot (b')^{-1} = h_2$, ho che $(ab)(a'b')^{-1} = ab(b')^{-1}(a')^{-1} = ah_2(a')^{-1}$, utilizzo l'ipotesi che le classi laterali siano uguali,

quindi se $ah_2 \in aH = Ha \implies \exists h_3 \in H | ah_2 = h_3 a$, quindi tornando all'identità precedente, $ah_2(a')^{-1} = h_3 a(a')^{-1} = h_3 \cdot h_1 \in H$. ■

L'elelemento neutro dell'operazione $*$ è H stesso, e per ogni Ha, il suo inverso è Ha^{-1}, dato che $Ha * Ha^{-1} = H(a \cdot a^{-1}) = H$.
Tale gruppo è detto **gruppo quoziente**, e si indica con ${}^{G}/_{H}$, è equivalente al gruppo delle classi di equivalenza della relazione ρ_D o ρ_S.

Definiamo adesso un applicazione $\pi : G \to {}^{G}/_{H}$ detta **proiezione canonica** di G sul quoziente ${}^{G}/_{H}$, definita nel seguente modo :

$$\pi(a) = Ha, \quad \forall a \in G$$

Tale applicazione è un omomorfismo :

$$\pi(ab) = Hab = Ha * Hb = \pi(a)\pi(b) \tag{57}$$

Risulta essere anche suriettiva.

8.8.1 gruppo quoziente per una relazione compatibile

Definizione : (Per l'osservazione seguente, si necessita di tale definizione) Sia $(G, \cdot)$ un gruppo, e ρ una relazione di equivalenza su G, si dice che la relazione è *compatibile* con l'operazione in G se :

$$a\rho a' \wedge b\rho b' \implies a \cdot b\rho a' \cdot b'$$

Se consideriamo ${}^{G}/_{\rho}$ l'insieme delle classi di equivalenza con l'operazione binaria :

$$[a] * [b] := [a \cdot b]$$

La condizione di *compatibilità* di ρ implica che tale operazione $*$ sia ben posta, vi è presente un inverso per ogni elemento ed un elemento neutro, . $({}^{G}/_{\rho}, *)$ è un gruppo, ed è detto *gruppo quoziente per una relazione compatibile.*

Osservazione : Il gruppo quoziente per un sottogruppo normale $({}^{G}/_{H}, *)$ definito all'inizio di questo capitolo 8.8, è un gruppo quoziente per una relazione compatibile, dato che è esso equivalente a ${}^{G}/_{\rho_D}$ dove ρ_D è una relazione compatibile con l'operazione :

$$a\rho_D b \wedge a'\rho_D b' \implies (ab)\rho_D(a'b')$$

Si ricordi che le classi di equivalenza di ρ_D sono proprio le classi laterali destre (equivalenti a quelle sinistre in quanto il gruppo è normale) che definiscono una partizione di G. Inoltre, che ρ_D e ρ_S siano identiche, è condizione necessaria per far si che ρ_D o ρ_S siano compatibili.

8.9 Teoremi di Isomorfismo

I teoremi di isomorfismo sono 3, vediamone il primo :

8.9.1 Teorema 1 (Teorema fondamentale di omomorfismo tra gruppi)

Sia $f : G \to G'$ un omomorfismo di gruppi, sappiamo che il suo nucleo $Kerf$ è un sottogruppo normale di G, quindi possiamo considerare il gruppo quoziente per un sottogruppo normale : ${}^{G}/_{Kerf}$, composto dalle classi laterali di $Kerf$.

Ricordando che π è la proiezione canonica, tale omomorfismo f induce un **unico isomorfismo** $F : {}^{G}/_{Kerf} \to Im(f)$, tale che $f = F \circ \pi$.

$$
\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Im(G) \\
& {}^{G}/_{Kerf} \arrow[ur, dotted, "F"'] &
\end{tikzcd}
$$

Dimostrazione : Definiamo un applicazione F in tal modo : $F(aKerf) := f(a) \quad \forall a \in G$. Tale applicazione è ben posta, dato che, se $aKerf = bKerf \iff ab^{-1} \in Kerf \iff f(ab^{-1}) = 1_{G'} \iff f(a)f(b^{-1}) = 1_{G'} \iff f(a)f(b)^{-1} = 1_{G'} \iff f(a) = f(b)$, dimostrando anche l'inieittività di F. Risulta che tale F mantiene le operazioni :

$$F(aKerf * bKerf) = F(abKerf) = f(ab) = f(a)f(b) = F(aKerf)F(bKerf)$$

Essendo che, qualsiasi elemento dell'immagine di f sarà del tipo $f(g)$ per qualche $g \in G$, tale $f(g)$ sarà mappato da F da un elemento di $gKerf$, quindi F è suriettiva, essendo anche iniettiva, risulta biettiva. Essendo F un omomorfismo biettivo, esso è un isomorfismo. ■

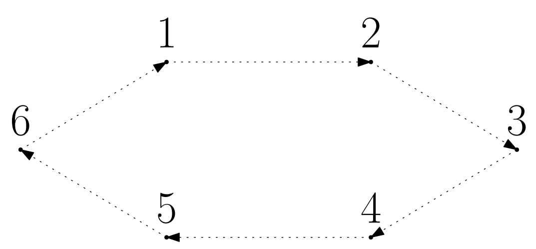
8.10 Gruppi Simmetrici

8.10.1 Definizione, Trasposizioni e k-cicli

Riprendiamo la definizione di gruppo simmetrico che abbiamo già dato nel capitolo 3.2.1, limitandola però agli insiemi finiti. Denotiamo con $\mathcal{S}_n$, il gruppo di cui gli elementi sono tutte le mappe biunivoche $\{1, 2, 3 \ldots, n\} \to \{1, 2, 3 \ldots, n\}$, denominato *gruppo simmetrico*, tali elementi (ossia le bigezioni) sono detti *permutazioni*, e l'operazione definita su tale gruppo è quella di composizione. Ci sono diversi modi di denotare una permutazione di $\mathcal{S}_n$:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} \tag{58}$$

Oppure con un grafo :



$$i \dashrightarrow j \quad := \sigma(i) = j$$

L'ordine (la cardinalità) di un gruppo simmetrico $\mathcal{S}_n$, è $n!$.

Definizione : Il *supporto* di una permutazione, sono gli indici degli elementi che sono punti *non fissati*, ossia :

$$\text{Supp}(\sigma) = \{j \in \sigma | \sigma(j) \neq j\}$$

Risulta chiaro che la restrizione di σ al di fuori del supporto, sia la funzione identità, $\sigma \backslash \text{Supp}(\sigma) = \text{Id}$.

Osservazione : Siano σ e τ due permutazioni, $\text{Supp}(\sigma) \cap \text{Supp}(\tau) = \emptyset \iff \tau \circ \sigma = \sigma \circ \tau$, se i supporti delle due permutazioni sono disgiunti, esse, commutano. In generale però, l'operazione di composizione in $\mathcal{S}_n$ non è commutativa.

Vediamo alcuni esempi di permutazioni note :

Le **trasposizioni** sono particolari permutazioni che si denotano con $(i \quad j)$, ed identificano una permutazione del tipo :

$$(i \quad j) = \begin{pmatrix} 1 & 2 & \dots & i & j & \dots & n \\ 1 & 2 & \dots & j & i & \dots & n \end{pmatrix} \tag{59}$$

Ossia che esclusi due valori i, j per cui $\sigma(i) = j$ e $\sigma(j) = i$, la bigezione è la funzione identità, si ha quindi che $\text{Supp}(\sigma) = \begin{pmatrix} i & j \\ j & i \end{pmatrix}$.

Generalzizziamo adesso l'idea di trasposizione, introducendo una permutazione detta k**-ciclo**, si identifica con $(j_1 \quad j_2 \quad ... \quad j_k)$, dove tali k elementi (si dice che k è la *lunghezza* del ciclo) sono il supporto di σ, (i restanti sono punti fissi), ed è definita in tal modo :

$$\sigma(j_1) = j_2 \quad \sigma(j_2) = j_3 \quad \sigma(j_3) = j_4 \quad \dots \quad \sigma(j_{k-1}) = j_k \quad \sigma(j_k) = j_1 \tag{60}$$

Ovviamente si ha che $\text{Supp}(\sigma) = \begin{pmatrix} j_1 & j_2 & \cdots & j_{k-1} & j_k \\ j_2 & j_3 & \cdots & j_k & j_1 \end{pmatrix}$, in rappresentazione con grafo risulta una cosa del tipo :

$$\begin{tikzcd} j_1 \arrow[r, dotted] & j_2 \arrow[r, dotted] & j_3 \arrow[r, dotted] & \dots \arrow[r, dotted] & j_{k-1} \arrow[r, dotted] & j_k \arrow[lllll, dotted, bend left] \end{tikzcd}$$

8.10.2 Scomposizione in k-cicli

Sappiamo che per il teorema fondamentale dell'aritmetica 2.5.1, un numero intero è fattorizzabile in un prodotto di numeri primi distinti, in simil-maniera, una qualsiasi permutazione è scomponibile in un **unico prodotto** (con prodotto, in questo caso si intende l'operazione di composizione) di k-cicli a supporto disgiunto :

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3 ..., \sigma_k \quad \forall i, j \leq k, \quad \text{Supp}(\sigma_j) \cap \text{Supp}(\sigma_i) = \emptyset$$

Daremo una dimostrazione con un esempio, consideriamo la permutazione :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix} \tag{61}$$

Parto dall'elemento 1 e noto che, $\sigma(1) = 3$, vedo allora dove viene mappato 3 e continuo, $\sigma(3) = 5$, e poi $\sigma(5) = 1$, ma 1 è l'elemento da cui siamo partiti, abbiamo quindi individuato il primo 3-ciclo, procedo iniziando da un nuovo elemento, prendo 2 e noto che $\sigma(2) = 6$ e che $\sigma(6) = 2$, ho quindi ottenuto un altro 2-ciclo, rimane esclusivamente l'elemento 4 che è un punto fisso, posso quindi scrivere la nostra permutazione iniziale come :

$$\sigma = (1 \quad 3 \quad 5)(2 \quad 6) \text{ come convenzione, posso omettere i punti fissi} \tag{62}$$

Adesso è una domanda lecita chiedersi, quale sia il rapporto fra l'ordine di una permutazione e l'ordine dei suoi k-cicli che la compongono.

Proposizione : L'ordine di una permutazione $\sigma \in \mathcal{S}_n$ è uguale al minimo comune multiplo delle lunghezze dei cicli che la compongono.

$$\sigma = (i_1^1 \quad i_2^1 \dots i_{d_1}^1)(i_1^2 \quad i_2^2 \dots i_{d_2}^2) \dots (i_1^k \quad i_2^k \dots i_{d_k}^k) \implies o(\sigma) = \text{mcm}(d_1, d_2 \dots, d_k)$$

Dimostrazione : Denotiamo $M = \text{mcm}(d_1, d_2 \dots, d_k)$, e vogliamo dimostrare che $o(\sigma) = N = M$, infatti, denotando con γ_i ogni singolo k-ciclo che compone σ, ho :

$$\sigma^M = (\gamma_1\gamma_2 \dots \gamma_k)^M = \text{ essendo i cicli disgiunti } = \gamma_1^M \gamma_2^M \dots \gamma_k^M = \text{Identità} \tag{63}$$

Quindi N divide M, inoltre (Denotando l'identità con id) :

$$\text{id} = \sigma^N = \gamma_1^N \gamma_2^N \dots \gamma_k^N = \text{id} \cdot \text{id} \cdot \text{id} \dots \text{id} \tag{64}$$

Allora l'ordine di ogni ciclo divide N, da cui M divide N, ne consegue che $M = N$. ■

8.10.3 Classi Coniugate in $\mathcal{S}_n$

In $\mathcal{S}_n$ risulta particolarmente facile stabilire una relazione di *coniugio*, che definisce appunto delle classi di equivalenza di elementi *coniugati* fra loro, definiamo tale relazione :

$$\sigma\rho\sigma' \iff \sigma = \tau\sigma'\tau^{-1} \text{ per qualche } \tau \in \mathcal{S}_n$$

Se sono in relazione, si dice che la permutazione σ è *coniugata* alla permutazione σ', ad esempio :

$$\sigma = (1 \quad 3 \quad 4) \qquad \text{e} \qquad \sigma' = (3 \quad 2 \quad 5)$$

Sono coniugate perché esiste $\tau = (1 \quad 3 \quad 2)(4 \quad 5)$ tale che $\sigma' = \tau\sigma\tau^{-1}$:

$$(3 \quad 2 \quad 5) = (1 \quad 3 \quad 2)(4 \quad 5) \circ (1 \quad 3 \quad 4) \circ (1 \quad 2 \quad 3)(4 \quad 5) \tag{65}$$

Non è stato chiaro però capire come selezionare questa $\tau \in \mathcal{S}_n$, notiamo cosa succede ad una permutazione se applichiamo l'operazione per stabilire se è coniuga ad un altra :

Prendo $\tau\sigma\tau^{-1}$ e so che $\sigma = (\sigma_1\sigma_2 \dots \sigma_k)$ dove ogni σ_i sarebbe il k-ciclo che compone σ, ho

$$\tau\sigma\tau^{-1} = \tau(\sigma_1\sigma_2 \dots \sigma_k)\tau^{-1} \text{ se fra ogni } \sigma_i, \sigma_{i+1} \text{ aggiungo } 1 = \tau^{-1}\tau \text{ ottengo :}$$

$$\tau(\sigma_1\sigma_2 \dots \sigma_k)\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1} \dots \tau\sigma_k\tau^{-1}$$

Vediamo adesso come si comporta su ogni i-esimo k-ciclo la composizione $\tau\sigma_i\tau^{-1}$, siano a e b due interi *consecutivi* di un qualunque σ_i, ossia $\sigma_i = (i_1 \quad i_2 \dots a \quad b \dots i_d)$, essendo un ciclo, ed essendo a e b consecutivi nella scrittura, ciò significa che $\sigma_i(a) = b$. Poniamo adesso $\tau(a) = s$ e $\tau(b) = t$, noto che :

$$\tau\sigma_i\tau^{-1}(s) = \tau\sigma_i(a) = \tau(b) = t$$

Se nella scrittura ciclica di σ_i, b è il successivo di a, allora $\tau(b)$ è il successivo di $\tau(a)$ nella scrittura ciclica di $\tau\sigma_i\tau^{-1}$, tale **risultato è fondamentale**, notiamo ad esempio come :

$$\sigma = (a \quad b \quad c \quad d)(e \quad f \quad g)(h \quad i) \tag{66}$$

$$\tau\sigma\tau^{-1} = (\tau(a) \quad \tau(b) \quad \tau(c) \quad \tau(d))(\tau(e) \quad \tau(f) \quad \tau(g))(\tau(h) \quad \tau(i)) \tag{67}$$

Questo ci dice che, se $\sigma' = \tau\sigma\tau^{-1}$, allora sicuramente σ e σ' hanno la stessa *struttura ciclica*, ciò vuol dire che, la loro scomposizione in k-cicli, condivide lo stesso numero di fattori, e tali fattori hanno la stessa lunghezza.
Spiegandolo in una maniera diversa, assegnamo ad ogni permutazione una tupla definita nel tal modo :

Sia σ una permutazione, la cui scomposizione in k-cicli è uguale a :
$\sigma = (i_1^1 \quad i_2^1 \dots \quad i_{d_1}^1)(i_1^2 \quad i_2^2 \dots \quad i_{d_2}^2)\dots(i_1^k \quad i_2^k \dots \quad i_{d_k}^k)$

Il primo k-ciclo ha lunghezza d_1, il secondo k-ciclo ha lunghezza d_2, fino al k-esimo k-ciclo che ha lunghezza d_k, la nostra tupla, è formata da queste lunghezze, ordinate in maniera crescende, quindi la tupla (formata da k lettere) assegnata a σ sarà :

$$Tupla(\sigma) = d_1 \leq d_2 \dots \leq d_k$$

Se due permutazioni hanno tupla identica, condividono la stessa struttura ciclica.

Esempio : la permutazione $\sigma = (a \quad b \quad c)(d \quad e)$ avrà tupla : $Tupla(\sigma) = 2 \leq 3$.
Un altra permutazione $\sigma' = (i \quad j)(f \quad g \quad h)$ avrà semptre tupla : $Tupla(\sigma') = 2 \leq 3$.
La permutazione $\sigma'' = (l \quad m \quad n \quad o)$ avrà tupla : $Tupla(\sigma'') = 4$.
Essendo che $Tupla(\sigma) = Tupla(\sigma')$, tali permutazioni hanno la stessa struttura ciclica.

Abbiamo dimostrato come, se σ è una permutazione, ed è coniugata a σ' ossia $\sigma = \tau\sigma'\tau^{-1}$ per qualche $\tau \in \mathcal{S}_n$, allora σ e σ' condividono la stessa struttura ciclica, e gli interi che compongono la scrittura ciclica di σ, si ottengono applicando τ agli interi che compongono la scrittura ciclica di σ'. ■

Proposizione : Se σ e σ' sono due permutazioni si $\mathcal{S}_n$ che condividono la stessa struttura ciclica, allora sono coniugate, $Tupla(\sigma) = Tupla(\sigma') \implies \exists \tau \in \mathcal{S}_n | \sigma' = \tau\sigma\tau^{-1}$

Dimostrazione : Diciamo quindi che σ e σ' hanno la stessa struttura ciclica :

$$\sigma = (a \quad b \quad c)(d \quad e)$$
$$\sigma' = (a' \quad b' \quad c')(d' \quad e')$$

Va provato che $\sigma' = \tau\sigma\tau^{-1}$, tale τ è una permutazione del tipo :

$$\tau = \begin{pmatrix} a & b & c & d & e \\ a' & b' & c' & d' & e' \end{pmatrix} \tag{68}$$

Che su gli elementi a, b, c, d, e si comporta come descritto, e sugli altri si comporta come vuole (compatibilmente col fatto che deve essere una permutazione). ■

Abbiamo adesso un metodo rapido per trovare una coniugata di una permutazione, vediamo un *esempio* : Si consideri il gruppo simmetrico $\mathcal{S}_7$, e le due permutazioni :

$$\sigma = (1 \quad 5)(2 \quad 3 \quad 4) \qquad \sigma' = (3 \quad 1 \quad 7)(5 \quad 2) \tag{69}$$

Condividendo la stessa struttura ciclica sono coniugate, vogliamo quindi trovare τ tale che $\sigma' = \tau\sigma\tau^{-1}$, la τ in questione dovrà comportarsi nel seguente modo :

$$3 = \tau(1), \quad 1 = \tau(3), \quad 7 = \tau(5), \quad 5 = \tau(2), \quad 2 = \tau(7) \tag{70}$$

τ dovrà mappare correttamente gli elementi 1,3,5,2,7, non è importante dove vengano mappati gli elementi 4 e 6, difatto, entrambe le seguenti permutazioni sono corrette :

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 4 & 7 & 6 & 2 \end{pmatrix} \qquad \tilde{\tau} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 & 2 \end{pmatrix}$$

E risulta che $\sigma' = \tau\sigma\tau^{-1} = \tilde{\tau}\sigma\tilde{\tau}^{-1}$.

Vediamo un'altro *esempio*, ho le due permutazioni :

$$\sigma = (2 \quad 6)(1 \quad 3 \quad 5) \qquad \tau = (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6) \tag{71}$$

Ho che :

$$\tau\sigma\tau^{-1} = (\tau(2) \quad \tau(6))(\tau(1) \quad \tau(3) \quad \tau(5)) = (3 \quad 1)(2 \quad 4 \quad 6) \tag{72}$$

La relazione di essere coniugati è una relazione di equivalenza che stabilisce quindi delle *classi coniugate*, che sono tante quante le diverse possibili strutture cicliche.

8.10.4 Decomposizione in Trasposizioni

Abbiamo già visto come ogni permutazione è un prodotto di k-cicli, facciamo adesso un osservazione, si consideri il 4-ciclo $\sigma = (1 \quad 2 \quad 3 \quad 4)$, noto adesso che posso riscrivere tale ciclo come prodotto di *trasposizioni*, de facto :

$$\sigma = (1 \quad 2 \quad 3 \quad 4) = (1 \quad 4)(1 \quad 3)(1 \quad 2) \tag{73}$$

Infatti :

$$(1 \quad 4) \circ (1 \quad 3)(1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \circ (1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4) \tag{74}$$

In generale, ogni k-ciclo può essere scritto come prodotto di trasposizioni, nel seguente modo :

$$(1 \quad 2 \quad 3 \ldots, n) = (1 \quad n)(1 \quad n-1)(1 \quad n-2) \ldots (1 \quad 3)(1 \quad 2)$$

Tale scrittura come prodotto di trasposizioni, **non** è unica, tutta via, una permutazione, avrà diverse fattorizzazioni in trasposizioni, ma la parità o disparità del numero dei fattori sarà ben definita, e non dipenderà dalla fattorizzazione scelta.
La permutazione $\sigma = (1 \quad 2 \quad 3 \quad 4)$ vista nell'esempio precedente, aveva scomposizione $(1 \quad 4)(1 \quad 3)(1 \quad 2)$, quindi è prodotto di un numero dispari di trasposizioni, quindi ogni singola fattorizzazione di σ, avrà un numero dispari di fattori.

Definizione : Una permutazione si dice *pari*, se il numero di fattori della scomposizione in trasposizioni che la compone è pari, analogamente, si dice *dispari*, se il numero di fattori della scomposizione in trasposizioni che la compone è dispari.

Osservazione : Il prodotto (composizione) di due permutazioni pari sarà una permutazione pari, il prodotto di due permutazioni dispari sarà una permutazione pari, il prodotto di una permutazione pari per una dispari sarà una permutazione dispari.

$$\text{Pari} \circ \text{Pari} = \text{Pari} \qquad \text{Dispari} \circ \text{Dispari} = \text{Pari} \qquad \text{Pari} \circ \text{Dispari} = \text{Dispari}$$

Osservazione : I k-cicli di lunghezzi pari sono permutazioni dispari, ed i k-cicli di lunghezza dispari sono permutazioni pari.

Possiamo adesso definire un sottogruppo di $\mathcal{S}_n$, ossia il **sottogruppo alterno**, definito in tal modo :

$$\mathcal{A}_n = \{\sigma \in \mathcal{S}_n | \sigma \text{ è una permutazione pari}\}$$

Ossia il gruppo formato da tutte e sole le permutazioni pari. Sappiamo che è un sottogruppo, perché il prodotto di due permutazioni pari, è ancora una permutazione pari. Inoltre, tale sottogruppo ha indice 2, è quindi un gruppo normale.

$$\mathcal{A}_n \trianglelefteq \mathcal{S}_n$$

A meno che di casi eccezionali in cui n è molto piccolo, solitamente il gruppo $\mathcal{S}_n$ ha $\mathcal{A}_n$ come unico gruppo normale. Essendo le trasposizioni delle permutazioni dispari, $\mathcal{A}_n$ non contiene trasposizioni.

Proposizione : L'ordine del sottogruppo alterno $\mathcal{A}_n$ di $\mathcal{S}_n$ è $\dfrac{n!}{2}$.

Algebra Lineare

9 Sistemi di Equazioni Lineari

Si consideri il seguente sistema di n equazioni a coefficenti reali, con n incognite :

$$\begin{cases} a_{1_1}x_1 + a_{1_2}x_2 \dots a_{1_n}x_n = b_1 \\ a_{2_1}x_1 + a_{2_2}x_2 \dots a_{2_n}x_n = b_2 \\ \dots \\ a_{n_1}x_1 + a_{n_2}x_2 \dots a_{n_n}x_n = b_n \end{cases}$$

Vogliamo chiederci, se tale sistema ammette soluzioni reali, e se ne ammette, quante? Ad un sistema lineare, è possibile associare una matrice.

Definizione : Una *matrice* $n \times m$ a coefficenti in un campo (in questo caso, $\mathbb{R}$), è una tabella di n righe ed m colonne, composta da numeri, si denota nella seguente forma :

$$A = \begin{bmatrix} a_{1_1} & a_{1_2} & . & a_{1_j} & . & a_{1_n} \\ a_{2_1} & a_{2_2} & . & a_{2_j} & . & a_{2_n} \\ . & & & . & & . \\ a_{i_1} & . & . & a_{i_j} & . & a_{i_n} \\ . & & & . & & . \\ a_{n_1} & a_{n_2} & . & a_{n_j} & . & a_{n_n} \end{bmatrix}$$

Vi sono due indici, e l'elemento a_{i_j} è quel numero che si trova all'i-esima riga ed alla j-esima colonna. Una matrice può anche avere 1 colonna ed n righe, la chiamiamo *ennupla*, ed è denotata nel seguente modo :

$$\bar{b} = \begin{bmatrix} b_1 \\ b_2 \\ . \\ . \\ b_n \end{bmatrix}$$

Un sistema di equazioni lineari quindi, può essere rappresentato con le matrici, dove ad ogni posizione di cordinata i, j, si associa il coefficente reale nella i-esima equazione che è moltiplicato alla j-esima incognita, tale matrice poi, si moltiplica alla ennupla delle incognite, e tale prodotta è identità della ennupla dei termini noti :

$$\begin{bmatrix} a_{1_1} & a_{1_2} & . & a_{1_j} & . & a_{1_n} \\ a_{2_1} & a_{2_2} & . & a_{2_j} & . & a_{2_n} \\ . & & & . & & . \\ a_{i_1} & . & . & a_{i_j} & . & a_{i_n} \\ . & & & . & & . \\ a_{n_1} & a_{n_2} & . & a_{n_j} & . & a_{n_n} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ . \\ . \\ . \\ b_n \end{bmatrix}$$

Quindi, si può scrivere tale sistema :

$$A\bar{x} = \bar{b}$$

Esempio : Il seguente sistema di equazioni lineari si rappresenta in forma di matrici :

$$\begin{cases} 3x_1 + 2x_2 + 3x_3 = 0 \\ 2x_1 - x_3 = 2 \\ x_1 + x_3 = 4 \end{cases} \qquad \text{si riscrive} \qquad \begin{bmatrix} 3 & 2 & 1 \\ 2 & 0 & -1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 4 \end{bmatrix}$$

Definizione : Sia A una matrice, esiste una funzione $\text{tr}: M_{n\times n} \to \mathbb{R}$, detta **traccia di una matrice**, che ad ogni matrice associa la somma degli elementi sulla sua diagonale :

$$\text{tr}(A) = a_{1_1} + a_{2_2} + a_{3_3} \cdots + a_{n_n}$$

Definizione : Una matrice quadrata $n \times n$ si dice **simmetrica** se, $\forall i, j \in \{1, 2 \dots, n\}$ si ha che $a_{i_j} = a_{j_i}$. Ad esempio, siano $a, b, c \in \mathbb{R}$, una qualsiasi matrice simmetrica 2×2 è della forma :

$$a \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + b \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + c \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a & c \\ c & b \end{bmatrix}$$

9.1 Metodo di Gauss

Esiste un semplice metodo per trovare la soluzione (o soluzioni) di un sistema di equazioni lineari, in questo paragrafo, ci ristringeremo al caso in cui il numero di equazioni è uguale al numero di incognite. Diamo prima un importante definizione.

Definizione di Sistemi Equivalenti: Siano $A\bar{x} = \bar{b}$ e $A'\bar{x} = \bar{b}'$ due sistemi di equazioni lineari, e sia $\Sigma = \{\bar{x} \in \mathbb{R}^n | A\bar{x} = \bar{b}\}$ l'insieme delle soluzioni del primo sistema, e $\Sigma' = \{\bar{x} \in \mathbb{R}^n | A'\bar{x} = \bar{b}'\}$ l'insieme delle soluzioni del secondo sistema. Se $\Sigma = \Sigma'$, ossia se i due sistemi distinti ammettono le stesse soluzioni, allora, si dicono *equivalenti*.

Prima di considerare il metodo per trovare le soluzioni di un sistema, si necessita ancora di un fondamentale lemma.

Lemma Fondamentale : Sia $A\bar{x} = \bar{b}$ un sistema di equazioni lineari $n \times n$, e siano

$$\star : \alpha_1 x_1 \cdots + \alpha_n x_n = \beta \qquad \text{ed} \qquad \star\star : \alpha'_1 x_1 \cdots + \alpha'_n x_n = \beta'$$

due equazioni del sistema, Si consideri l'equazione

$$\tilde{\star\star} : h(\alpha_1 x_1 \cdots + \alpha_n x_n) + k(\alpha'_1 x_1 \cdots + \alpha'_n x_n) = h\beta + k\beta'$$

dove k ed h sono due coefficenti reali, con $k \neq 0$. Sia $\tilde{A}\bar{x} = \tilde{\bar{b}}$ un nuovo sistema identico al primo, con la sola differenza che, al posto dell'equazione $\star\star$, vi è l'equazione $\tilde{\star\star}$, allora, $\tilde{A}\bar{x} = \tilde{\bar{b}}$ e $A\bar{x} = \bar{b}$ sono equivalenti.

Dimostrazione : Abbiamo $\star$ e $\star\star$, due equazioni del sistema, che ha soluzioni Σ, sia $\bar{y} \in \Sigma$, quindi $\bar{y}$ soddisfa $\star$ e $\star\star$, quindi :

$$\alpha_1 y_1 \cdots + \alpha_n y_n - \beta = 0 \qquad \text{e} \qquad \alpha'_1 y_1 \cdots + \alpha'_n y_n - \beta' = 0 \tag{75}$$

Ne segue che, considerando due coefficenti reali h e $k \neq 0$:

$$h(\alpha_1 y_1 \cdots + \alpha_n y_n - \beta) + k(\alpha'_1 y_1 \cdots + \alpha'_n y_n - \beta') = 0 \tag{76}$$

Questo, significa che $\bar{y}$ soddisfa la nuova equazione :

$$\tilde{\star\star} : h(\alpha_1 x_1 \cdots + \alpha_n x_n) + k(\alpha'_1 x_1 \cdots + \alpha'_n x_n) = h\beta + k\beta' \tag{77}$$

Ciò vuol dire che, se consideriamo un nuovo sistema $\tilde{A}\bar{x} = \tilde{\bar{b}}$ identico al primo, ma dove al posto di $\star\star$ compare $\tilde{\star\star}$, dove $\tilde{\Sigma}$ sono le soluzioni di questo nuovo sistema, essendo che, una qualsiasi soluzione del sistema iniziale soddisfa anche $\tilde{A}\bar{x} = \tilde{\bar{b}}$, possiamo dire che $\Sigma \subseteq \tilde{\Sigma}$.

Si consideri adesso una qualsiasi soluzione di $\tilde{A}\bar{x} = \tilde{\tilde{b}}$, ossia $\bar{z} \in \tilde{\Sigma}$, vale che $\bar{z}$, soddisfa $\star$, dato che $\star$ è presente anche in $\tilde{A}\bar{x} = \tilde{\tilde{b}}$, questo significa che :

$$!\alpha_1 z_1 \cdots + \alpha_n z_n - \beta = 0 \tag{78}$$

Adesso, prendo l'equazione $\tilde{\star\star}$ in $\tilde{A}\bar{x} = \tilde{\tilde{b}}$ e sostituisco l'incognita con $\bar{z}$:

$$h(\alpha_1 z_1 \cdots + \alpha_n z_n) + k(\alpha'_1 z_1 \cdots + \alpha'_n z_n) = h\beta + k\beta' \implies \tag{79}$$

$$h(\alpha_1 z_1 \cdots + \alpha_n z_n - \beta) + k(\alpha'_1 z_1 \cdots + \alpha'_n z_n - \beta') = 0 \tag{80}$$

Ma per ! ottengo :

$$h(0) + k(\alpha'_1 z_1 \cdots + \alpha'_n z_n - \beta') = 0 \implies \alpha'_1 z_1 \cdots + \alpha'_n z_n = \beta' \tag{81}$$

Questo significa che una qualsiasi $\bar{z} \in \tilde{\Sigma}$ soddisfa anche $\star\star$, ossia equazione del primo sistema, ne consegue che $\tilde{\Sigma} \subseteq \Sigma \implies \Sigma = \tilde{\Sigma}$. ■

Adesso che conosciamo il lemma, vogliamo utilizzarlo per trasformare il nostro sistema, in un sistema risolvibile facilmente, necessitiamo prima di tutto di una definizione.

Definizione di Matrice Triangolare : Una matrice quadrata $n \times n$ si dice *triangolare superiore* se, $i > j \implies a_{i_j} = 0$, graficamente, sotto la diagonale principale (composta da tutti gli elementi a_{i_j} per cui $i = j$), tutti gli elementi sono uguali a 0, sopra la diagonali principale invece i valori possono essere diversi da 0.

$$\textit{Esempio} : \begin{bmatrix} 1 & 4 & 5 & 7 & 1 \\ 0 & 2 & 5 & 6 & 9 \\ 0 & 0 & 1 & 9 & 4 \\ 0 & 0 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 7 \end{bmatrix}$$

Analogamente, si dice *triangolare inferiore* se, $i < j \implies a_{i_j} = 0$, graficamente, sopra la diagonale principale, tutti gli elementi sono uguali a 0, sotto la diagonali principale invece i valori possono essere diversi da 0.

$$\textit{Esempio} : \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 4 & 2 & 0 & 0 & 0 \\ 5 & 6 & 1 & 0 & 0 \\ 1 & 2 & 6 & 4 & 0 \\ 8 & 7 & 3 & 2 & 7 \end{bmatrix}$$

Un sistema di equazioni lineari si dice triangolare se la matrice ad esso associata è triangolare, un sistema di questo tipo, risulta estremamente facile da risolvere, in quanto è possibile partire dall'equazione con una sola incognita, risolverla, e procedere "dal basso verso l'alto" per sostituzione. Un esempio di sistema triangolare :

$$\begin{cases} t_{1_1}x_1 + t_{1_2}x_2 + t_{1_3}x_3 + t_{1_4}x_4 = b_1 \\ t_{2_2}x_2 + t_{2_3}x_3 + t_{2_4}x_4 = b_2 \\ t_{3_3}x_3 + t_{3_4}x_4 = b_3 \\ t_{4_4}x_4 = b_4 \end{cases} \quad \text{Ha matrice associata :} \quad \begin{bmatrix} t_{1_1} & t_{1_2} & t_{1_3} & t_{1_4} \\ 0 & t_{2_2} & t_{2_3} & t_{2_4} \\ 0 & 0 & t_{3_3} & t_{3_4} \\ 0 & 0 & 0 & t_{4_4} \end{bmatrix}$$

Ritorniamo adesso al metodo di risoluzione di un sistema di equazioni lineari, utilizzando le nozioni appena affrontate.

9.1.1 Teorema di Gauss

Ogni sistema di n equazioni lineari ad n incognite è equivalente ad un sistema triangolare.

Tale teorema è di fondamentale importanza, de facto, il metodo di gauss consiste nell'applicare più volte in maniera iterativa il **lemma fondamentale** ad un sistema per trasformarlo in un sistema triangolare che ha le stesse soluzioni del sistema originale.

Osservazione : Ovviamente, le equazioni di un sistema lineare possono scambiarsi di ordine, il sistema rimane lo stesso, con le stesse soluzioni.

Vediamo adesso il **metodo di risoluzione**, esso, su un sistema che ha una matrice $n \times n$ associata, sarà composto da $n-1$ passaggi (o step), ogni i-esimo passaggio, avrà come scopo, quello di trasformare la i-esima colonna, facendo si che tale colonna, abbia i elementi diversi da 0, ed i restanti $n-i$ elementi, uguali a 0. Si consideri il seguente esempio

$$\text{Se la matrice è } \begin{bmatrix} a_{1_1} & a_{1_2} & a_{1_3} \\ a_{2_1} & a_{2_2} & a_{2_3} \\ a_{3_1} & a_{3_2} & a_{3_3} \end{bmatrix}$$

- il *Passo 1* ha come obbiettivo di avere come prima colonna : $\begin{bmatrix} a_{1_1} \\ 0 \\ 0 \end{bmatrix}$
- il *Passo 2* ha come obbiettivo di avere come prima colonna : $\begin{bmatrix} a_{1_2} \\ a_{2_2} \\ 0 \end{bmatrix}$

Una volta completati questi due passi, la matrice è diventata triangolare. Ci rimane da capire come operare su ogni singolo passo, per far si che l'obbiettivo sia portato a termine.

Operare ad Ogni Passo : Sia l'i-esimo passo, dobbiamo quindi operare sull'i-esima colonna e trasformare $n-i$ elementi in modo che siano uguali a zero. Prima di tutto, si seleziona un qualsiasi elemento dalla colonna, diverso da zero, detto *pivot*, che denomineremo p_i. A questo punto, abbiamo il pivot, che sarebbe l'elemento a_{k_i}, con $k = 1, 2 \ldots, n$ (può essere un quasiasi elemento dell'i-esima colonna, a patto che sia diverso da zero). Adesso, in quella colonna, ci sta un elemento che è il pivot, poi ci sono i elementi che dovranno preservare il loro valore, ed $n-i$ elementi che dovranno diventare 0, ci concentreremo su questi ultimi, si dia il caso, che questi $n-i$ elementi, sono del tipo a_{l_i} con $l = \{i+1, i+2 \ldots, n\}$, per ognuno di questi elementi, si considera un nuovo valore, ossia $h_l = -\dfrac{a_{l_i}}{p_i}$,tale elemento, si moltiplica per tutta la k-esima riga (ossia, la riga dalla quale si è selezionato il pivot), ottenendo una nuova riga, e si somma, tutta la l-esima riga alla nuova riga ottenuta. Così facendo, tutti gli elementi $a_{i+1_i}, a_{i+2_i} \ldots, a_{n_i}$ diventeranno uguali a 0.

Attenzione, per quanto la spiegazione generale di questo algoritmo sembri contorta, in realtà è sufficentemente intuitiva, un esempio di applicazione sarà necessario per rendere l'idea.

9.1.2 Esempio di Applicazione del Metodo di Gauss

Si considera il seguente sistema con matrice associata :

$$\begin{cases} x+3+z-w=1 \\ 3x+9+4z+w=1 \\ 2x+y+5z+2w=0 \\ y-z-w=2 \end{cases} \qquad A=\begin{bmatrix} 1 & 3 & 1 & -1 \\ 3 & 9 & 4 & 1 \\ 2 & 1 & 5 & 2 \\ 0 & 1 & -1 & -1 \end{bmatrix} \bar{b}=\begin{bmatrix} 1 \\ 1 \\ 0 \\ 2 \end{bmatrix} \tag{82}$$

Passo 1 : Prendo dalla prima colonna un coefficente diverso da 0, seleziono come pivot : $p_1 = a_{1_1} = 1$. Considero $h_2 = -\frac{a_{2_1}}{p_1} = -\frac{3}{1}$, moltiplico tale valore per la riga 1 (dalla quale si è selezionato il pivot), ed ottengo la riga : $\begin{bmatrix} -3 & -9 & -3 & 3 \end{bmatrix} \begin{bmatrix} -3 \end{bmatrix}$, adesso, sommo questa riga alla riga numero 2, la nuova matrice ottenuta (equivalente per il lemma fondamentale) è :

$$A=\begin{bmatrix} 1 & 3 & 1 & -1 \\ 0 & 0 & 1 & 4 \\ 2 & 1 & 5 & 2 \\ 0 & 1 & -1 & -1 \end{bmatrix} \bar{b}=\begin{bmatrix} 1 \\ -2 \\ 0 \\ 2 \end{bmatrix}$$

Continuo con lo stesso procedimento per la terza riga. Considero $h_3 = -\frac{a_{3_1}}{p_1} = -\frac{2}{1}$, moltiplico tale valore per la riga 1 (dalla quale si è selezionato il pivot), ed ottengo la riga : $\begin{bmatrix} -2 & -6 & -2 & 2 \end{bmatrix} \begin{bmatrix} -2 \end{bmatrix}$, adesso, sommo questa riga alla riga numero 3, la nuova matrice ottenuta (equivalente per il lemma fondamentale) è :

$$A=\begin{bmatrix} 1 & 3 & 1 & -1 \\ 0 & 0 & 1 & 4 \\ 0 & -5 & 3 & 4 \\ 0 & 1 & -1 & -1 \end{bmatrix} \bar{b}=\begin{bmatrix} 1 \\ -2 \\ -2 \\ 2 \end{bmatrix}$$

Scambio l'ordine di alcune righe ed ottengo :

$$A=\begin{bmatrix} 1 & 3 & 1 & -1 \\ 0 & -5 & 3 & 4 \\ 0 & 0 & 1 & 4 \\ 0 & 1 & -1 & -1 \end{bmatrix} \bar{b}=\begin{bmatrix} 1 \\ -2 \\ -2 \\ 2 \end{bmatrix}$$

Adesso, la riga 1, ha 1 elemento diverso da zero, procedo con il prossimo passo.

Passo 2 : Prendo dalla seconda colonna un coefficente diverso da 0, seleziono come pivot : $p_2 = a_{2_2} = -5$. Considero $h_4 = -\frac{a_{4_1}}{p_2} = -\frac{1}{(-5)} = \frac{1}{5}$, moltiplico tale valore per la riga 2 (dalla quale si è selezionato il pivot), ed ottengo la riga : $\begin{bmatrix} 0 & -1 & {}^3/_5 & {}^4/_5 \end{bmatrix} \begin{bmatrix} -{}^2/_5 \end{bmatrix}$ adesso, sommo questa riga alla riga numero 4, la nuova matrice ottenuta (equivalente per il lemma fondamentale) è :

$$A=\begin{bmatrix} 1 & 3 & 1 & -1 \\ 0 & -5 & 3 & 4 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & -{}^2/_5 & -{}^1/_5 \end{bmatrix} \bar{b}=\begin{bmatrix} 1 \\ -2 \\ -2 \\ {}^8/_5 \end{bmatrix}$$

Adesso, la riga 2, ha 2 elementi diverso da zero, procedo con il prossimo passo.

Passo 3 : Prendo dalla terza colonna un coefficente diverso da 0, seleziono come pivot : $p_3 = a_{3_3} = 1$. Considero $h_3 = -\frac{a_{3_4}}{p_3} = -\frac{(-2/5)}{1} = \frac{2}{5}$, moltiplico tale valore per la riga 3 (dalla quale si è selezionato il pivot), ed ottengo la riga : $\begin{bmatrix} 0 & 0 & 2/5 & 8/5 \end{bmatrix} \begin{bmatrix} -4/5 \end{bmatrix}$ adesso, sommo questa riga alla riga numero 4, la nuova matrice ottenuta (equivalente per il lemma fondamentale) è :

$$A = \begin{bmatrix} 1 & 3 & 1 & -1 \\ 0 & -5 & 3 & 4 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 7/5 \end{bmatrix} \bar{b} = \begin{bmatrix} 1 \\ -2 \\ -2 \\ 4/5 \end{bmatrix}$$

Qui mi fermo. Per il lemma fondamentale, questa nuova matrice, è associata ad un sistema che è equivalente a quello iniziale. Il nuovo sistema triangolare è :

$$\begin{cases} x + 3y + z - 2 = 1 \\ -5y + 3z + 4w = -2 \\ z + 4w = -2 \\ \frac{7}{5}w = \frac{4}{5} \end{cases} \tag{83}$$

Posso risolverlo facilmente partendo dall'ultima equazione :

$$\begin{cases} x + 3y + z - w = 1 \\ -5y + 3z + 4w = -2 \\ z + 4w = -2 \\ w = 4/7 \end{cases} \implies \begin{cases} x + 3y + z - w = 1 \\ -5y + 3z + 4w = -2 \\ z + 16/7 = -2 \\ w = 4/7 \end{cases} \implies \begin{cases} x + 3y + z - w = 1 \\ -5y + 3z + 4w = -2 \\ z = -30/7 \\ w = 4/7 \end{cases} \tag{84}$$

$$\begin{cases} x + 3y + z - w = 1 \\ -5y + 3(-30/7) + 4(4/7) = -2 \\ z = -30/7 \\ w = 4/7 \end{cases} \implies \begin{cases} x + 3y + z - w = 1 \\ y = -12/7 \\ z = -30/7 \\ w = 4/7 \end{cases} \implies \tag{85}$$

$$\begin{cases} x + 3(-12/7) + (-30/7) - (4/7) = 1 \\ y = -12/7 \\ z = -30/7 \\ w = 4/7 \end{cases} \implies \begin{cases} x = 11 \\ y = -12/7 \\ z = -30/7 \\ w = 4/7 \end{cases} \tag{86}$$

Quindi, la soluzione è $\bar{x} = \begin{bmatrix} 11 \\ 12/7 \\ -30/7 \\ 4/7 \end{bmatrix}$.

9.1.3 Teorema dei Sistemi Triangolari

Sia $T\bar{x} = \bar{c}$ un sistema triangolare $n \times n$, tale sistema ammette soluzione **unica** se e solo se, $\forall i \in \{1, 2 \dots n\}$, $t_{i_i} \neq 0$, ossia, se la diagonale principale non ha valori nulli. Differentemente, se $\exists j \in \{1, 2 \dots n\} | t_{j_j} = 0$, allora il sistema, o non ammette soluzione, o ne ammette infinite.

A questo punto, come si fa a capire se un sistema ammette o non ammette soluzione? Come si tratta un sistema in cui il numero delle incognite è diverso dal numero delle equazioni? Per tutto ciò, occorre introdurre una nuova struttura algebrica.

10 Spazio Vettoriale sul Campo dei Reali

Lo spazio vettoriale, è una struttura del tipo $(V, +, \bar{o}, \cdot)$ definita su un campo (nel nostro caso, $\mathbb{R}$). $\bar{o}$ è l'elemento neutro, e tale struttura segue i seguenti assiomi :

1. $(V, +)$ è un gruppo commutativo, dove $+$ è un operazione binaria :

$$+ : V \times V \to V \text{ tale che } (\bar{v}, \bar{w}) \to \bar{v} + \bar{w}$$

2. Esiste un operazione esterna $\cdot$:

$$\cdot : \mathbb{R} \times V \to V \text{ tale che } (\alpha, \bar{v}) \to \alpha\bar{v}$$

$\forall \bar{v}, \bar{w} \in V$ e $\forall \lambda, \mu \in \mathbb{R}$, valgono le seguenti regole :

- (i) $\lambda \cdot (\bar{v} + \bar{w}) = \lambda\bar{v} + \lambda\bar{w}$ tale operazione si chiama *prodotto per uno scalare*
- (ii) $1 \cdot \bar{v} = \bar{v}$
- (iii) $(\lambda + \mu) \cdot \bar{v} = \lambda\bar{v} + \mu\bar{v}$
- (iiii) $(\lambda\mu) \cdot \bar{v} = \lambda \cdot (\mu \cdot \bar{v})$

Vediamo due esempi di noti spazi vettoriali :

- $(\mathbb{R}^n, +, \bar{0}, \cdot)$ è uno spazio vettoriale, con elemento neutro, somma, prodotto scalare ed inverso definiti in tal modo :

$$\bar{0} := \begin{bmatrix} 0 \\ 0 \\ . \\ . \\ 0 \end{bmatrix} \qquad \bar{x} + \bar{y} := \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ . \\ . \\ x_n + y_n \end{bmatrix} \qquad \lambda \cdot \bar{x} := \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ . \\ . \\ \lambda x_n \end{bmatrix} \qquad (\bar{x})^{-1} = \begin{bmatrix} -x_1 \\ -x_2 \\ . \\ . \\ -x_n \end{bmatrix}$$

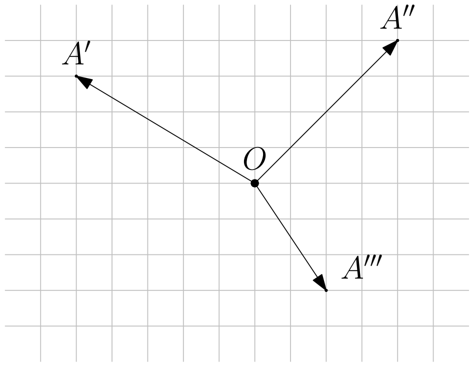
- L'insieme V delle funzioni continue su $\mathbb{R}$ è uno spazio vettoriale, con elemento neutro, somma, prodotto scalare ed inverso definiti in tal modo :

$$f_0 := f(x) = 0 \quad (f + g)(x) := f(x) + g(x) \quad (\lambda f)(x) := \lambda \cdot f(x) \quad (f(x)^{-1}) := -f(x)$$

10.0.1 Lo Spazio dei Vettori sul Piano Euclideo

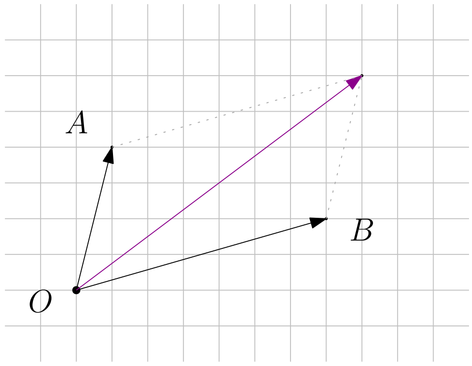
Vediamo adesso uno dei più noti spazi vettoriali, che viene introdotto ad ogni studente sin dalle scuole superiori, si consideri il *piano della geometria euclidea* $\mathbb{R} \times \mathbb{R}$, e si fissi un punto O. Consideriamo adesso l'insieme $V = \{$segmenti orientati centrati in $O\}$, ossia l'insieme dei vettori applicati in O, che denoteremo $\vec{OA}$, dove A è un qualsiasi punto nel piano. L'elemento neutro di tale insieme, è il vettore che va da O in O, ossia $\vec{OO}$.

Sul piano, rappresentati i vettori $\vec{OA'}$, $\vec{OA''}$ e $\vec{OA'''}$.



Introduciamo adesso un operazione in V, detta somma di due vettori $+ : V \times V \to V$, tale che $\vec{OA} + \vec{OB} = \vec{OC}$, dove $\vec{OC}$, è il segmento che va da O fino al quarto vertice del parallelogramma indicato da $\vec{OA}$ e $\vec{OB}$, tale vertice, è indicato, dal vettore centrato in A, della stessa lunghezza, verso e direzione di $\vec{OB}$.

Rappresentato sul piano (in viola) il vettore $\vec{OC}$



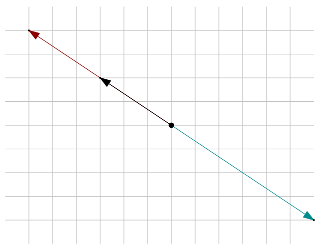
Proposizione : Con l'operazione di somma, ed elemento neutro $\vec{OO}$, tale V è un gruppo commutativo.

L'inverso di un vettore $\vec{OA}$, ha la stessa lunghezza del vettore $\vec{OA}$, ma ha direzione opposta.

Introduco adesso una nuova operazione, $\cdot : \mathbb{R} \times V \in V$, detta **prodotto per uno scalare**, tale che $(\lambda, \vec{OA}) \to \lambda \cdot \vec{OA}$, il vettore $\lambda\vec{OA}$:

- Se $\lambda \geq 0$, ha stessa direzione e verso del vettore $\vec{OA}$, ma la sua lunghezza, è uguale a $\lambda \cdot$ (lunghezza di $\vec{OA}$).
- Se $\lambda < 0$, per il vettore $\lambda\vec{OA}$, considero $-(|\lambda|\vec{OA})$, il vettore di lunghezza $|\lambda| \cdot$ (lunghezza di $\vec{OA}$) centrato in O, nella direzione opposta di $\vec{OA}$.

Rappresentati sul piano il vettore $\vec{OA}$ in nero, il vettore $2\vec{OA}$ in rosso, ed il vettore $(-2)\vec{OA}$ in azzurro



Proposizione : Con le operazioni di somma e prodotto vettoriale, V è uno spazio vettoriale su $\mathbb{R}$, denotato V_O^2. Analogamente, esiste anche V_O^3, dove i vettori sono posizionati nello spazio tri-dimensionale.

10.1 Sottospazi Vettoriali

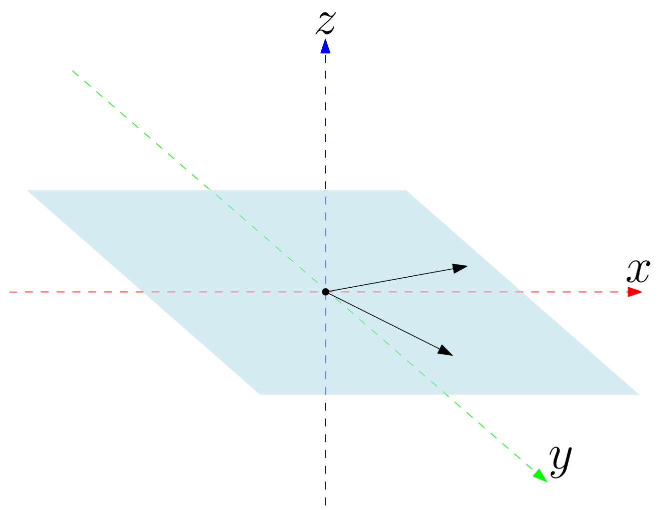
Sia V uno spazio vettoriale sul campo $\mathbb{R}$ (ma ciò vale per qualsiasi campo), e sia W un sottoinsieme di V. Diremo che W è un *sottospazio vettoriale* di V, e denoteremo $W \leq V$ se :

1. $\forall \bar{w}, \bar{w}' \in W$, $\bar{w} + \bar{w}' \in W$
2. $\forall \bar{w} \in W, \forall \lambda \in \mathbb{R}$, $\lambda \bar{w} \in W$

Osservazione : $\forall \bar{w} \in W$, $-\bar{w} \in W$, $(W, +)$ è un sottogruppo di $(V, +)$.

Per stabilire se W sia un sottogruppo, possiamo utilizzare il criterio (3) visto nel capitolo 8.2, prendere due qualsiasi $\bar{w}, \bar{w}' \in W$, e controllare che $\bar{w} + (\bar{w}')^{-1} = \bar{w} + (-1)\bar{w}' \in W$.

Ad *esempio*, su V_O^3, tutti i vettori che "poggiano" su un piano, rappresentano un sottospazio, nell'immagine sotto-stante, presi due qualsiasi i vettori sul piano $f(x, y) = 0$ (ossia, tutti i vettori che hanno la terza coordinata nulla), le operazioni di somma e prodotto su di essi, restituiranno sempre un vettore che poggia sullo stesso piano.



Torniamo adesso ai *sistemi lineari*, e consideriamo A, la matrice $m \times n$ associata ad un sistema a coefficenti reali nel campo $\mathbb{R}$, si ricordi, che posso rappresentare un sistema con la notazione $A\bar{x} = \bar{b}$. Considero un sistema **omogeneo**, ossia, dove tutti i termini noti sono nulli, della forma $A\bar{x} = \bar{0}$, sia allora $\Sigma_0 = \{\bar{y} \in \mathbb{R}^n | A\bar{y} = \bar{0}\}$, ossia l'insieme di tutte le soluzioni di un certo sistema omogeneo.

Proposizione : Σ_0 è un sottospazio vettoriale di $\mathbb{R}^n$.

Dimostrazione : Mostriamo i due punti necessari per la verifica in ordine.

(1) : Siano $\bar{y}$ e $\bar{y}'$ due soluzioni del sistema $A\bar{x} = \bar{0}$, si ha che :

$$\begin{cases} a_{1_1}y_1 + a_{1_2}y_2 \cdots + a_{1_n}y_n = 0 \\ a_{2_1}y_1 + a_{2_2}y_2 \cdots + a_{2_n}y_n = 0 \\ \cdots \\ a_{n_1}y_1 + a_{n_2}y_2 \cdots + a_{n_n}y_n = 0 \end{cases} \qquad \begin{cases} a_{1_1}y'_1 + a_{1_2}y'_2 \cdots + a_{1_n}y'_n = 0 \\ a_{2_1}y'_1 + a_{2_2}y'_2 \cdots + a_{2_n}y'_n = 0 \\ \cdots \\ a_{n_1}y'_1 + a_{n_2}y'_2 \cdots + a_{n_n}y'_n = 0 \end{cases} \tag{87}$$

Risulta ovvio che :

$$\begin{cases} (a_{1_1}y_1 + a_{1_2}y_2 \cdots + a_{1_n}y_n) + (a_{1_1}y'_1 + a_{1_2}y'_2 \cdots + a_{1_n}y'_n) = 0 \\ (a_{2_1}y_1 + a_{2_2}y_2 \cdots + a_{2_n}y_n) + (a_{2_1}y'_1 + a_{2_2}y'_2 \cdots + a_{2_n}y'_n) = 0 \\ \cdots \\ (a_{n_1}y_1 + a_{n_2}y_2 \cdots + a_{n_n}y_n) + (a_{n_1}y'_1 + a_{n_2}y'_2 \cdots + a_{n_n}y'_n) = 0 \end{cases} \tag{88}$$

Ricordando che $\bar{y}$ e $\bar{y}'$ non sono incognite ma soluzioni, nel sistema abbiamo esclusivamente numeri reali, possiamo quindi applicare la proprietà distributiva in tal modo :

$$\begin{cases} a_{1_1}(y_1 + y'_1) + a_{1_2}(y_2 + y'_2) \cdots + a_{1_n}(y_n + y'_n) = 0 \\ a_{2_1}(y_1 + y'_1) + a_{2_2}(y_2 + y'_2) \cdots + a_{2_n}(y_n + y'_n) = 0 \\ \cdots \\ a_{n_1}(y_1 + y'_1) + a_{n_2}(y_2 + y'_2) \cdots + a_{n_n}(y_n + y'_n) = 0 \end{cases} \tag{89}$$

Ne concludiamo che $\bar{y} + \bar{y}' \in \Sigma_0$.

(2) : Sia $\bar{y}$ una soluzione di $A\bar{x} = \bar{0}$, e λ un qualsiasi numero reale, sappiamo che :

$$\begin{cases} a_{1_1}y_1 + a_{1_2}y_2 \cdots + a_{1_n}y_n = 0 \\ a_{2_1}y_1 + a_{2_2}y_2 \cdots + a_{2_n}y_n = 0 \\ \cdots \\ a_{n_1}y_1 + a_{n_2}y_2 \cdots + a_{n_n}y_n = 0 \end{cases} \tag{90}$$

Moltiplichiamo da entrambi i lati di ogni equazione, il numero reale λ, ottenendo :

$$\begin{cases} \lambda \cdot (a_{1_1}y_1 + a_{1_2}y_2 \cdots + a_{1_n}y_n) = \lambda \cdot 0 \\ \lambda \cdot (a_{2_1}y_1 + a_{2_2}y_2 \cdots + a_{2_n}y_n) = \lambda \cdot 0 \\ \cdots \\ \lambda \cdot (a_{n_1}y_1 + a_{n_2}y_2 \cdots + a_{n_n}y_n) = \lambda \cdot 0 \end{cases} \Longrightarrow \begin{cases} \lambda \cdot (a_{1_1}y_1 + a_{1_2}y_2 \cdots + a_{1_n}y_n) = 0 \\ \lambda \cdot (a_{2_1}y_1 + a_{2_2}y_2 \cdots + a_{2_n}y_n) = 0 \\ \cdots \\ \lambda \cdot (a_{n_1}y_1 + a_{n_2}y_2 \cdots + a_{n_n}y_n) = 0 \end{cases} \tag{91}$$

Applicando la proprietà distributiva dei numeri reali ottengo :

$$\begin{cases} \lambda \cdot a_{1_1}y_1 + \lambda \cdot a_{1_2}y_2 \cdots + \lambda \cdot a_{1_n}y_n = 0 \\ \lambda \cdot a_{2_1}y_1 + \lambda \cdot a_{2_2}y_2 \cdots + \lambda \cdot a_{2_n}y_n = 0 \\ \cdots \\ \lambda \cdot a_{n_1}y_1 + \lambda \cdot a_{n_2}y_2 \cdots + \lambda \cdot a_{n_n}y_n = 0 \end{cases} \tag{92}$$

Applicando la proprietà associativa e distributiva dei numeri reali ottengo :

$$\begin{cases} a_{1_1}(y_1 \cdot \lambda) + a_{1_2}(y_2 \cdot \lambda) \cdots + a_{1_n}(y_n \cdot \lambda) = 0 \\ a_{2_1}(y_1 \cdot \lambda) + a_{2_2}(y_2 \cdot \lambda) \cdots + a_{2_n}(y_n \cdot \lambda) = 0 \\ \cdots \\ a_{n_1}(y_1 \cdot \lambda) + a_{n_2}(y_2 \cdot \lambda) \cdots + a_{n_n}(y_n \cdot \lambda) = 0 \end{cases} \tag{93}$$

Ne concludo che, se $\bar{y}$ è soluzione, anche $\lambda\bar{y}$ è soluzione del sistema. La verifica dei punti **(1)** e **(2)**, è necessaria per constatare che Σ_0 è un sottospazio vettoriale. ■

Osservazione, l'insieme di tutte le soluzioni di un sistema $A\bar{x} = \bar{b}$, dove $\bar{b} \neq \bar{0}$, definito $\Sigma = \{\bar{y} | A\bar{y} = \bar{b}\}$, non è un sottospazio vettoriale, in quanto non contiene l'elemento neutro $\bar{0}$.

10.2 Combinazioni Lineari

Sia V uno spazio vettoriale, e $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$ un insieme di vettori in V. Una *combinazione lineare di* V, è il vettore

$$\alpha_1 \cdot \bar{v}_1 + \alpha_2 \cdot \bar{v}_2 \dots + \alpha_k \cdot \bar{v}_k$$

Dove $\alpha_1, \alpha_2 \dots, \alpha_k$, è un qualsiasi insieme di coefficenti nel campo.

Esempio : In V_O^2, si considerino i vettori $\vec{OA}, \vec{OB}, \vec{OC}$:

- $\vec{OA} + \vec{OB} + \vec{OC}$ è una combinazione lineare dei 3 vettori.
- $4\vec{OA} - 2\vec{OB} + \dfrac{1}{2}\vec{OC}$ è una combinazione lineare dei 3 vettori.
- $-\vec{OA} + \pi \cdot \vec{OB} + (1.012031 \cdot 10^9)\vec{OC}$ è una combinazione lineare dei 3 vettori.

Definizione di Span : Preso un insieme di vettori $\{\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k\}$ di uno spazio vettoriale V, definiamo il loro *Span*, l'insieme di tutte le loro possibili combinazioni lineari.

$$\text{Span}(\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k) = \{\alpha_1 \cdot \bar{v}_1 + \alpha_2 \cdot \bar{v}_2 \dots + \alpha_k \cdot \bar{v}_k | \alpha_j \in \mathbb{R}\}$$

Osservazione : Uno Span è un sottospazio.

Osservazione : Lo Span di un certo insieme W, è uguale allo Span di $W \cup \{\bar{a}, \bar{b} \dots, \bar{n}\}$, se $\{\bar{a}, \bar{b} \dots, \bar{n}\} \subseteq \text{Span}(W)$, ciò vuol dire che, lo Span di un insieme di elementi, è uguale allo Span dell'unione dell'insieme originale di elementi con nuovi elementi che sono già nello Span degli elementi originali (rileggere lentamente).

$$\text{Span}(\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k) = \text{Span}(\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k, \alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \dots + \alpha_k\bar{v}_k)$$

Proposizione : Il sistema lineare $A\bar{x} = \bar{b}$, con matrice associata $A \in M_{m\times n}(\mathbb{R})$, dove $M_{mn}(\mathbb{R})$ è l'insieme delle matrici con m righe ed n colonne a coefficenti reali, ammette soluzione se e solo se $\bar{b} \in \text{Span}(A^1, A^2 \dots, A^n)$, dove A^j è la j-esima colonna di A.

10.3 Indipendenza Lineare

Siano $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$ k vettori di uno spazio vettoriale V. Tali vettori, si dicono **linearmente indipendenti** se ogni combinazione lineare dei k vettori, uguale al vettore nullo : $\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \dots + \alpha_k\bar{v}_k = \bar{0}$, ha tutti i coefficenti nulli : $\alpha_1 = \alpha_2 \dots = \alpha_k = 0$. Analogamente, se esiste un insieme di coefficenti reali $\alpha_1, \alpha_2 \dots, \alpha_k$ *non tutti nulli* tali che $\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \dots + \alpha_k\bar{v}_k = \bar{0}$, allora, i vettori si dicono **linearmente dipendenti**.

Esempio : In $\mathbb{R}^n$, i vettori :

$$\bar{e}_1 = \begin{bmatrix} 1 \\ . \\ . \\ 0 \end{bmatrix} \bar{e}_2 = \begin{bmatrix} 0 \\ 1 \\ . \\ 0 \end{bmatrix} \dots \bar{e}_k = \begin{bmatrix} 0 \\ . \\ . \\ 1 \end{bmatrix}$$

Sono linearmente indipendenti, in quanto una loro combinazione lineare diventa :

$$\alpha_1 \begin{bmatrix} 1 \\ . \\ . \\ 0 \end{bmatrix} + \dots + \alpha_k \begin{bmatrix} 0 \\ . \\ . \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ . \\ . \\ 0 \end{bmatrix} + \dots + \begin{bmatrix} 0 \\ . \\ . \\ \alpha_k \end{bmatrix} = 0 \iff \alpha_1, \alpha_2 \dots, \alpha_k = 0$$

Osservazione 1 : Se in $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$, vi è anche il vettore nullo $\bar{0}$, allora i vettori sono linearmente dipendenti.

Dimostrazione Oss. 1 : Per ipotesi $\exists j | \bar{v}_j = \bar{0}$, si consideri la seguente combinazione lineare: $0 \cdot \bar{v}_1 + 0 \cdot \bar{v}_2 \dots 0 \cdot \bar{v}_{j-1} + 1\bar{v}_j + 0 \cdot \bar{v}_{j+1} \dots + 0 \cdot \bar{v}_k = \bar{0}$, nonostante il coefficente di $\bar{v}_j$ sia diverso da 0, la combinazione lineare è ugualmente nulla, in quanto $\alpha \cdot \bar{0} = \bar{0}$, quindi i vettori sono linearmente dipendenti. ■

Osservazione 2 : I vettori $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$ sono linearmente dipendenti, se e solo se, uno di essi è combinazione lineare degli altri.

$\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$ sono lin. dipendenti $\iff \exists j \in \{1, 2 \dots, k\} | \bar{v}_j \in \text{Span}(\{\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k\} \backslash \{\bar{v}_j\})$

Dimostrazione Oss. 2 : Iniziamo dimostrando il primo verso dell'implicazione, per ipotesi, i vettori $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$ sono linearmente dipendenti, prendo una loro combinazione lineare uguale al vettore nullo, dove vi è un coefficente α_l diverso da zero, ho che :

$$\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \dots + \alpha_{l-1}\bar{v}_{l-1} + \alpha_l\bar{v}_l + \alpha_{l+1}\bar{v}_{l+1} \dots + \alpha_k\bar{v}_k = \bar{0} \tag{94}$$

$$\alpha_l\bar{v}_l = -\alpha_1\bar{v}_1 - \alpha_2\bar{v}_2 \dots - \alpha_{l-1}\bar{v}_{l-1} - \alpha_{l+1}\bar{v}_{l+1} \dots - \alpha_k\bar{v}_k \tag{95}$$

Essendo $\alpha_l \neq 0$, posso dividere tutto per α_l :

$$\bar{v}_l = -\frac{\alpha_1}{\alpha_l}\bar{v}_1 - \frac{\alpha_2}{\alpha_l}\bar{v}_2 \dots - \frac{\alpha_{l-1}}{\alpha_l}\bar{v}_{l-1} - \frac{\alpha_{l+1}}{\alpha_l}\bar{v}_{l+1} \dots - \frac{\alpha_k}{\alpha_l}\bar{v}_k \tag{96}$$

Scritto in questa forma, risulta chiaro che $\bar{v}_l$ è risultato di una combinazione lineare degli altri vettori. Dimostriamo adesso il secondo verso dell'implicazione, l'ipotesi è che un vettore $\bar{v}_i$ sia combinazione lineare degli altri :

$$\bar{v}_i = \beta_1\bar{v}_1 + \beta_2\bar{v}_2 \dots + \beta_k\bar{v}_k$$

Adesso, sommo ad entrambi i membri il termine $-(\bar{v}_i)$, ed ottengo :

$$\beta_1\bar{v}_1 + \beta_2\bar{v}_2 \dots + \beta_k\bar{v}_k - \bar{v}_i = \bar{0}$$

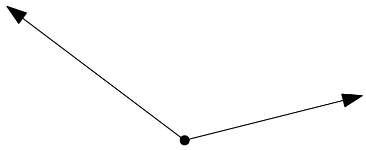
Adesso, il coefficente di $\bar{v}_i$ è -1, ma il risultato della combinazione lineare è il vettore nullo, quindi sono linearmente dipendenti. ■

Osservazione 3 : Presi due vettori $\bar{v}_1$ e $\bar{v}_2$, essi sono linearmente dipendenti, se e solo se $\exists \alpha \neq 0 | \bar{v}_1 = \alpha \cdot \bar{v}_2$ (sono proporzionali).

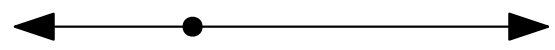
Dimostrazione Oss. 3 : Iniziamo dimostrando il primo verso dell'implicazione, per ipotesi, $\bar{v}_1$ e $\bar{v}_2$ sono linearmente dipendenti : $\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 = \bar{0}$, si dia il caso che $\alpha_1 \neq 0$, allora $v_1 = -\frac{\alpha_2}{\alpha_1}\bar{v}_2$. Dimostriamo ora il secondo verso dell'implicazione, se $\bar{v}_1 = \alpha\bar{v}_2$ per qualche α, allora $\bar{v}_1 - \alpha\bar{v}_2 = \bar{0}$, ed il coefficente di $\bar{v}_1$ è diverso da 0. ■

10.3.1 Esempi Geometrici

Si consideri lo spazio vettoriale V_0^2 visto nel capitolo 10.0.1, abbiamo visto che due vettori sono linearmente indipendenti, se e solo se non sono proporzionali, geometricamente parlando, sul piano, due vettori sono linearmente indipendenti se non giaciono sulla stessa retta.

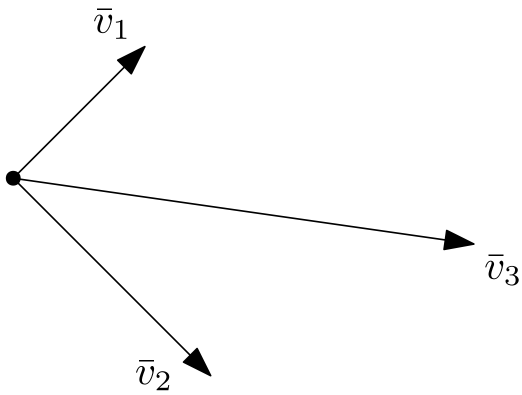


Sono linearmente indipendenti

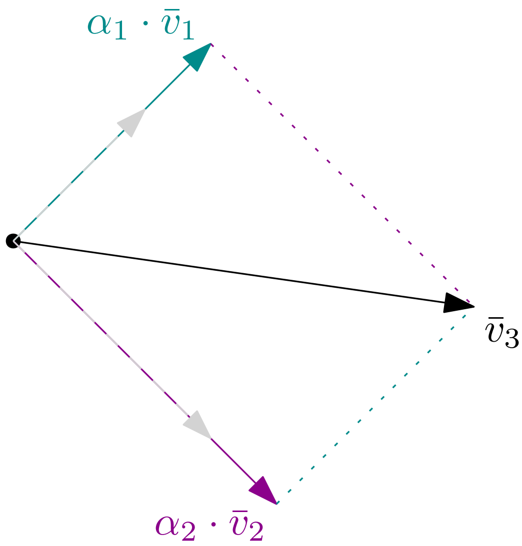


Sono linearmente dipendenti

Consideriamo adesso 3 vettori sul piano :



Notiamo che la somma di $\bar{v}_1 + \bar{v}_2 \neq \bar{v}_3$, ma $\exists \alpha_1, \alpha_2 \in \mathbb{R} | \bar{\alpha}_1 v_1 + \bar{\alpha}_2 v_2 = \bar{v}_3$, allungando o restringendo i due vettori, possiamo formare i due lati, del parallelogramma di diagonale $\bar{v}_3$:



Questo vuol dire che, $\bar{v}_3$ è risultato di una combinazione lineare di $\bar{v}_1, \bar{v}_2$, per l'osservazione 2, sono linearmente dipendenti, ne segue la seguente proposizione :

Proposizione : Siano $\bar{v}_1, \bar{v}_2, \bar{v}_3$ 3 vettori in V_0^2, se $\bar{v}_1$ e $\bar{v}_2$ sono linearmente indipendenti, allora $\bar{v}_1, \bar{v}_2, \bar{v}_3$ sono linearmente dipendenti.

Osservazione : Si considerino i k vettori dello spazio $W = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k\}$, se in W vi sono j vettori (con $j < k$) linearmente dipendenti, allora, anche i vettori $W = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k\}$ sono linearmente dipendenti.

Dimostrazione : Supponiamo che $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_j$ siano j linearmente dipendenti, ne segue che $\alpha_1\bar{v}_1 + \cdots + \alpha_j\bar{v}_j = \bar{0}$, con i coefficenti non tutti nulli. Consideriamo adesso $\bar{v}_{j+1}, \bar{v}_{j+2} \ldots, \bar{v}_k$, e sommiamoli alla combinazione lineare, moltiplicati a dei coefficenti nulli, del tipo :

$$\alpha_1\bar{v}_1 + \cdots + \alpha_j\bar{v}_j + 0 \cdot \bar{v}_{j+1} + 0 \cdot \bar{v}_{j+2} \cdots + 0 \cdot \bar{v}_k = \bar{0}$$

Ma questa, è pure sempre una combinazione lineare nulla con coefficenti non tutti nulli, quindi, i vettori $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_j, \bar{v}_{j+1}, \bar{v}_{j+2} \ldots, \bar{v}_k$ sono linearmente dipendenti. ■

Osservazione : Se in $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k$ ci sono due vettori identici, allora $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k$ sono linerarmente dipendenti.

10.4 Base di uno Spazio Vettoriale

Sia V uno spazio vettoriale, allora, una collezione finita di vettori $\mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k\}$ si dice *base* per V se:

- $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k$ sono linearmente indipendenti.
- $V = \text{Span}(\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k)$

Esempio : In V_O^2, qualsiasi coppia di vettori non proporzionali è una base.

Osservazione : Se $\mathcal{B}$ è una base, è un massimale di vettori linearmente indipendenti in V.

In questo corso ci occuperemo di spazi vettoriali **finitamente generati**, ossia, che hanno base di cardinalità finita. Tutte le basi di uno spazio V hanno la stessa cardinalità (lo vedremo in uno dei teoremi che seguono), e tale cardinalità è detta **dimensione** dello spazio vettoriale, ad esempio, $\mathbb{R}^n$ ha dimensione n, invece V_O^2 ha dimensione 2.

Teorema 1 : Se V è uno spazio vettoriale finitamente generato, allora ha una base.

Teorema del Completamento : Sia $\mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_n\}$ n vettori che costituiscono una base di V, e siano $\{\bar{w}_1, \bar{w}_2 \ldots, \bar{w}_k\}$ k vettori di V linearmente indipendenti, con $k \leq n$. Allora, esistono esattamente $n - k$ vettori in $\mathcal{B}$, tali che, se aggiunti all'insieme $\{\bar{w}_1, \bar{w}_2 \ldots, \bar{w}_k\}$, esso costituirà una base di V.

Corollario : Se V è uno spazio vettoriale finitamente generato, e $\mathcal{B}$ e $\mathcal{B}'$ sono due basi di V, allora $|\mathcal{B}| = |\mathcal{B}'|$.

Dimostrazione Corollario : Siano $\mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_n\}$ e $\mathcal{B}' = \{\bar{v}'_1, \bar{v}'_2 \ldots, \bar{v}'_m\}$ due basi di V, se $n > m$, posso trovare $n - m$ vettori in $\mathcal{B}'$ in modo tale che $\{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_n, \bar{v}'_i \ldots, \bar{v}'_{i_{n-m}}\}$ sia una base, ma questo va in contraddizione con il fatto che una base, dovrebbe essere un massimale di vettori linearmente indipendenti, quindi è impossibile che $n > m$, può essere che $n \geq m$. Analogamente, se $n < m$, posso trovare $m - n$ vettori in $\mathcal{B}$ in modo tale che

$\{\bar{v}'_1, \bar{v}'_2 \dots, \bar{v}'_n, \bar{v}_i \dots, \bar{v}_{i_{n-m}}\}$ sia una base, ma questo va in contraddizione con il fatto che una base, dovrebbe essere un massimale di vettori linearmente indipendenti, quindi è impossibile che $n < m$, può essere che $n \leq m$. Ne concludiamo che $n = m$. ■

Un esempio di spazio vettoriale di *dimensione infinita*, quindi che non è finitamente generato, è lo spazio $V = \mathbb{R}[x]$ dei polinomi a coefficenti reali ad una variabile, alcuni esempi :

$$x^2 \qquad x+1 \qquad 4x^3 - 2x + 6$$

Non esiste nessun insieme finito che può generare qualsiasi polinomio, in quanto, un qualsiasi polinomio di grado n, richiede almeno un elemento nell'insieme dei generatori di grado n, essendo che un polinomio può assumere qualsiasi grado, l'insieme dei generatori sarà infinito (ma numerabile).

Proposizione : Se V è uno spazio vettoriale su un campo $\mathbb{K}$, finitamente generato, allora la mappa :

$$\phi_B : \mathbb{K}^n \to V \text{ tale che } \phi_B(a_1, a_2 \dots, a_n) = a_1\bar{v}_1 + a_2\bar{v}_2 \dots + a_n\bar{v}_n$$

È un *isomorfismo* di spazi vettoriali.

Dimostrazione : La suriettività deriva dal fatto che ogni elemento di V può essere scritto come combinazione lineare $a_1\bar{v}_1 + a_2\bar{v}_2 \dots + a_n\bar{v}_n$. Inoltre tale mappa mantiene le operazioni :

$$\phi_B((a_1, a_2 \dots, a_n) + (b_1, b_2 \dots, b_n)) = (a_1 + b_1)\bar{v}_1 + (a_2 + b_2)\bar{v}_2 \dots + (a_n + b_n)\bar{v}_n \tag{97}$$

$$= (a_1\bar{v}_1 + a_2\bar{v}_2 \dots + a_n\bar{v}_n) + (b_1\bar{v}_1 + b_2\bar{v}_2 \dots + b_n\bar{v}_n) = \phi_B(a_1, a_2 \dots, a_n) + \phi_B(b_1, b_2 \dots, b_n) \tag{98}$$

Anche sul prodotto per uno scalare :

$$\phi_B(\lambda \cdot (a_1, a_2 \dots, a_n)) = \lambda a_1\bar{v}_1 + \lambda a_2\bar{v}_2 \dots + \lambda a_n\bar{v}_n = \lambda\phi_B(a_1, a_2 \dots, a_n) \tag{99}$$

Essendo che la base di V è composta da vettori linearmente indipendenti, è anche iniettiva. ■

10.4.1 Criteri per la Ricerca di una Base

Presi k elementi di uno spazio vettoriale V, dove k è la dimensione dello spazio, se questi sono generatori, oppure linearmente indipendenti, allora costituiscono una base di V.

Notazione : La dimensione di uno spazio vettoriale V, sarà denotata $\dim(V)$.

Proposizione : Sia V uno spazio vettoriale finitamente generato sul campo $\mathbb{K}$, e sia W un suo sottospazio vettoriale, allora :

1. W ha una dimensione finita ed è finitamente generato.
2. Se $W \neq V$ allora $\dim(W) < \dim(V)$, altrimenti $\dim(W) = \dim(V)$.

Dimostrazione : Si consideri $\bar{w}_1 \in W$ un qualsiasi elemento di W, ci sono due possibilità, o $\bar{w}_1$ genera W (e quindi si dimostra che W è finitamente generato), oppure,
$\exists \bar{w}_2 \in W \backslash \text{Span}(\bar{w}_1)$. tale $\bar{w}_2$, è linearmente indipendente da $\bar{w}_1$, ci sono due possibilità, o $\bar{w}_1, \bar{w}_2$ generano W (e quindi si dimostra che W è finitamente generato), oppure,
$\exists \bar{w}_3 \in W \backslash \text{Span}(\bar{w}_1, \bar{w}_2)$, e quest'ultimo è linearmente indipendente da $\bar{w}_1, \bar{w}_2$. Si continua in

maniera iterativa il procedimento, che ovviamente non può continuare all'infinito, in quanto al più si trovera un insieme $\bar{w}_1, \bar{w}_2 \dots, \bar{w}_n$ che genera tutto V. ■

L'insieme della matrici simmetriche $n \times n$, che denoteremo S_n, rappresenta un sottospazio vettoriale dell'insieme delle matrici $M_{n\times n}$, stessa cosa per le matrici antisimmetriche A_n, ossia per cui ($\forall i, j$, si ha che $a_{i_j} = -a_{j_i}$).

Ci chiediamo adesso quale sia sia la dimensione di S_n. Denotiamo con E_{i_j} la matrice che ha 0 in tutte le posizioni, esclusa la posizione i, j in cui ha 1. La collezione di tutte le matrici E_{i_j} $\forall i, j$ costituisce una base di $M_{n\times n}$. Le matrici simmetriche possono essere scritte nella forma :

$$a_{1_1}E_{1_1} + a_{2_2}E_{2_2} \cdots + a_{n_n}E_{n_n} + \sum_{i\leq 1<j\leq n} a_{i_j}(E_{i_j} + E_{j_i}) \tag{100}$$

E questi elementi costituiscono la base di S_n, che ha dimensione $\dfrac{n\cdot(n+1)}{2}$. Analogamente, le matrici antisimmetriche hanno dimensione $\dfrac{n\cdot(n-1)}{2}$, si noti che :

$$\dim(S_n) + \dim(A_n) = \frac{n\cdot(n+1)}{2} + \frac{n\cdot(n-1)}{2} = n^2 = \dim(M_{n\times n}) \tag{101}$$

Non è una coincidenza, in quanto ogni matrice $n \times n$ si scrive in modo unico come somma di una matrice simmetrica per una antisimmetrica.

Definizione : La *matrice trasposta* di una matrice A, indicata con ${}^tA$, è la matrice che, in ogni posizione i, j, ha l'elemento $a_{j_i} \in A$. Sia A una qualsiasi matrice, si ha che : $\dfrac{A + {}^tA}{2}$ è una matrice simmetrica e $\dfrac{A - {}^tA}{2}$ è una matrice antisimmetrica.

Proposizione : Ogni matrice A, può essere scritta nella forma $\dfrac{A + {}^tA}{2} + \dfrac{A - {}^tA}{2}$, e tale scrittura è *unica.*

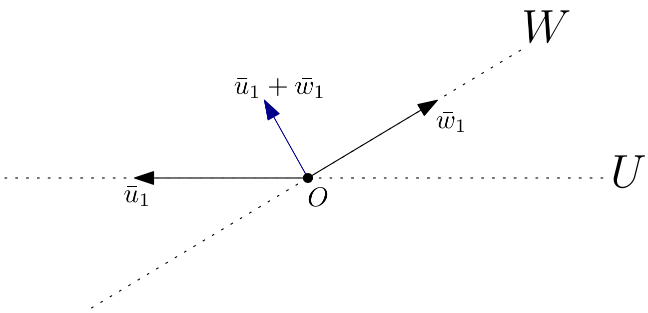
Dimostrazione (unicità) : Sia A una matrice non nulla, poniamo che possa essere scritta come somma di matrice simmetrica per antisimmetrica in due modi : $A = S + T$ e $A = S' + T'$, con S, S' simmetriche e T, T' antisimmetriche. Si ha che $A = S + T = S' + T' \implies S - S' = T - T'$, questo significherebbe che tale matrice è sia simmetrica che antisimmetrica, e l'unica matriche con tali caratteristiche è la matrice nulla, quindi $S - S' = T - T' = \bar{0} \implies S = S' \wedge T = T'$. ■

10.5 Intersezione e Somma di Sottospazi

Siano $W \leq V$ e $U \leq V$ due sottospazi dello spazio V, è possibile considerare l'intersezione in senso insiemistico, ossia $U \cap W$, ebbene, anche questo è ancora un sottospazio vettoriale di V.

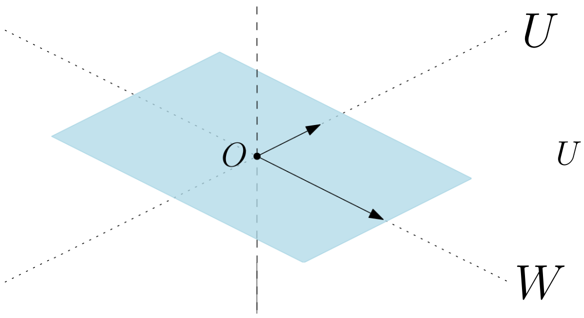
$$\begin{cases} \bar{z}_1, \bar{z}_2 \in W \\ \bar{z}_1, \bar{z}_2 \in U \\ \lambda_1, \lambda_2 \in \mathbb{R} \end{cases} \implies \begin{cases} \lambda_1\bar{z}_1 + \lambda_2\bar{z}_2 \in W \\ \lambda_1\bar{z}_1 + \lambda_2\bar{z}_2 \in U \end{cases} \implies \lambda_1\bar{z}_1 + \lambda_2\bar{z}_2 \in U \cap W \tag{102}$$

Differentemente, l'unione insiemistica, non rappresenta necessariamente un sottospazio, si consideri il seguente esempio in V_O^2, dove i sottospazi (ossia l'insieme dei vettori sulle rette) W ed U, contengono rispettivamente $\bar{u}_1$ e $\bar{w}_1$, la quale somma, si trova al di fuori di $U \cup W$.

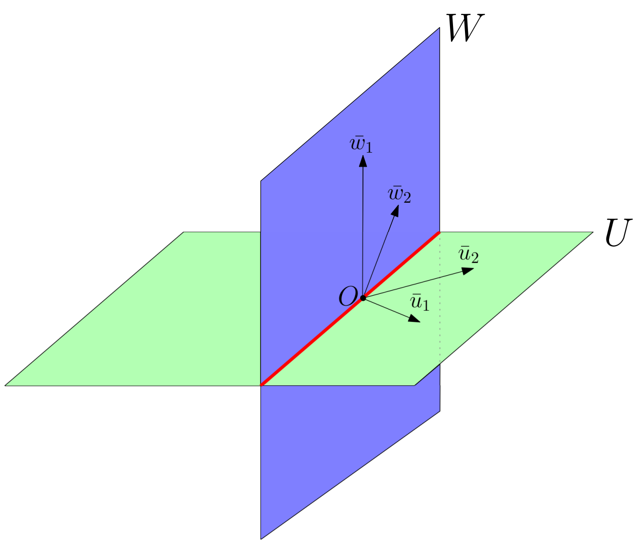


Esiste però, un altro tipo di spazio vettoriale derivante da due sottospazi, ed è il **sottospazio somma**, siano $W \leq V$ e $U \leq V$ due sottospazi dello spazio V, tali che $U = \{\lambda \bar{u}, \lambda \in \mathbb{R}\}$ e $W = \{\lambda \bar{w}, \lambda \in \mathbb{R}\}$, si ha $W + U = \{\lambda_1 \bar{u} + \lambda_2 \bar{w} | \bar{u} \in U, \bar{w} \in W, \lambda_1, \lambda_2 \in \mathbb{R}\}$, si può pensare come lo spazio generato dall'insieme dei generatori di U e di W, ovviamente, i vettori $\bar{u}$ e $\bar{w}$ presi in considerazione sono linearmente indipendenti.

Si consideri il seguente esempio in V_O^3, dove la somma di due sottospazi definiti da due rette, rispettivamente W ed U, generano un piano.



Se $\{\bar{u}_1, \bar{u}_2 \dots, \bar{u}_k\}$ è una base per U, e $\{\bar{w}_1, \bar{w}_2 \dots, \bar{w}_n\}$ è una base per W, è chiaro che $\{\bar{w}_1, \bar{w}_2 \dots, \bar{w}_n, \bar{u}_1, \bar{u}_2 \dots, \bar{u}_k\}$ sia un insieme di generatori per $W + U$, non è detto però, che tale insieme risulti una base. Si consideri di fatto il seguente esempio in V_O^3 :



Si hanno il sottospazio W rappresentato dal piano azzurro, ed il sottospazio U rappresentato dal piano verde, con le rispettive basi $\{\bar{w}_1, \bar{w}_2\}$ per W e $\{\bar{u}_1, \bar{u}_2\}$ per U. La somma di tale sottospazi, ossia lo spazio $U + W$ che ha generatori $\{\bar{w}_1, \bar{w}_2, \bar{u}_1, \bar{u}_2\}$, è uguale a V^3_O, eppure $\{\bar{w}_1, \bar{w}_2, \bar{u}_1, \bar{u}_2\}$ non rappresentano una base per esso, in quanto sappiamo che una base di V^3_O è composta da 3 elementi. La spiegazione formale è data dalla seguente formula.

10.5.1 Formula di Grassmann

Siano U, W due sottospazi di V, vale il seguente enunciato :

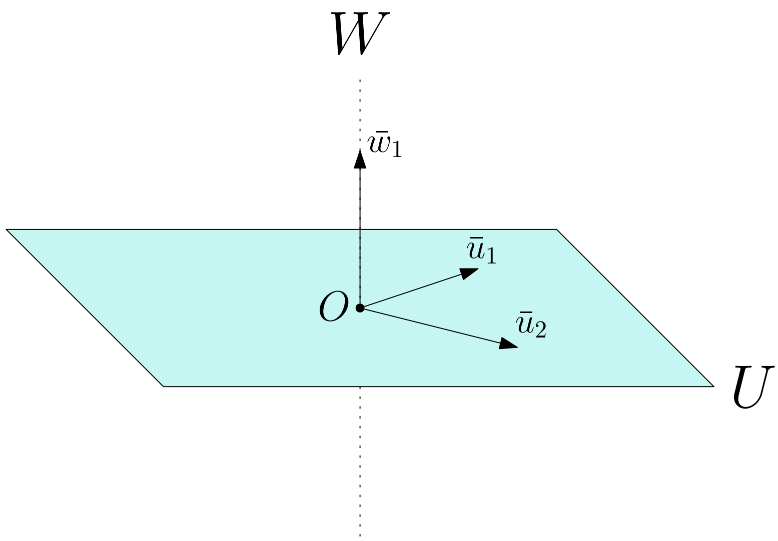
$$\dim(U \cap W) + \dim(U + W) = \dim(U) + \dim(W)$$

L'unione delle due basi, da la base della somma, se e solo se, l'intersezione dei due sottospazi ha solamente il vettore nullo, generante quindi uno spazio di dimensione 0.

Difatti, nell'esempio precedente, l'intersezione dei due piani, rappresentato dalla retta rossa, è essa stessa un sottospazio di dimensione 1, essendo una retta, di fatto, considerando sempre tale esempio, la formula dava l'identità :

$$\dim(U \cap W) + \dim(U + W) = \dim(U) + \dim(W) \implies 1 + 3 = 2 + 2 \tag{103}$$

Ad esempio, consideriamo in V^3_O, due sottospazi W ed U. W, è una retta, con base $\{\bar{w}_1\}$, ed U un piano, con base $\{\bar{u}_1, \bar{u}_2\}$. La retta W, passa per il piano intersecandolo in un punto, l'intersezione, avrà quindi dimensione zero, de facto, per la formula di Grassmann, l'unione fra la base di W e la base di U, forniranno una base per $U + W$, che sarebbe tutto V^3_O.



Definizione : Siano U e W due sottospazi di V, diremo che la somma dei due è *diretta*, e scriveremo $U \oplus W$, se $U \cap W = \{\bar{0}\}$, ne consegue che $\dim(U \oplus W) = \dim(U) + \dim(W)$.

Definizione : Sia U un sottospazio di V, diremo che il sottospazio W di V, è il *supplementare* di U in V, se $V = U \oplus W$. Nell'esempio precedente, si ha che $U \oplus W = V^3_O$, quindi sono fra loro supplementari.

Proposizione : Dato un sottospazio, esiste sempre un complementare.

Dimostrazione : Sia U un sottospazio di V, la base di U è $\mathcal{B}_U = \{\bar{u}_1, \bar{u}_2 \ldots, \bar{u}_k\}$, e la base di V è $\mathcal{B}_V = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_n\}$, per il teorema del completamento, esiste un insieme di vettori linearmente indipendenti, sia fra loro, che con $\mathcal{B}_U$, che sono in numero $n-k$, che se aggiunti a $\mathcal{B}_U$ forniscono una base per V. Per definizione, tale insieme risulta essere la base del supplementare di V, garantendone quindi l'esistenza. ■

11 Applicazioni Lineari

Nel capitolo 8 si è parlato di omomorfismi fra gruppi, vediamo adesso il corrispettivo per gli spazi vettoriali.

Siano $(V, +_V, \cdot_V)$ e $(W +_W, \cdot_W)$ due spazi vettoriali su un campo $\mathbb{K}$, e sia $T : V \to W$ un'applicazione fra di essi. Tale applicazione è detta **lineare** se, conserva le operazioni :

$$\begin{matrix} T(\bar{v}_1 +_V \bar{v}_2) = T(\bar{v}_1) +_W T(\bar{v}_2) \\ T(\lambda \cdot_V \bar{v}_1) = \lambda \cdot_W T(\bar{v}_1) \end{matrix} \qquad \bar{v}_1, \bar{v}_2 \in V, \quad \lambda \in \mathbb{K}$$

Esempio fondamentale : Si fissi una matrice $A \in M_{m\times n}(\mathbb{R})$, e considero la seguente applicazione $L_A : \mathbb{R}^n \to \mathbb{R}^m$, tale che :

$$L_A\left(\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix}\right) = \begin{bmatrix} a_{1_1}x_1 + a_{1_2}x_2 \cdots + a_{1_n}x_n \\ a_{2_1}x_1 + a_{2_2}x_2 \cdots + a_{2_n}x_n \\ \cdots \\ a_{m_1}x_1 + a_{m_2}x_2 \cdots + a_{m_n}x_n \end{bmatrix} \equiv x_1 \begin{bmatrix} a_{1_1} \\ a_{2_1} \\ \cdot \\ a_{m_1} \end{bmatrix} + x_2 \begin{bmatrix} a_{1_2} \\ a_{2_2} \\ \cdot \\ a_{m_2} \end{bmatrix} \cdots + x_n \begin{bmatrix} a_{1_n} \\ a_{2_n} \\ \cdot \\ a_{m_n} \end{bmatrix}$$

Dove a_{i_j} è il coefficente reale alla posizione (i, j) della matrice A. Tale applicazione, risulta essere *lineare*, data la seguente verifica :

$$L_A\left(\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix} + \begin{bmatrix} x'_1 \\ x'_2 \\ \cdot \\ x'_n \end{bmatrix}\right) = \begin{bmatrix} a_{1_1}(x_1 + x'_1) + a_{1_2}(x_2 + x'_2) \cdots + a_{1_n}(x_n + x'_n) \\ a_{2_1}(x_1 + x'_1) + a_{2_2}(x_2 + x'_2) \cdots + a_{2_n}(x_n + x'_n) \\ \cdots \\ a_{m_1}(x_1 + x'_1) + a_{m_2}(x_2 + x'_2) \cdots + a_{m_n}(x_n + x'_n) \end{bmatrix} \tag{104}$$

Essendo nel campo $\mathbb{R}$, posso applicare le proprietà di campo :

$$= \begin{bmatrix} a_{1_1}x_1 + a_{1_1}x'_1 + a_{1_2}x_2 + a_{1_2}x'_2 \cdots + a_{1_n}x_n + a_{1_n}x'_n \\ a_{2_1}x_1 + a_{2_1}x'_1 + a_{2_2}x_2 + a_{2_2}x'_2 \cdots + a_{2_n}x_n + a_{2_n}x'_n \\ \cdots \\ a_{m_1}x_1 + a_{m_1}x'_1 + a_{m_2}x_2 + a_{m_2}x'_2 \cdots + a_{m_n}x_n + a_{m_n}x'_n \end{bmatrix} = \tag{105}$$

$$= \begin{bmatrix} a_{1_1}x_1 + a_{1_2}x_2 \cdots + a_{1_n}x_n \\ a_{2_1}x_1 + a_{2_2}x_2 \cdots + a_{2_n}x_n \\ \cdots \\ a_{m_1}x_1 + a_{m_2}x_2 \cdots + a_{m_n}x_n \end{bmatrix} + \begin{bmatrix} a_{1_1}x'_1 + a_{1_2}x'_2 \cdots + a_{1_n}x'_n \\ a_{2_1}x'_1 + a_{2_2}x'_2 \cdots + a_{2_n}x'_n \\ \cdots \\ a_{m_1}x'_1 + a_{m_2}x'_2 \cdots + a_{m_n}x'_n \end{bmatrix} = L_A\left(\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix}\right) + L_A\left(\begin{bmatrix} x'_1 \\ x'_2 \\ \cdot \\ x'_n \end{bmatrix}\right) \tag{106}$$

Analogamente, si verifica che $L_A\left(\lambda \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix}\right) = \lambda L_A\left(\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix}\right)$.

Proprietà : Se $T : V \to W$ è un applicazione lineare, allora $T(\bar{0}_V) = \bar{0}_W$. La verifica risulta semplice, di fatto $T(\bar{0}_V) = T(0 \cdot \bar{0}_V) = 0 \cdot T(\bar{0}_V) = \bar{0}_W$.

Consideriamo adesso un altra importante applicazione lineare nota, sia V uno spazio vettoriale di dimension n sul campo $\mathbb{R}$ (o qualsiasi altro campo), V ha base $\mathcal{B} = \{\bar{b}_1 \dots, \bar{b}_n\}$. Esiste un applicazione lineare $F_{\mathcal{B}} : V \to \mathbb{R}^n$, che associa ad un vettore $\bar{v}$, le sue coordinate, ossia i coefficenti della combinazione lineare che ha come risultato proprio $\bar{v}$.

$$F_{\mathcal{B}}(\bar{v}) = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdot \\ \alpha_n \end{bmatrix} \qquad \text{tale che} \qquad \bar{v} = \alpha_1 \bar{b}_1 + \alpha_2 \bar{b}_2 \cdots + \alpha_n \bar{b}_n$$

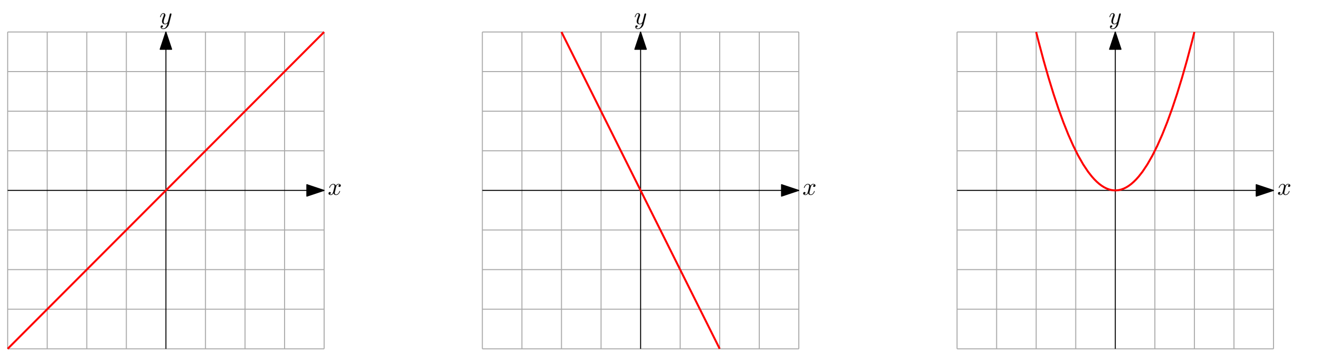
Si ha infatti che le coordinate del vettore $\bar{v} + \bar{v}'$, sono le coordinate del vettore $\bar{v}$ sommate alle coordinate del vettore $\bar{v}'$.

Vediamo adesso un esempio di applicazione *non* lineare, ossia $T : \mathbb{R}^2 \to \mathbb{R}^2$ tale che : $T((x_1, x_2)) = (x_1^2 + x_2^2, x_1^2 - x_2^2)$. Tale applicazione non conserva le operazioni, infatti :

$$T((1,1) + (-1,-1)) = T((0,0)) = (0,0) \neq (2,0) = T((1,1)) + T((-1,-1)) \tag{107}$$

Non è lineare perché vi sono i quadrati, le applicazioni lineari infatti sono molto particolari, nel corso di *Analisi*, sono state trattate funzioni, per la maggiorparte non lineari, le uniche funzioni di una variabile reale lineari, son quelle del tipo $f(x) = c \cdot x$, dove c è una costante.

$f(x) = x$ $\qquad$ $f(x) = -2x$ $\qquad$ $f(x) = x^2$



lineare $\qquad$ lineare $\qquad$ non lineare

Proposizione : Si consideri la trasformazione lineare vista in precedenza $L_A : \mathbb{R}^n \to \mathbb{R}^m$, si ha che $L_A = L_B \iff A = B$.

11.1 Nucleo ed Immagine di un Applicazione Lineare

Data un'applicazione lineare, esistono due **noti sottospazi**, sia $T : V \to W$, si ha che :

1. $Im(T) = \{T(\bar{v}) | \bar{v} \in V\}$ è un sottospazio di W.
2. $KerT = \{\bar{v} | T(\bar{v}) = \bar{0}_W\}$ è un sottospazio di V.

Dimostrazione : (1) - Siano $\bar{y}_1, \bar{y}_2 \in Im(T)$, quindi $\bar{y}_1 = T(\bar{v}_1)$ e $\bar{y}_2 = T(\bar{v}_2)$, ho che $\bar{y}_1 + \bar{y}_2 = T(\bar{v}_1) + T(\bar{v}_2)$ =per linearità= $T(\bar{v}_1 + \bar{v}_2) \in Im(T)$, inoltre, $\lambda \bar{y}_1 = \lambda T(\bar{v}_1)$ =per linearità= $T(\lambda \bar{v}_1) \in Im(T)$.

(2) - Siano $\bar{v}_1, \bar{v}_2 \in KerT$, allora
$T(\bar{v}_1 + \bar{v}_2) = T(\bar{v}_1) + T(\bar{v}_2) = 0_W + 0_W = 0_W \implies \bar{v}_1 + \bar{v}_2 \in KerT$, analogamente,
$T(\lambda \bar{v}_1) = \lambda T(\bar{v}_1) = \lambda 0_W = 0_W \implies \lambda \bar{v}_1 \in KerT$. ■

Proposizione : Un applicazione lineare $T : V \to W$ è iniettiva se e solo se $KerT = \{\bar{0}_V\}$.

Dimostrazione : Dimostriamo il primo verso dell'implicazione, l'ipotesi è che l'applicazione sia iniettiva. Per definizione, $\bar{v} \in KerT \implies T(\bar{v}) = \bar{0}_W$, ma sicuramente, per definizione di applicazione lineare, $T(\bar{0}_V) = \bar{0}_W$, si ha che $T(\bar{v}) = T(\bar{0}_V)$, essendo però T iniettiva, $\bar{v} = \bar{0}_V$.
Dimostriamo l'altro verso, supponendo che $KerT = \{\bar{0}_V\}$. Siano $\bar{v}_1, \bar{v}_2 \in V$, so che
$T(\bar{v}_1) = T(\bar{v}_2) \iff T(\bar{v}_1) - T(\bar{v}_2) = \bar{0}_W \iff T(\bar{v}_1 - \bar{v}_2) = \bar{0}_W$, ma allora, per ipotesi
$\bar{v}_1 - \bar{v}_2 = \bar{0}_V \implies \bar{v}_1 = \bar{v}_2 \implies T$ è iniettiva. ■

Proposizione : Sia $T : V \to W$ un applicazione lineare, e $\mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_n\}$ una base di V, allora $Im(T) = \text{Span}(T(\bar{v}_1), T(\bar{v}_2) \ldots, T(\bar{v}_n))$, quindi $T(\bar{v}_1), T(\bar{v}_2) \ldots, T(\bar{v}_n)$ sono dei generatori per l'immagine di T, ma non necessariamente una base.

Dimostrazione : $Im(T) = \{T(\alpha_1 \bar{v}_1 + \alpha_2 \bar{v}_2 \cdots + \alpha_n \bar{v}_n)\}$, applico la linearità :
$Im(T) = \{T(\alpha_1 \bar{v}_1) + T(\alpha_2 \bar{v}_2) \cdots + T(\alpha_n \bar{v}_n)\} = \{\alpha_1 T(\bar{v}_1) + \alpha_2 T(\bar{v}_2) \cdots + \alpha_n T(\bar{v}_n)\} =$
$\text{Span}(T(\bar{v}_1), T(\bar{v}_2) \ldots, T(\bar{v}_n))$. ■

Corollario : Sia L_A l'applicazione lineare definita all'inizio del capitolo 11, con $A \in M_{m \times n}(\mathbb{R})$, dove $A^1, A^2 \ldots, A^n$ sono le colonne (quindi tuple di m elementi) della matrice A, si ha che:

$$Im(L_A) = \text{Span}(A^1, A^2 \ldots, A^n)$$

Esempio : Sia $A = \begin{bmatrix} 1 & -1 & 0 \\ -2 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, con $L_A(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}) = x_1 \begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} -1 \\ 2 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, ho che:

$$KerL_A = \{\bar{x} | \begin{cases} x_1 - x_2 = 0 \\ -2x_1 + 2x_2 = 0 \\ x_3 = 0 \end{cases} \} \text{ che è equivalente a } \{\bar{x} | \begin{cases} x_1 - x_2 = 0 \\ x_3 = 0 \end{cases} \}$$

Noto che le soluzioni di tale sistema, sono proprio il nucleo di L_A, che risulta essere :

$$KerL_A = \text{Span}(\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix})$$

Per il corollario precedente, so che $Im(L_A) = \text{Span}(\begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix})$, ma le prime due colonne, sono proporzionali, quindi posso riscrivere : $Im(L_A) = \text{Span}(\begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix})$.

A questo punto, ho trovato le basi di immagine e nucleo, e so che hanno rispettivamente dimensione 2 e 1. L'applicazione lineare L_A, ha come insieme di partenza $\mathbb{R}^3$, che ha dimensione 3, ci si rende quindi conto di un importante correlazione.

11.1.1 Teorema della Dimensione

Sia $T : V \to W$ un applicazione lineare, vale che :

$$\dim(V) = \dim(Im(T)) + \dim(KerT)$$

La somma delle dimensioni dell'immagine e del nucleo, è uguale alla dimensione dell'insieme di partenza.

Appunto sulla *Notazione* !

- Denotiamo $\text{rg}(T) = \dim(Im(T))$, detto **rango di** T.
- Denotiamo $\text{rg}(A) = \text{rg}(L_A) = \dim(Im(L_A))$. Il **rango di una matrice** è il rango dell'applicazione ad essa associata.

Si ha che $\text{rg}(T) \leq \dim(W)$ e $\text{rg}(T) \leq \dim(V)$.

Dimostrazione : Sia $\dim(V) = n$, si consideri il sottospazio $KerT \leq V$, che ha base $\{\bar{v}_1 \ldots, \bar{v}_r\}$, per il teorema del completamento, posso aggiungere $n - r$ vettori $\{\bar{v}_{r+1} \ldots, \bar{v}_n\}$, tale che $\{\bar{v}_1 \ldots, \bar{v}_r, \bar{v}_{r+1} \ldots, \bar{v}_n\}$ costituiscano una base di V. Considero l'immagine dei vettori aggiunti, ossia, gli $n - r$ vettori : $\{T(\bar{v}_{r+1}) = \bar{w}_1 \ldots, T(\bar{v}_n) = \bar{w}_{n-r}\}$, mi basta dimostrare adesso, che $\bar{w}_1 \ldots, \bar{w}_{n-r}$ siano una base per $Im(T)$. So che
$Im(T) = \{T(\bar{v})|\bar{v} \in V\} = \{T(\alpha_1\bar{v}_1 \cdots + \alpha_r\bar{v}_r + \beta_1\bar{v}_{r+1} \cdots + \beta_{n-r}\bar{v}_n)|\alpha_i, \beta_j \in \mathbb{R}\}$, dato che un qualsiasi vettore $\bar{v}$ è combinazione lineare dei vettori $\{\bar{v}_1 \ldots, \bar{v}_r, \bar{v}_{r+1} \ldots, \bar{v}_n\}$. Ora applico la linearità di T, ed ho che
$Im(T) = \{\alpha_1T(\bar{v}_1) \cdots + \alpha_rT(\bar{v}_r) + \beta_1T(\bar{v}_{r+1}) \ldots \beta_{n-r}T(\bar{v}_n)|\alpha_i, \beta_j \in \mathbb{R}\}$, ma ricordando che i vettori $\{\bar{v}_1 \ldots, \bar{v}_r\}$ fanno parte del nucleo, ne consegue che : $Im(T) =$
$\{\beta_1T(\bar{v}_{r+1}) \ldots \beta_{n-r}T(\bar{v}_n)|\beta_j \in \mathbb{R}\} = \text{Span}(T(\bar{v}_{r+1}), T(\bar{v}_{r+2}) \ldots, T(\bar{v}_{r+n})) = \text{Span}(\bar{w}_1 \ldots, \bar{w}_{n-r})$, quindi tali elementi generano $Im(T)$, dimostro ora che sono indipendenti :

$$\gamma_1\bar{w}_1 \cdots + \gamma_{n-r}\bar{w}_{n-r} = \bar{0} \implies \gamma_1T(\bar{v}_{r+1}) \cdots + \gamma_{n-r}T(\bar{v}_{n-r}) = \bar{0} \tag{108}$$

$$\implies T(\gamma_1\bar{v}_{r+1} \cdots + \gamma_{n-r}\bar{v}_{n-r}) = \bar{0} \implies \gamma_1\bar{v}_{r+1} \cdots + \gamma_{n-r}\bar{v}_{n-r} \in KerT \tag{109}$$

$$\implies \gamma_1\bar{v}_{r+1} \cdots + \gamma_{n-r}\bar{v}_{n-r} = \delta_1\bar{v}_1 \cdots + \delta_r\bar{v}_r \implies \delta_1\bar{v}_1 \cdots + \delta_r\bar{v}_r + (-\gamma_1)\bar{v}_{r+1} \cdots + (-\gamma_{n-r})\bar{v}_{n-r} = \bar{0} \tag{110}$$

$$\implies \delta_1 = \cdots = \delta_r = -\gamma_{r+1} = \cdots = -\gamma_{n-r} = 0 \implies \gamma_{r+1} = \cdots = \gamma_{n-r} = 0 \tag{111}$$

Quindi, i vettori $\bar{w}_1 \ldots, \bar{w}_{n-r}$ sono linearmente indipendenti, e costituiscono una base per l'immagine di T. ■

Corollario : Sia $T : V \to W$ un applicazione lineare :

1. T è iniettiva se e solo se $\text{rg}(T) = \dim(V)$.
2. T è suriettiva se e solo se $\text{rg}(T) = \dim(W)$.
3. Se $\dim(V) = \dim(W)$, allora T è biettiva.

Prima di enunciare un altro importante teorema, è necessario introdurre il concetto seguente.

Proposizione : Sia $\Sigma \subset \mathbb{R}^n$ l'insieme delle soluzioni del sistema $A\bar{x} = \bar{b}$, con $A \in M_{n\times n}(\mathbb{R})$. Sia Σ_0, l'insieme delle soluzioni del sistema omogeneo associato $A\bar{x} = \bar{0}$. Sia $\tilde{x} \in \Sigma$ una soluzione particolare del sistema, si ha che $\Sigma = \tilde{x} + \Sigma_0$.

Dimostrazione : $\boxed{\tilde{x} + \Sigma_0 \subseteq \Sigma}$: Considero $\bar{w} \in \tilde{x} + \Sigma_0 \implies \bar{w} = \tilde{x} + \bar{y}$ con $\bar{y} \in \Sigma_0$, ciò implica che $L_A(\bar{w}) = L_A(\tilde{x} + \bar{y})$, ma per linearità ho $L_A(\bar{w}) = L_A(\tilde{x}) + L_A(\bar{y})$, ma essendo $\bar{y}$ soluzione del sistema omogeneo, ho che $L_A(\bar{y}) = 0$, quindi $L_A(\bar{w}) = L_A(\tilde{x}) \implies \bar{w} \in \Sigma$.
$\boxed{\Sigma \subseteq \tilde{x} + \Sigma_0}$: Considero un qualsiasi $\bar{z} \in \Sigma$, vuol dire che $L_A(\bar{z}) = \bar{b}$, adesso, riscrivo $\bar{z} = \tilde{x} + (\bar{z} - \tilde{x})$, dove $\tilde{x}$ è una soluzione particolare di Σ. A questo punto, mi basta dimostrare che $(\bar{z} - \tilde{x}) \in \Sigma_0$, considero $L_A(\bar{z} - \tilde{x})$, per linearità ho $L_A(\bar{z}) - L_A(\tilde{x})$, ma essendo entrambe soluzioni del sistema, ne risulta che $L_A(\bar{z}) - L_A(\tilde{x}) = \bar{b} - \bar{b} = \bar{0}$, ma $\bar{0}$ è sicuramente soluzione del sistema omogeneo associato, quindi $\bar{z} - \tilde{x} \in \Sigma_0 \implies \bar{z} \in \tilde{x} + \Sigma_0$. $\blacksquare$

11.1.2 Teorema di Rouché-Capelli

Sia $A\bar{x} = \bar{b}$ un sistema lineare quadrato, tale che $A \in M_{n\times n}(\mathbb{R})$, e sia $A|\bar{b}$, la matrice ottenuta, aggiungendo alla matrice A, una nuova colonna, ossia $\bar{b}$, ne segue che :

1. $A\bar{x} = \bar{b}$ ammette soluzione se e soltanto se $\text{rg}(A) = \text{rg}(A|\bar{b})$.

2. Esiste un unica soluzione se e soltanto se $\text{rg}(A) = n$.

Dimostrazione : (1) - Abbiamo visto nel capitolo 10.2, che il sistema $A\bar{x} = \bar{b}$ ammette soluzione se e solo se $\bar{b} \in \text{Span}(A^1, A^2 \dots, A^n)$, dove A^j è la j-esima colonna di A, questo vuol dire che, essendo $\bar{b}$ combinazione lineare delle colonne, vale che
$\text{Span}(A^1, A^2 \dots, A^n) = \text{Span}(A^1, A^2 \dots, A^n, \bar{b})$, ma lo span delle colonne, per il corollario vista in precedenza, è l'immagine di L_A, si ha quindi che
$\dim(Im(L_A)) = \dim(Im(L_{A|\bar{b}})) \implies \text{rg}(A) = \text{rg}(A|\bar{b})$.
(2) - Il sistema, ha un unica soluzione, se e solo se, l'unica soluzione del sistema omogeneo associato è $\bar{0}$, questo implicherebbe che $KerL_A = \{\bar{0}\} \implies \dim(KerL_A) = 0$, per il teorema della dimensione, so che $\dim(\mathbb{R}^n) = \dim(Im(L_A)) + \dim(KerL_A)$, ma ho che :

$$\begin{cases} \dim(\mathbb{R}^n) = n \\ \dim(KerL_A) = 0 \end{cases} \implies \dim(Im(L_A)) = \text{rg}(L_A) = \text{rg}(A) = n \qquad \blacksquare$$

Teorema : Sia A una matrice, vale che $\text{rg}(A) = \text{rg}({}^tA)$.

Definizione : Una matrice rettangolare $m \times n$, è detta **a scala** se è della seguente forma :

$$S = \begin{array}{c} \begin{array}{cccccccccccccccccc} & & & S^{j_1} & & & & S^{j_2} & & & & S^{j_3} & & & S^{j_r} & & & \end{array} \\ \begin{bmatrix} 0 & \cdots & 0 & p_1 & * & \cdots & * & * & * & \cdots & * & * & * & \cdots & * & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & p_2 & * & \cdots & * & * & * & \cdots & * & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & p_3 & * & \cdots & * & * & \cdots & * \\ \vdots & & & & & \vdots & & & & \vdots & & & & \vdots & & & \vdots & \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & p_r & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ & \vdots & & & & & \vdots & & & & \vdots & & & & \vdots & & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \end{array}$$

In rosso, sono cerchiati i *pivot*

Gli elementi $p_1, p_2 \dots p_r$ son detti *pivot*, ed identificanto le colonne $S^{j_1}, S^{j_2} \dots, S^{j_r}$.

Proposizione : $Im(L_S) = Im(S) = \text{Span}(\bar{e}_1 \dots, \bar{e}_r)$, ricordando che $\bar{e}_1 \dots, \bar{e}_n$ sono i vettori della base canonica di $\mathbb{R}^n$. Si ha che $\text{rg}(S) = r$ e che la base dell'immagine di S è $\{S^{j_1}, S^{j_2} \dots, S^{j_r}\}$.

Dimostrazione : Risulta chiaro che $\text{Span}(S^1 \dots, S^n) \subseteq \text{Span}(\bar{e}_1 \dots, \bar{e}_n)$, dimostro che i vettori, ossia le colonne $S^{j_1}, S^{j_2} \dots, S^{j_r}$ sono linearmente indipendenti. Per fare ciò, è necessario trovare tutte le soluzioni del sistema $\alpha_1 S^{j_1} + \alpha_2 S^{j_2} \dots + \alpha_r^{j_r} = \bar{0}$, sicuramente $\bar{0}$ è una soluzione, ma si noti che questo sistema, è triangolare, quindi ha una sola soluzione, che è appunto il vettore nullo, ne consegue che $S^{j_1}, S^{j_2} \dots, S^{j_r}$ sono linearmente indipendenti. ■

Corollario : Sia $S\bar{x} = \bar{c}$ un sistema, dove S è una matrice a scala, tale sistema ha soluzione se e solo se $\bar{c} \in Im(S) \iff \bar{c} \in \text{Span}(\bar{e}_1 \dots, \bar{e}_r) \iff c_{r+1} = c_{r+2} \dots = c_m = 0$. Se il sistema ammette soluzione, allora, l'insieme delle soluzioni sarà uguale all'insieme delle soluzioni del sistema omogeneo associato $S\bar{x} = \bar{0}$, più una soluzione particolare, e si avrà che $\dim(KerS) = n - r$.

Teorema : Sia $A \in M_{m \times n}(\mathbb{R})$, e sia $A\bar{x} = \bar{b}$ un sistema. Tale sistema, può essere ridotto ad un sistema equivalente a scala $S\bar{x} = \bar{c}$ tramite il metodo di Gauss, e ne segue che :

1. $KerA = KerS$
2. $\text{rg}(A) = n - \dim(KerA) = n - \dim(KerS) = \text{rg}(S)$
3. Se $S^{j_1}, S^{j_2} \dots, S^{j_r}$ sono le colonne contenenti i pivot di S, allora $A^{j_1}, A^{j_2} \dots, A^{j_r}$ costituiscono una base di $Im(A)$.

Quali sono le conclusioni di tale teorema? Abbiamo iniziato il capitolo sull'algebra lineare parlando di sistemi quadrati di equazioni lineari, abbiamo poi trattato la teoria degli spazi vettoriale per poter trovare una formula chiusa volta alla risoluzione di sistemi rettangolari.

Se ho un insieme di vettori $\bar{w}_1, \bar{w}_2 \dots, \bar{w}_l$, come trovo una base per $\text{Span}(\bar{w}_1, \bar{w}_2 \dots, \bar{w}_l)$? Per ciò che abbiamo visto dal teorema, formiamo la matrice ;

$$D = \begin{bmatrix} \bar{w}_1 & \bar{w}_2 & \dots & \bar{w}_l \end{bmatrix}$$

Applico il metodo di Gauss per ottenere una matrice a scala S equivalente, essa ha i pivot nelle colonne $S^{j_1}, S^{j_2} \dots, S^{j_r}$, allora, per il teorema visto prima, so che la base per $\text{Span}(\bar{w}_1, \bar{w}_2 \dots, \bar{w}_l)$ è $\bar{w}_{j_1}, \bar{w}_{j_2} \dots, \bar{w}_{j_r}$.

11.1.3 Ricerca del Completamento

Si è parlato poi di teorema del completamento, siano $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$, esattamente k vettori in $\mathbb{R}^n$, con $n > k$, so che esistono $n - k$ vettori, che uniti a questi formano una base per $\mathbb{R}^n$, ma come si trovano? Come prima cosa, considero i vettori della base canonica $\bar{e}_1, \bar{e}_2 \dots, \bar{e}_n$, e formo la matrice

$$D = \begin{bmatrix} \bar{v}_1 & \bar{v}_2 & \dots & \bar{v}_k & \bar{e}_1 & \bar{e}_2 & \dots & \bar{e}_n \end{bmatrix}$$

Applico il metodo di Gauss ed ottengo una matrice a scala S, che ha lo stesso numero di colonne di D, ossia $n+k$. Siano $S^{j_1}, S^{j_2} \dots, S^{j_n}$ le colonne di S dove son contenuti i pivot, e sono in numero n. In queste n colonne, sappiamo già che le prime k, sono linearmente indipendenti, in quanto la matrice D aveva le prime k colonne formate da vettori linearmente indipendenti. Le restanti colonne conteneti i pivot sono $S^{j_{k+1}}, S^{j_{k+2}} \dots, S^{j_r}$, allora, le colonne $D^{j_{k+1}}, D^{j_{k+2}} \dots, D^{j_r}$ son quelle conteneti il completamento.

11.2 Equazioni Parametriche e Cartesiane

Abbiamo due modi per definire un sottospazio W di $\mathbb{R}^n$:

- **Con un equazione parametrica** : $W = \text{Span}(\bar{w}_1, \bar{w}_2 \dots, \bar{w}_k)$.
- **Con delle equazioni cartesiane** :$W = \{\bar{x} \in \mathbb{R}^n | A\bar{x} = \bar{0}\}$ dove A è una matrice con n colonne ed $n-k$ righe. Definendo il sottospazio in questo modo, si ha che $W = KerA$.

Ad esempio, posso rappresentare un piano in $\mathbb{R}^3$ come Span di 2 vettori, oppure come nucleo di una matrice di 3 colonne ed 1 riga.

Come posso passare da un tipo di base all'altro? Vediamolo con un esempio.

$\boxed{\texttt{Cartesiane}\rightarrow\texttt{Parametriche}}$: Ho lo spazio $W = \{\bar{x} \in \mathbb{R}^n | A\bar{x} = \bar{0}\}$, posso considerare la matrice A, ridurla a scala per trovare S, ed avere che $Ker(S) = Ker(A) = W$.
Esempio : Ho $W = \{\bar{x} \in \mathbb{R}^3 | \begin{bmatrix} 1 & -1 & 3 \end{bmatrix} \bar{x} = \bar{0}\}$, ho che la matrice $\begin{bmatrix} 1 & -1 & 3 \end{bmatrix}$ è già a scala, quindi procedo nel trovare la soluzione : Il pivot è a_{1_1}, considero

$$\begin{cases} x_1 = x_2 - 3x_3 \\ x_2 = t_1 \\ x_3 = t_2 \end{cases} \implies \begin{cases} x_1 = t_1 - 3t_2 \\ x_2 = t_1 \\ x_3 = t_2 \end{cases} \implies W = t_1 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + t_2 \begin{bmatrix} -3 \\ 0 \\ 1 \end{bmatrix}, t_1, t_2 \in R$$

Ho quindi trovato i due vettori della base di W.

$\boxed{\texttt{Parametriche}\rightarrow\texttt{Cartesiane}}$: Ho $W = \text{Span}(\bar{w}_1, \bar{w}_2 \dots, \bar{w}_k) \leq \mathbb{R}^n$, so che $\bar{x} \in W \iff \bar{x} = t_1\bar{w}_1 + \dots + t_k\bar{w}_k$ per qualche $t_1, t_2 \dots, t_k$, se il sistema $\begin{bmatrix} \\ \bar{w}_1 & \bar{w}_2 & \dots & \bar{w}_k \\ \\ \end{bmatrix} \begin{bmatrix} \bar{x}_1 \\ . \\ \bar{x}_n \end{bmatrix}$ ha soluzione, lo riduco con Gauss ottenendo un sistema a scala e ne impongo la compatibilità.

Esempio : Ho $W = \text{Span}(\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 1 \end{bmatrix})$, considero $\begin{bmatrix} 1 & -3 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ e lo riduco a scala ottenendo : $\begin{bmatrix} 1 & -3 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2/2 - x_3/3 \\ x_3 - x_2/3 + x_1/3 \end{bmatrix}$ Che è compatibile se e solo se $x_3 - x_2/3 + x_1/3 = 0 \iff x_1 - x_2 + 3x_3 = 0$, che è appunto l'equazione cartesiana ricercata.

11.3 Correlazione fra Mappe Lineari e Matrici

Una matrice, non è altro che un applicazione lineare $f : \mathbb{R}^n \to \mathbb{R}^m$. Cercheremo in questo capitolo di costruire un dizionario tra mappe lineari e matrici. Prima però è necessario considerare alcuni aspetti teorici.

11.3.1 Omomorfismi ed Endomorfismi Lineari

Siano V e W due spazi vettoriali, definiamo un insieme
$\hom(V, W) = \{f : V \to W | f \text{ è lineare}\}$, ossia l'insieme di tutte le applicazioni lineari da V a W. Tale insieme è detto spazio degli *omomorfismi lineari*, e come si può intuire dal nome, ha una naturale struttura di spazio vettoriale, con le seguenti operazioni :

$$f, g \in \hom(V, W), \qquad (f + g)(x) = f(x) + g(x)$$

$$(\lambda \cdot f)(x) = \lambda \cdot f(x)$$

Proposizione : Se $f : V \to W$ è un applicazione lineare *biunivoca*, lo è anche la sua inversa.

Dimostrazione : Essendo f biunivoca esistono unici
$a, b \in V | f(a) = x \wedge f(b) = y \implies f^{-1}(x + y) = f^{-1}(f(a) + f(b))$ ma f è lineare
$\implies f^{-1}(f(a + b)) = a + b = f^{-1}(x) + f^{-1}(y)$. ■

Inoltre la mappe lineari prevedono anche un operazione di **composizione**, se f e g sono due mappe lineari, allora anche $g \circ f$ è lineare.

$$g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y))$$

$$g((f(\lambda x))) = g(\lambda f(x)) = \lambda g(f(x))$$

Quindi definiamo una nuova operazione $(f, g) \to g \circ f$, che ad ogni coppia di mappe lineare, associa la loro composizione, ne seguono le seguenti proprietà :

1. $(f + f') \circ g = f \circ g + f' \circ g$
2. $(\lambda f) \circ g = \lambda(f \circ g)$
3. $f \circ (g + g') = f \circ g + f \circ g'$
4. $f \circ (\lambda g) = \lambda(f \circ g)$

Verifica della la proprietà 1.

$$((f+f')\circ g)(x) = (f+f')(g(x)) = f(g(x))+f'(g(x)) = (f\circ g)(x)+(f'\circ g)(x) = (f\circ g+g'\circ g)(x)$$

Consideriamo adesso un caso particolare degli omomorfismi lineari, ossia quelli delle mappe da V in V : $\hom(V, V)$, si denota con $\mathrm{End}(V)$ ed è detto insieme degli **endomorfismi lineari**. Anche esso è ovviamente uno spazio vettoriale, ma con l'aggiunta dell'operazione di composizione, tenendo conto delle proprietà appena esposte, esso assume una struttura di *anello unitario non commutativo* 3.3. L'unità, è la mappa identità, denotata Id.

Sorge naturali porsi il quesito, di quali siano gli elementi *invertibili* di $\mathrm{End}(V)$, diamo prima una definizione.

Definizione : Un omomorfismo lineare biunivoco, è detto *isomorfismo*.

In una proposizione precedente abbiamo enunciato e dimostrato che, un omomorfismo lineare biunivoco, che ora chiameremo isomorfismo lineare, vede la sua funzione inversa essere ancora lineare. Ciò, fa giungere alla naturale conclusione che, se $\text{End}(V)$ è l'anello degli omomorfismi lineari, i suoi invertibili sono proprio gli isomorfismi.

$$\mathcal{U}(\text{End}(V)) = \{f : V \to V | f \text{ Isomorfismo}\}$$

Tornando allo spazio $\hom(V, W)$, fino ad'ora, non si è parlato di correlazione fra le dimensioni di quest'ultimo e quelle di V e W. Vedremo che se questi due spazi hanno dimensione finita, allora anche $\hom(V, W)$ avrà dimensione finita. So che un applicazione lineare è completamente determinata dalle immagini che ha sui generatori dello spazio di partenza, di fatto, siano $\bar{v}_1, \bar{v}_2 \dots, \bar{v}_k$ una base di V, tale che $\dim(V) = k$, l'applicazione $\phi : \hom(V, W) \to W \times W \cdots \times W$ che associa ad ogni mappa lineare le immagini che ha sulla base, è biettiva.

$$\phi(f) = f(\bar{v}_1), f(\bar{v}_2) \dots, f(\bar{v}_k)$$

Ne deduciamo che $\dim(\hom(V, W)) \leq \dim(W \times W \cdots \times W) \leq k \cdot \dim(W)$. Ne segue che

$$\dim(\hom(V, W)) = \dim(V) \cdot \dim(W)$$

Lemma : Per il teorema della dimensione 11.1.1, sappiamo che f è un isomorfismo se e solo se f è iniettiva (quindi $Ker f = \{\bar{0}\}$) se e solo se f è suriettiva (quindi $Im(f) = W$) se e solo se $\dim(W) = \dim(V)$.

Ciò si ricollega al fatto che, essendo che $\text{End}(V)$ è un anello, ha elementi invertibili, ossia ha isomorfismi, e ciò è possibili perché $\text{End}(V) = \hom(V, V) \implies \dim(V) = \dim(V)$.

11.3.2 Dizionario Mappe-Matrici

Abbiamo parlato di spazio degli omomorfismi lineari, consideriamo adesso $\hom(\mathbb{R}^n, \mathbb{R}^m)$, ossia l'insieme delle applicazioni lineari $f : \mathbb{R}^n \to \mathbb{R}^m$. Sappiamo che un applicazione lineare è determinata da come si comporta sui generatori, consideriamo quindi la base canonica :

$$f\Big(\begin{bmatrix} x_1 \\ x_2 \\ . \\ x_n \end{bmatrix}\Big) = f\Big(x_1\bar{e}_1 + x_2\bar{e}_2 \cdots + x_n\bar{e}_n\Big) = f\Big(\begin{bmatrix} x_1 \\ 0 \\ . \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ x_2 \\ . \\ 0 \end{bmatrix} \cdots + \begin{bmatrix} 0 \\ 0 \\ . \\ x_n \end{bmatrix}\Big) = \begin{bmatrix} f(\bar{e}_1) & \dots & f(\bar{e}_n) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ . \\ x_n \end{bmatrix}$$

Quindi, $f(\bar{x})$ equivale a moltiplicare il vettore $\bar{x}$ per la matrice, le quali colonne sono le immagini di f sui vettori della base canonica dello spazio di partenza. Si nota subito come tale matrice, abbia un numero di colonne pari alla dimensione dello spazio di partenza $\mathbb{R}^n$, ed un numero di righe pari alla dimensione dello spazio di arrivo $\mathbb{R}^m$.

Possiamo quindi vedere $\hom(\mathbb{R}^n, \mathbb{R}^m)$ come lo spazio delle matrici $M_{m \times n}(\mathbb{R})$. L'operazione di somma fra due applicazioni lineari, diventa la somma fra due matrici, che equivale semplicemente a sommare le due matrici componente per componente : $(A + B)_{i_j} = A_{i_j} + B_{i_j}$.

Moltiplicare una matrice A per un vettore $\bar{x}$, da come risultato un vettore $\bar{y}$, dove ogni coordinata y_j è equivalente al prodotto fra la riga A_j e $\bar{x}$.

Esempio :

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} \tag{112}$$

Dove

$$v_1 = [1 \quad 2 \quad 3] \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = 6 \quad v_2 = [4 \quad 5 \quad 6] \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = 15 \quad v_3 = [7 \quad 8 \quad 9] \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = 24 \tag{113}$$

Il risultato di tale prodotto è quindi $\begin{bmatrix} 6 \\ 15 \\ 24 \end{bmatrix}$. Conoscendo ora come si comporta un applicazione f sui generatori dello spazio di partenza, possiamo definirne la matrice associata, che verrà indicata con A_f (si ricordi che $\bar{e}_i$ sono i vettori della base canonica).

$$\hom(\mathbb{R}^n, \mathbb{R}^m) \to M_{m\times n}(\mathbb{R}) \text{ tale che } f \to \begin{bmatrix} f(\bar{e}_1) & \dots & f(\bar{e}_n) \end{bmatrix} = A_f$$

E data una matrice A posso definire la sua conseguente applicazione lineare, denotata f_A :

$$f_A\Big(\begin{bmatrix} x_1 \\ x_2 \\ . \\ x_n \end{bmatrix} \Big) = A \cdot \begin{bmatrix} x_1 \\ x_2 \\ . \\ x_n \end{bmatrix} = x_1 A^1 + x_2 A^2 \dots x_n A^n$$

In precedenza, abbiamo denotato quest'applicazione L_A.

11.3.3 Prodotto tra Matrici

In questo capitolo, prima di parlare di correlazione diretta tra matrici ed applicazioni lineari, abbiamo astratto il concetto parlando dello spazio $\hom(V, W)$, definendo delle operazioni di somma e prodotto, e dimostrandone la linearità.

Abbiamo visto come $M_{m\times n}(\mathbb{R})$ è uno spazio vettoriale del tipo $\hom(\mathbb{R}^n, \mathbb{R}^m)$, in quanto rappresenta delle applicazioni lineari. Sappiamo però, che esiste fra le applicazioni un operazione di composizione, se le matrici sono applicazioni, vuol dire che **deve esistere un operazione fra due matrici, che ne associa la matrice rappresentate l'applicazione composta**, tale operazione, è detta prodotto fra matrici.

Prima di presentare il prodotto fra matrici, proviamo a "srotolarne" la definizione, con un procedimento simile a quello adoperato per mostrare il prodotto matrice per vettore. Se la composizione fra due applicazioni è un applicazione, il prodotto fra matrici risulterà in una nuova matrice :

$$\begin{tikzcd} \mathbb{R}^n \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & \mathbb{R}^m \arrow[r, "g"] & \mathbb{R}^p \end{tikzcd}$$

La matrice risultante sarà un applicazione da $\mathbb{R}^n$ ad $\mathbb{R}^p$, avrà quindi p righe ed n colonne. Applichiamo la definizione, siano $f : \mathbb{R}^n \to \mathbb{R}^m$ e $g : \mathbb{R}^m \to \mathbb{R}^p$:

$$(g \circ f)\Big(\begin{bmatrix} x_1 \\ x_2 \\ . \\ x_n \end{bmatrix} \Big) = \begin{bmatrix} g(f(\bar{e}_1)) & \dots & g(f(\bar{e}_n)) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ . \\ x_n \end{bmatrix} =$$

Denotiamo con $\bar{u}_i$ i vettori della base canonica di $\mathbb{R}^m$, ho che :

$$g(f(\bar{e}_j)) = \begin{bmatrix} g(\bar{u}_1) & \dots & g(\bar{u}_m) \end{bmatrix} \cdot \begin{bmatrix} f(\bar{e}_j) \end{bmatrix} \text{ (prodotto matrice-vettore)}$$

Ne consegue che :

$$\implies (g \circ f)\left(\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix} \right) = \begin{bmatrix} \begin{bmatrix} g(\bar{u}_1) & \dots & g(\bar{u}_m) \end{bmatrix} \cdot \begin{bmatrix} f(\bar{e}_1) \end{bmatrix} & \dots & \begin{bmatrix} g(\bar{u}_1) & \dots & g(\bar{u}_m) \end{bmatrix} \cdot \begin{bmatrix} f(\bar{e}_n) \end{bmatrix} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix}$$

È quindi in questo modo definito il prodotto fra due matrici, che da come risultato una nuova matrice rappresentate la composizione di applicazioni.

$$\hom(\mathbb{R}^n, \mathbb{R}^m) \times \hom(\mathbb{R}^m, \mathbb{R}^p) \to \hom(\mathbb{R}^n, \mathbb{R}^p)$$

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

$$M_{m \times n}(\mathbb{R}) \times M_{p \times m}(\mathbb{R}) \to M_{p \times n}(\mathbb{R})$$

Ma come si calcola in maniera iterativa ed algoritmica il prodotto fra matrici? Siano $A \in M_{m \times n}(\mathbb{R})$ e $B \in M_{p \times m}(\mathbb{R})$, sapremo che $A \cdot B \in M_{p \times n}(\mathbb{R})$, precisamente, ogni elemento di $A \cdot B$ sarà definito nel seguente modo :

$$(A \cdot B)_{i_j} = B_i \cdot A^j$$

Ossia l'elemento alla i-esima riga e j-esima colonna di $A \cdot B$ sarà uguale al prodotto fra l'i-esima riga di B e la j-esima colonna di A.

Esempio :

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 4 \end{bmatrix} \quad (114)$$

Per le matrici, valgono le stesse proprietà viste per il caso generale, siano $A, B, C \in M_{m \times n}(\mathbb{R})$:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$
2. $A \cdot (B + C) = A \cdot B + A \cdot C$
3. $B \cdot (A + C) = B \cdot A + B \cdot C$
4. $(\lambda A) \cdot B = A \cdot (\lambda B) = \lambda(A \cdot B)$
5. $A \cdot Id = A = Id \cdot A$
6. $A \cdot 0 = 0$ dove 0 è la matrice con tutti zeri.
7. ${}^t(A \cdot B) = {}^tA + {}^tB$

La matrice identità Id, è la matrice che ha tutti 1 sulla diagonale principale, e 0 altrove : $i \neq j \implies (Id)_{i_j} = 0 \wedge i = j \implies (Id)_{i_j} = 1$.

Abbiamo parlato di elementi invertibili nell'anello degli omomorfismi lineari, affermando che essi sono gli isomorfismi, riguardo le matrici quadrate si ha il seguente.

Lemma : Una matrice quadrata $A \in M_{n\times n}(\mathbb{R})$, che identificherebbe l'anello degli endomorfismi $\text{End}(\mathbb{R}^n)$, è invertibile *se e solo se* le colonne di A sono linearmente indipendenti ($Kerf_A = \{\bar{0}\}$), ossia, le colonne di A sono un insieme di generatori per $\mathbb{R}^n$.

Ma come si calcola l'inversa di una matrice? Per il caso 2×2, essite una formula chiusa :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Verifica :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} da-bc & 0 \\ 0 & ad-bc \end{bmatrix} = \frac{ad-bc}{ad-bc}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = Id$$

11.4 Determinante di una Matrice Quadrata

Sia $M_{n\times n}(\mathbb{R})$ lo spazio vettoriale delle matrici $n \times n$ sul campo $\mathbb{R}$ (o qualsiasi altro campo), il **determinante** è un applicazione :

$$\det : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$$

Definito in tal modo, sia $A \in M_{n\times n}(\mathbb{R})$:

$$\det(A) := \sum_{p\in\mathcal{S}_n} (-1)^{\sigma(p)} \prod_{k=1}^{n} a_{k_{p(k)}} = \sum_{p\in\mathcal{S}_n} (-1)^{\sigma(p)} a_{1_{p(1)}} \cdot a_{2_{p(2)}} \cdot \dots \cdot a_{n_{p(n)}}$$

Dove $\sigma(p)$, è la funzione che associa ad ogni permutazione p, il numero di trasposizioni che compongono p, e a_{i_j} è l'elemento all'i-esima riga e j-esima colonna di A. È consigliato ripassare il capitolo sui gruppi simmetrici 8.10.

Vediamo un esempio, con le formule per calcolare il determinante di matrici 2×2 e 3×3:

Caso 2×2 : $A = \begin{bmatrix} a_{1_1} & a_{1_2} \\ a_{2_1} & a_{2_2} \end{bmatrix}$, $\mathcal{S}_2 = \{Id, (1 \quad 2)\} \implies \det(A) = a_{1_1}a_{2_2} - a_{1_2}a_{2_1}$

Caso 3×3 : $A = \begin{bmatrix} a_{1_1} & a_{1_2} & a_{1_3} \\ a_{2_1} & a_{2_2} & a_{2_3} \\ a_{3_1} & a_{3_2} & a_{3_3} \end{bmatrix}$, $\mathcal{S}_3 = \{Id, (1 \quad 2), (1 \quad 3), (2 \quad 3), (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)\}$

$$\implies \det(A) = a_{1_1}a_{2_2}a_{3_3} - a_{1_1}a_{2_3}a_{3_2} + a_{1_2}a_{2_3}a_{3_1} - a_{1_2}a_{2_1}a_{3_3} + a_{1_3}a_{2_1}a_{3_2} - a_{1_3}a_{2_2}a_{3_1}$$

Vediamo le 4 **proprietà fondamentali** che caratterizzano il determinante. Si pensi al determinante di una matrice $A \in M_{n\times n}(\mathbb{R})$, come una funzione che ha come parametri le righe di A : $\det(A) = \det(A_1, A_2 \dots, A_n)$.

1. $\exists i \neq j \in \{1, 2 \dots, n\} | A_i = A_j \implies \det(A_1, A_2 \dots, A_n) = 0$ Se una matrice ha 2 righe identiche, il suo determinante è lo zero.

2. $\det(A_1, A_2 \ldots, \lambda \cdot A_i \ldots, A_n) = \lambda \cdot \det(A_1, A_2 \ldots, A_i \ldots, A_n)\ \forall \lambda \in \mathbb{R}$.
3. $\det(A_1, A_2 \ldots, \bar{v}_1 + \bar{v}_2 \ldots, A_n) = \det(A_1, A_2 \ldots, \bar{v}_1 \ldots, A_n) + \det(A_1, A_2 \ldots, \bar{v}_2 \ldots, A_n)$ dove $\bar{v}_1, \bar{v}_2$ sono elementi di $\mathbb{R}^n$, ricordando che le righe di una matrice $n \times n$ sono elementi di $\mathbb{R}^n$.
4. $\det(Id) = 1$ il determinante della matrice identità è 1.

Da queste, seguono altre 4 ulteriori proprietà :

- (i) - $\det(A_1, A_2 \ldots, \bar{0} \ldots, A_n) = 0$ Se in A vi è una riga di tutti zeri, il suo determinate è zero.
- (ii) - $\det(A_1, A_2 \ldots, A_i \ldots, A_j \ldots, A_n) = \det(A_1, A_2 \ldots, A_i + \lambda \cdot A_j \ldots, A_j \ldots, A_n)$ questo rimanda al lemma fondamentale sulla quale si basa il metodo di Gauss 9.1.
- (iii) - $\det(A_1, A_2 \ldots, A_i \ldots, A_j \ldots, A_n) = (-1) \cdot \det(A_1, A_2 \ldots, A_j \ldots, A_i \ldots, A_n)$
- (iv) - Se A è una matrice, ed S è una matrice triangolare ottenuta riducendo A con il metodo di Gauss, dalle (ii) e (iii) ne segue che $\det(A) = (-1)^k \det(S)$, dove k è il numero di scambi di righe applicati durante il metodo di Gauss.

Quest'ultima proprietà ci garantisce che per calcolare il determinante di una matrice, è possibile ridurla ad una matrice triangolare, e calcolarne il determinante, che vedremo essere molto meno laborioso.

11.4.1 Calcolo del Determinante

Teorema (unicità del determinante) : Sia $\tilde{\det} : M_{n \times n}(\mathbb{R}) \to \mathbb{R}$ una funzione che gode delle proprietà 1,2,3 e 4 prima elencate, allora $\tilde{\det} = \det$. La funzione determinante è unica.

Vogliamo adesso introdurre un metodo volto al calcolo del determinante, ma prima è necessaria la seguente informazione.

Definizione : Sia A una matrice $n \times n$, e sia a_{i_j} l'elemento all'i-esima riga e j-esima colonna di A, definiamo il *complemento algebrico* di a_{i_j}, e denotiamo $A_{(i,j)}$, la matrice $(n-1) \times (n-1)$ ottenuta rimuovendo da A la i-esima riga e la j-esima colonna, ad esempio :

$$A = \begin{bmatrix} 1 & 3 & 1 \\ 4 & 7 & 2 \\ 2 & 9 & 0 \end{bmatrix} \qquad A_{(2,2)} = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}$$

Teorema (Sviluppo di Laplace) : Sia $A \in M_{n \times n}(\mathbb{R})$ e $i \in \{1, 2 \ldots, n\}$, si ha che :

$$\det(A) = \sum_{k=1}^{n} (-1)^{i+k} \cdot a_{i_k} \cdot \det(A_{(i,k)})$$

Scritto in forma estesa :

$$\det(A) = (-1)^{i+1} \cdot a_{i_1} \cdot \det(A_{(i,1)}) + (-1)^{i+2} \cdot a_{i_2} \cdot \det(A_{(i,2)}) \cdots + (-1)^{i+n} \cdot a_{i_n} \cdot \det(A_{(i,n)})$$

Questo teorema risulta estremamente efficiente in quanto i può essere un qualsiasi numero da 1 ad n, ciò significa che si può sviluppare la formula a partire da qualsiasi riga della matrice, ma il risultato sarà sempre lo stesso. Tale sviluppo, si può applicare anche ad una qualsiasi colonna, de facto, sia $l \in \{1, 2 \ldots, n\}$, si ha che :

$$\det(A) = \sum_{k=1}^{n} (-1)^{l+k} \cdot a_{k_l} \cdot \det(A_{(k,l)})$$

Può risultare poco chiaro, per questo vediamo un *esempio* di applicazione :

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 3 \\ 2 & 1 & 1 & 4 \\ 0 & 2 & 3 & -1 \end{bmatrix} \tag{115}$$

Decido di selezionare la prima riga per lo sviluppo, avrò quindi $i = 1$:

$$\det(A) = (-1)^{1+1} \cdot 0 \cdot \det\left(\begin{bmatrix} 0 & -1 & 3 \\ 1 & 1 & 4 \\ 2 & 3 & -1 \end{bmatrix} \right) + (-1)^{1+2} \cdot 1 \cdot \det\left(\begin{bmatrix} 0 & -1 & 3 \\ 2 & 1 & 4 \\ 0 & 3 & -1 \end{bmatrix} \right) +$$
$$(-1)^{1+3} \cdot 0 \cdot \det\left(\begin{bmatrix} 0 & 0 & 3 \\ 2 & 1 & 4 \\ 0 & 2 & -1 \end{bmatrix} \right) + (-1)^{1+4} \cdot 0 \cdot \det\left(\begin{bmatrix} 0 & 0 & -1 \\ 2 & 1 & 1 \\ 0 & 2 & 3 \end{bmatrix} \right)$$

Attenzione, avrò per lo sviluppo 4 termini, ognuno di essi, avrà moltiplicato un elemento sulla i-esima riga, che in questo caso è zero, ciò suggerisce, che conviene selezionare una riga (o eventualmente una colonna) che contenga il maggior numero di zeri, in modo da annullare più termini possibili, di fatti si noti come nell'equazione appena scritta, rimane un solo termine :

$$\det(A) = (-1)^3 \cdot 1 \cdot \det\left(\begin{bmatrix} 0 & -1 & 3 \\ 2 & 1 & 4 \\ 0 & 3 & -1 \end{bmatrix} \right) \tag{116}$$

A questo punto, per calcolare il determinante della matrice 3×3 rimasta, è possibile applicare nuovamente lo sviluppo (selezionando la colonna 1, in quanto con maggior numero di zeri), oppure applicando la formula esplicita del determinante per una matrice 3×3 vista ad inizio capitolo 11.4.

Nonostante lo sviluppo di Laplace sia un metodo chiaro, risulta essere molto laborioso, in quanto si devono sviluppare più equazioni, e per matrici molto grandi, risulta richiedere troppo tempo. Qui entra in gioco un importante nozione.

Proposizione (fondamentale) : Sia S una *matrice triangolare* superiore $n \times n$, e α_{i_j} l'elemento all'i-esima riga e j-esima colonna di S, si ha che :

$$\det(S) = \prod_{k=1}^{n} \alpha_{k_k}$$

Ossia, il determinante di una matrice triangolare superiore, non è altro che il prodotto di tutti gli elementi sulla diagonale principale. Ciò, fornisce un perfetto metodo di calcolo per il determinante, ricordando la proprietà (iv) vista in precedenza, che annuncia che $\det(A) = (-1)^k \det(S)$, si ha il seguente procedimento :

Si vuole calcolare il determinante di $A \in M_{n \times n}(\mathbb{R})$:

1. Si applica il metodo di Gauss ad A, tenendo in conto il numero di scambi di righe che si fanno, che denominiamo k, ottenendo quindi una matrice S triangolare equivalente alla matrice A.

2. Sia $d = p_1 \cdot p_2 \dots p_n$ il prodotto degli elementi sulla diagonale principale di S.

3. Si ha che $\det(A) = (-1)^k \cdot d$.

Corollario : Sia A una matrice quadrata $n \times n$, essa è *non singolare* (ossia vale che $\text{rg}(A) = n$) se e soltanto se $\det(A) \neq 0$, in particolare, ne segue che $KerA \neq \{\bar{0}\}$ se e soltanto se $\det(A) = 0$, ricordando il teorema della dimensione, si ha che $\dim(KerA) > 0 \iff \text{rg}(A) < n$, ne consegue che :

$$A \textit{ è invertibile se e solo se } \det(A) \neq 0.$$

Teorema di Binet : Siano $A, B \in M_{n\times n}(\mathbb{R})$, si ha che :

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Per dimostrarlo, è necessario dimostrare che l'applicazione $\tilde{d}(A) = \dfrac{\det(A \cdot B)}{\det(B)}$ gode delle proprietà del determinante.

11.5 Matrice Associata ad un'Applicazione Lineare

Consideriamo dua spazi vettoriali V e W, con $\dim(V) = n$ e $\dim(W) = m$, e sia $T : V \to W$ un applicazione lineare. Fissiamo :

$$\mathcal{B} = \{\bar{b}_1, \bar{b}_2 \dots, \bar{b}_n\} \quad \mathcal{E} = \{\bar{\varepsilon}_1, \bar{\varepsilon}_2 \dots, \bar{\varepsilon}_m\}$$

Dove $\mathcal{B}$ costituisce una base per V e $\mathcal{E}$ costituisce una base per W. Sorge spontaneo il seguente quesito : Se $\bar{v} \in V$ ha coordinate $\bar{x}$ nella base $\mathcal{B}$, allora, $T(\bar{v})$ che coordinate ha nella base $\mathcal{E}$? Definiamo una matrice associata a T con questa scelta di basi, denotata con $M_{\mathcal{E},\mathcal{B}}(T)$, che sarà la diretta risposta al quesito posto.

Siano $\bar{x}$ le coordinate di $\bar{v}$ in $\mathcal{B}$, ne consegue che :

$$\bar{v} = x_1\bar{b}_1 + x_2\bar{b}_2 \dots + x_n\bar{b}_n$$

Consideriamo $T(\bar{v})$, che ha coordinate $\bar{y}$ in $\mathcal{E}$, si avrà che :

$$T(\bar{v}) = T(x_1\bar{b}_1 + x_2\bar{b}_2 \dots + x_n\bar{b}_n) = \textbf{ per linearità } = x_1T(\bar{b}_1) + x_2T(\bar{b}_2) \dots + x_nT(\bar{b}_n)$$

Sappiamo che $T(\bar{b}_i)$ è un elemento di W, sarà quindi $T(\bar{b}_i) = a_{1_i}\bar{\varepsilon}_1 + a_{2_i}\bar{\varepsilon}_2 \dots + a_{m_i}\bar{\varepsilon}_m$, ne segue :

$$T(\bar{v}) = x_1(a_{1_1}\bar{\varepsilon}_1 + a_{2_1}\bar{\varepsilon}_2 \dots + a_{m_1}\bar{\varepsilon}_m) + x_1(a_{1_2}\bar{\varepsilon}_1 + a_{2_2}\bar{\varepsilon}_2 \dots + a_{m_2}\bar{\varepsilon}_m) \dots + x_n(a_{1_n}\bar{\varepsilon}_1 + a_{2_n}\bar{\varepsilon}_2 \dots + a_{m_n}\bar{\varepsilon}_m)$$

$$= (a_{1_1}x_1 + \dots a_{1_n}x_n)\bar{\varepsilon}_1 + \dots + (a_{m_1}x_1 + \dots a_{m_n}x_n)\bar{\varepsilon}_m = y_1\bar{\varepsilon}_1 + \dots + y_m\bar{\varepsilon}_m = T(\bar{v})$$

Ma da questo, risulta chiaro che :

$$\bar{y} = \begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ y_m \end{bmatrix} = \begin{bmatrix} a_{1_1}x_1 + \dots + a_{1_n}x_n \\ a_{2_1}x_1 + \dots + a_{2_n}x_n \\ \cdot \\ a_{m_1}x_1 + \dots + a_{m_n}x_n \end{bmatrix}$$

Quest'ultimo elemento è proprio il prodotto di una matrice per il vettore delle coordinate di $\bar{v}$ in $\mathcal{B}$, questa matrice ha le seguenti componenti :

$$M_{\mathcal{E},\mathcal{B}}(T) = \begin{bmatrix} a_{1_1} & a_{1_2} & \dots & a_{1_n} \\ a_{2_1} & a_{2_2} & \dots & a_{2_n} \\ . & . & & . \\ . & . & & . \\ a_{m_1} & a_{m_2} & \dots & a_{m_n} \end{bmatrix}$$

Ricordando che gli elementi a_{i_j} sono le coordinate degli elementi immagine della base $\mathcal{B}$ di V. Abbiamo denotato tale matrice $M_{\mathcal{E},\mathcal{B}}(T)$, e vale la seguente proposizione.

Proposizione : Siano $\bar{x}$ le coordinate di $\bar{v}$ in $\mathcal{B}$, allora le coordinate di $T(\bar{v})$ in $\mathcal{E}$ sono il prodotto matrice per vettore $\bar{x} \cdot M_{\mathcal{E},\mathcal{B}}(T)$.

Proposizione : Siano V, W, U 3 spazi vettoriali, con rispettive basi $\mathcal{B}, \mathcal{E}, \mathcal{F}$, consideriamo le due applicazioni $T : V \to W$ e $S : W \to U$, considero l'applicazione composta $S \circ T : V \to U$, ho che la matrice associata a tale applicazione, è il prodotto fra le matrici associate alle due applicazioni T ed S.

$$M_{\mathcal{F},\mathcal{B}}(S \circ T) = M_{\mathcal{F},\mathcal{E}}(S) \cdot M_{\mathcal{E},\mathcal{B}}(T)$$

Dimostrazione : Sia $\bar{x}$ il vettore delle cordinate in V associato alla base $\mathcal{B}$, ed $\bar{y}$ il vettore delle cordinate in W associato alla base $\mathcal{E}$, so che $\bar{y} = M_{\mathcal{E},\mathcal{B}}(T) \cdot \bar{x}$. Sia $\bar{z}$ il vettore delle cordinate in U associato alla base $\mathcal{F}$, ho che $\bar{z} = M_{\mathcal{F},\mathcal{E}}(S) \cdot \bar{y}$. So che $\bar{z} = M_{\mathcal{F},\mathcal{B}}(S \circ T) \cdot \bar{x}$ ma $\bar{z} = M_{\mathcal{F},\mathcal{E}}(S) \cdot M_{\mathcal{E},\mathcal{B}}(T) \cdot \bar{x}$. ■

11.5.1 Cambiamento di Base

Considero adesso un *isomorfismo* $\varphi : V \to W$, sappiamo che esiste l'applicazione inversa $\varphi^{-1} : W \to V$ e che $\varphi \circ \varphi^{-1} = Id_W$ e $\varphi^{-1} \circ \varphi = Id_V$. Considero $\mathcal{B}$ la base di V e $\mathcal{E}$ la base di W. Ho la matrice associata all'identità in V : $M_{\mathcal{B},\mathcal{B}}(Id_V)$ che è per l'appunto identica ad $M_{\mathcal{B},\mathcal{B}}(\varphi^{-1} \circ \varphi)$, a questo punto applico la proposizione appena vista :

$$M_{\mathcal{B},\mathcal{B}}(\varphi^{-1} \circ \varphi) = M_{\mathcal{B},\mathcal{E}}(\varphi^{-1}) \cdot M_{\mathcal{E},\mathcal{B}}(\varphi)$$

Sappiamo che la matrice identità è della seguente forma :

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

Ossia, ha la diagonale principale composta da tutti 1, ed il resto composto da tutti zeri. L'applicazione identità Id_V è definita da V in V, supponiamo, di considerare appunto tale applicazione, ma considerando due basi diverse per lo stesso spazio V. Voglio quindi definire la matrice associata all'applicazione identità, considerando come base di partenza $\mathcal{B}$ e come base di arrivo $\mathcal{B}'$, ossia $M_{\mathcal{B}',\mathcal{B}}(Id_V)$, l'applicazione identità, è un isomorfismo ed è *invertibile*, esiste quindi una matrice inversa, che è appunto sempre la matrice identità :

$$(M_{\mathcal{B}',\mathcal{B}}(Id_V))^{-1} = M_{\mathcal{B},\mathcal{B}'}(Id_V)$$

Quindi, sia $\bar{x}$ il vettore delle coordinate in V associato alla base $\mathcal{B}$ e $\bar{x}'$ il vettore delle coordinate in V associato alla base $\mathcal{B}'$, si ha che :

$$\bar{x}' = M_{\mathcal{B}',\mathcal{B}}(Id_V) \cdot \bar{x} \qquad\qquad \bar{x} = M_{\mathcal{B},\mathcal{B}'}(Id_V) \cdot \bar{x}'$$

Tali matrici sono dette del **cambiamento di base**, e fornisce informazioni sulla correlazione fra le coordinate. Ricordando che $M_{\mathcal{B}',\mathcal{B}}(Id_V)$ è la matrice che ha come j-esima colonna le coordinate $Id_V(\bar{b}_j) = \bar{b}_j$, dove $\bar{b}_j \in \mathcal{B}$.

Definizione : Due matrici A e A' si dicono **simili** se esiste una matrice C invertibile tale che $A' = C^{-1} \cdot A \cdot C$.

Proposizione : Consideriamo adesso un *endomorfismo* $T : V \to V$, fisso due basi per V, ossia $\mathcal{B}$ e $\mathcal{B}'$, e considero due matrici associate : $M_{\mathcal{B},\mathcal{B}}(T)$ e $M_{\mathcal{B}',\mathcal{B}'}(T)$. Si ha che :

$$M_{\mathcal{B}',\mathcal{B}'}(T) = M_{\mathcal{B}',\mathcal{B}'}(Id_V \circ T \circ Id_V) = \text{ applico la proposizione precedente}$$

$$= M_{\mathcal{B}',\mathcal{B}}(Id_V) \cdot M_{\mathcal{B},\mathcal{B}}(T) \cdot M_{\mathcal{B},\mathcal{B}'}(Id_V)$$

Ma ho visto prima che $M_{\mathcal{B}',\mathcal{B}}(Id_V) = (M_{\mathcal{B},\mathcal{B}'}(Id_V))^{-1}$

$$\implies M_{\mathcal{B}',\mathcal{B}'}(T) = (M_{\mathcal{B},\mathcal{B}'}(Id_V))^{-1} \cdot M_{\mathcal{B},\mathcal{B}}(T) \cdot M_{\mathcal{B},\mathcal{B}'}(Id_V)$$

Quindi $M_{\mathcal{B}',\mathcal{B}'}(T)$ e $M_{\mathcal{B},\mathcal{B}}(T)$ sono due matrici *simili*.

12 Autovalori, Autovettori e Diagonalizzabilità

Sia V uno spazio vettoriale sul campo $\mathbb{K}$, e sia $T : V \to V$ un applicazione lineare, diremo che $\bar{v} \neq \bar{0}$ è un **autovettore** *associato* all'**autovalore** $\lambda \in \mathbb{K}$ se :

$$T(\bar{v}) = \lambda \cdot \bar{v}$$

Ossia, se T trasforma $\bar{v}$ in un suo multiplo. Se $\bar{v}$ è un autovettore, anche $\alpha \cdot \bar{v}$ lo è, con α un qualsiasi elemento del campo $\mathbb{K}$. Ciò è di facile verifica : $T(\alpha\bar{v}) = \alpha T(\bar{v}) = \alpha\lambda\bar{v} = \lambda \cdot (\alpha\bar{v})$.

L'**autospazio** associato a $\lambda \in \mathbb{K}$, è l'insieme degli autovettori che hanno λ come autovalore, ossia :

$$V_\lambda = \{\bar{0}\} \cup \{\text{autovettori associati a } \lambda\} = \{\bar{v} \in V | T(\bar{v}) = \lambda\bar{v}\} = \{\bar{v} \in V | T(\bar{v}) - \lambda\bar{v} = \bar{0}\}$$

Consideriamo l'applicazione $T - \lambda Id_V$ e si noti come :

$$V_\lambda = \{\bar{v} \in V | (T - \lambda Id_V)(\bar{v}) = \bar{0}\} = Ker(T - \lambda Id_V)$$

Ne concludiamo che l'autospazio associato ad un autovalore è un nucleo di un applicazione, è quindi un *sottospazio*.

12.1 Diagonalizzabilità di un Applicazione

Consideriamo sempre lo spazio vettoriale V sul campo $\mathbb{K}$, sia $\mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_n\}$ la base di V, e supponiamo che tutti i vettori della base siano *autovettori.* Ossia che :

$$T(\bar{v}_1) = \lambda_1 \bar{v}_1 \tag{117}$$
$$T(\bar{v}_2) = \lambda_2 \bar{v}_2 \tag{118}$$
$$\vdots \tag{119}$$
$$T(\bar{v}_n) = \lambda_n \bar{v}_n \tag{120}$$

Gli autovalori associati agli autovettori della base sono quindi $\lambda_1, \lambda_2 \ldots, \lambda_n$. Considero adesso la matrice associata a T nella base $\mathcal{B}$, ossia $M_{\mathcal{B},\mathcal{B}}(T)$, si ricordi che tale matrice, ha come j-esima colonna le coordinate di $\bar{v}_j$ in $\mathcal{B}$. Tali coordinate sono :

$$T(\bar{v}_1) = \lambda_1 \bar{v}_1 + 0 \cdot \bar{v}_2 \cdots + 0 \cdot \bar{v}_n \tag{121}$$
$$T(\bar{v}_2) = 0 \cdot \bar{v}_1 + \lambda_2 \bar{v}_2 \cdots + 0 \cdot \bar{v}_n \tag{122}$$
$$\vdots \tag{123}$$
$$T(\bar{v}_n) = 0 \cdot \bar{v}_1 + 0 \cdot \bar{v}_2 \cdots + \lambda_n \bar{v}_n \tag{124}$$

Risulta chiaro che :

$$M_{\mathcal{B},\mathcal{B}}(T) = \begin{bmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{bmatrix}$$

Tale matrice è detta *diagonale*, un applicazione T è quindi detta **diagonalizzabile** se ammette una matrice associata diagonale, ossia se ammette una base costituita da autovettori. Ci interessa capire se un applicazione è diagonalizzabile, dato che la matrice associata diagonale è particolarmente semplice da studiare. È chiaro che non tutte le applicazioni sono diagonalizzabili, ne vedremo in seguito un esempio.

12.1.1 Polinomio Caratteristico

Vogliamo adesso capire se un certo numero dato è o non è un autovalore. Sappiamo che λ è un autovalore se e solo se esiste un autovettore associato, quindi se l'autospazio $V_\lambda \neq \{\bar{0}\}$, ciò è equivalente a dire che il nucleo $Ker(T - \lambda Id_V) \neq \{\bar{0}\}$. Data una base $\mathcal{B} = \{\bar{b}_1, \bar{b}_2 \ldots, \bar{b}_n\}$, so che l'applicazione $T - \lambda Id_V$ ha una matrice associata $M_{\mathcal{B},\mathcal{B}}(T)$ che per semplicità denomineremo A. Quindi T è diagonalizzabile se $Ker(A - \lambda I_n) \neq \{\bar{0}\}$, dove I_n è la matrice identità $n \times n$, che sarebbe la matrice associata all'applicazione Id_V. In conclusione :

$$Ker(A - \lambda I_n) \neq \{\bar{0}\} \iff \det(A - \lambda I_n) = 0$$

Per capire se λ è un autovalore, bisogna ricavarsi quindi $\det(A - \lambda I_n)$, denotato $P_T(\lambda)$ e detto **polinomio caratteristico**, se λ è una radice di tale polinomio e soddisfa l'identità $P_T(\lambda) = 0$, allora è un autovalore.

Proposizione : Il polinomio caratteristico dipende esclusivamente da un applicazione $T : V \to V$ e non dalla scelta della base per V.

Dimostrazione : Sia $T : V \to V$ un applicazione, $\mathcal{B}$ la base di V e $P_T(\lambda) = \det(A - \lambda I_n)$ il polinomio caratteristico. Consideriamo ora un altra base di V, ossia $\mathcal{B}'$, e sia $A' = M_{\mathcal{B}',\mathcal{B}'}(T)$ la matrice associata a T con tale base. Considero quindi il polinomio caratteristico $\det(A' - \lambda I_n)$. So che A ed A', essendo matrici associate alla stessa applicazione ma con diversa scelta di basi, sono *simili*, quindi $\exists C | A' = C^{-1}AC$, e tale C è la matrice del cambiamento di base. Ne consegue che :

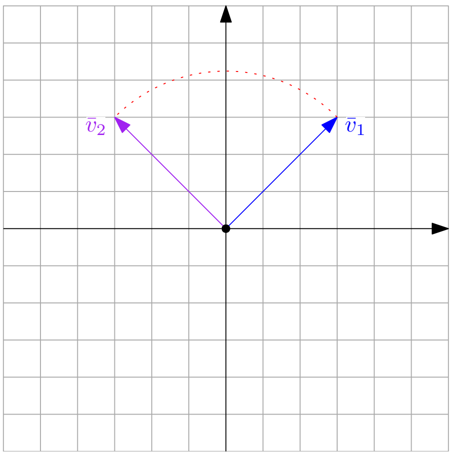
$$\det(A' - \lambda I_n) = \det(C^{-1}AC - \lambda I_n) = \det(C^{-1}(A - \lambda I_n)C)$$

Per il teorema di Binet so che :

$$\det(C^{-1}(A - \lambda I_n)C) = \det(C^{-1}) \cdot \det(A - \lambda I_n) \cdot \det(C) =$$

$$\frac{1}{\det(C)} \cdot \det(A - \lambda I_n) \cdot \det(C) = \det(A - \lambda I_n) \qquad \blacksquare$$

Vediamo un *esempio* di applicazione non diagonalizzabile, si consideri $R_{\pi/2} : \mathbb{R}^2 \to \mathbb{R}^2$, ossia l'applicazione che associa ad un punto sul piano cartesiano, il suo corrispettivo ruotato di 90°.



$$R_{\pi/2}(\bar{v}_1) = \bar{v}_2$$

Considero come base i vettori della base canonica, ossia $\mathcal{B} = \{\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}\}$, Ho che

$$\begin{cases} R_{\pi/2}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ \\ R_{\pi/2}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} -1 \\ 0 \end{bmatrix} = -1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{cases} \implies M_{\mathcal{B},\mathcal{B}}(R_{\pi/2}) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Calcolo il polinomio caratteristico :

$$P_{R_{\pi/2}}(\lambda) = \det(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) = \det(\begin{bmatrix} -\lambda & 1 \\ 1 & -\lambda \end{bmatrix}) = \lambda^2 + 1$$

$R_{\pi/2}$ non è diagonalizzabile perché non esistono autovalori, in quanto non esiste nessun $\lambda \in \mathbb{R}$ tale che $\lambda^2 + 1 = 0$. Questa, è anche una chiara dimostrazione di come l'esistenza degli autovalori, dipenda dal campo sulla quale è basato lo spazio vettoriale, infatti, $\lambda^2 + 1 = 0$ non ammette soluzioni in $\mathbb{R}$, ma ammette soluzioni in $\mathbb{C}$.

12.1.2 Molteplicità e Criterio di Diagonalizzabilità

È necessario introdurre 2 concetti fondamentali :

Definizione : Sia $P(\lambda)$ un polinomio caratteristico e λ_0 un'autovalore radice di tale polinomio. Esiste $h \geq 1 \in \mathbb{N}$ tale che $P(\lambda) = (\lambda - \lambda_0)^h \cdot f(\lambda)$, dove f è una funzione tale che $f(\lambda_0) \neq 0$. Tale numero naturale h è detto *molteplicità algebrica* di λ_0, ed è denotato $\text{molt}(\lambda_0)$. Differentemente, $\dim(Ker(T - \lambda_0 Id_V))$ è detta *molteplicità geometrica* di λ_0.

Teorema (Criterio) : Sia V uno spazio vettoriale sul campo $\mathbb{K}$, sia $T : V \to V$ un applicazione lineare, e siano $\lambda_1, \lambda_2 \ldots, \lambda_k$ gli autovalori distinti per T, le seguenti sono equivalenti :

1. T è diagonalizzabile.
2. $\forall j \in \{1, 2 \ldots, k\}$, si ha che $\text{molt}(\lambda_j) = \dim(V_{\lambda_j})$, ricordando che la dimensione dell'autospazio associato a λ_j, è detta la sua molteplicità geometrica.
3. $\displaystyle\sum_{j=1}^{k} \dim(V_{\lambda_j}) = \dim(V)$

Dimostrazione : $\boxed{\texttt{(1)} \implies \texttt{(2)}}$: Sappiamo che T è diagonalizzabile se esiste una base $\mathcal{B}$ di V composta da autovettori di T, ne consegue che la matrice associata a T con tale base, ossia $M_{\mathcal{B},\mathcal{B}}(T)$, è una matrice diagonale, con appunto, gli autovalori sulla diagonale, ed ha il polinomio caratteristico della forma $(\lambda_1 - \lambda)^{\text{molt}(\lambda_1)} + (\lambda_2 - \lambda)^{\text{molt}(\lambda_2)} \cdots + (\lambda_k - \lambda)^{\text{molt}(\lambda_k)}$, si ha che il numero di ingressi sulla diagonale per cui $\lambda_j = \text{molt}(\lambda_j)$, equivale a $\dim(Ker(M_{\mathcal{B},\mathcal{B}}(T)))$. $\boxed{\texttt{(2)} \implies \texttt{(3)}}$: Si ha che il polinomio caratteristico ha grado $\dim(V) = \text{molt}(\lambda_1) + \text{molt}(\lambda_2) \cdots + \text{molt}(\lambda_k)$, dato che per ipotesi $\forall j \in \{1, 2 \ldots, k\}$, si ha che $\text{molt}(\lambda_j) = \dim(V_{\lambda_j})$, ne consegue che la somma delle moltiplicità geometriche è uguale alla dimensione di V. $\boxed{\texttt{(3)} \implies \texttt{(1)}}$: Si ha che gli autospazi associati ad autovalori distinti sono in somma diretta (proposizione che vedremo in seguito), ne segue che $\dim(V) = \dim(V_{\lambda_1}) + \dim(V_{\lambda_2}) \cdots + \dim(V_{\lambda_k})$, sia allora $\mathcal{B}_j$ una base per V_{λ_j}, si ha che i vettori delle base dei diversi autospazi sono tutti linearmente indipendenti fra loro, e sono in numero uguale alla dimensione di V, si ha quindi che $V = \text{Span}(\mathcal{B}_1 \cup \mathcal{B}_2 \cdots \cup \mathcal{B}_k)$, ne segue che V ammette una base di autovettori di T, quindi T è diagonalizzabile. $\blacksquare$

Lemma : Sia V uno spazio vettoriale di dimensione n sul campo $\mathbb{K}$ e sia $\varphi : V \to V$ un endomorfismo lineare. Supponiamo che $\lambda_1, \lambda_2 \ldots, \lambda_k$ siano gli autovalori di φ, si ha che i relativi autospazi $V_{\lambda_1}, V_{\lambda_2} \ldots, V_{\lambda_k}$ sono in posizione di *somma diretta*, e che gli autovettori che costituiscono le basi dei diversi autospazi sono tutti linearmente indipendenti fra loro.

Dimostrazione : Si procede per induzione su k numero di autovettori.
Caso base ($k = 1$) - Un solo vettore non nullo è ovviamente linearmente indipendente.
Ipotesi induttiva - Supponiamo sia vero per $k - 1$ vettori.
Passo induttivo - Consideriamo $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k$ autovettori associati ad autovalori distinti, consideriamo una combinazione lineare uguale al vettore nullo :

$$\alpha_1 \bar{v}_1 + \alpha_2 \bar{v}_2 \cdots + \alpha_k \bar{v}_k = \bar{0}$$

Ne segue che :

$$\alpha_k \bar{v}_k = -(\alpha_1 \bar{v}_1 + \alpha_2 \bar{v}_2 \cdots + \alpha_{k-1} \bar{v}_{k-1})$$

Essendo φ lineare, sappiamo che mappa il vettore nullo nel vettore nullo, quindi :

$$\varphi(\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \cdots + \alpha_k\bar{v}_k) = \bar{0} \implies \alpha_1\varphi(\bar{v}_1) + \alpha_2\varphi(\bar{v}_2) \cdots + \alpha_k\varphi(\bar{v}_k) = \bar{0}$$

Ma, essendo $\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_k$ autovettori si ha che :

$$\alpha_1\lambda_1\bar{v}_1 + \alpha_2\varphi\lambda_2\bar{v}_2 \cdots + \alpha_k\lambda_k\bar{v}_k = \bar{0}$$

Ricordando che $\alpha_k\bar{v}_k = -(\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \cdots + \alpha_{k-1}\bar{v}_{k-1})$, riscrivo :

$$\alpha_1\lambda_1\bar{v}_1 + \alpha_2\varphi\lambda_2\bar{v}_2 \cdots + \lambda_k(-\alpha_1\bar{v}_1 - \alpha_2\bar{v}_2 \cdots - \alpha_{k-1}\bar{v}_{k-1}) = \bar{0}$$

Riorganizzo i termini nel seguente modo :

$$\alpha_1(\lambda_1 - \lambda_k)\bar{v}_1 + \alpha_1(\lambda_2 - \lambda_k)\bar{v}_2 \cdots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k)\bar{v}_{k-1} = \bar{0}$$

A questo punto però, si applica l'ipotesi induttiva, sappiamo già che i $k-1$ autovettori sono linearmente indipendenti, quindi i coefficenti $\alpha_1, \alpha_2 \ldots, \alpha - k - 1$ sono nulli, inoltre sappiamo che, $\forall j \in \{1, 2 \ldots, k\}$ si ha che $(\lambda_j - \lambda_k) \neq 0$ in quanto questi sono autovalori. Ne consegue che la combinazione lineare iniziale $\alpha_1\bar{v}_1 + \alpha_2\bar{v}_2 \cdots + \alpha_k\bar{v}_k$ è uguale al vettore nullo se tutti i coefficienti sono nulli, quindi i k autovettori sono linearmente indipendenti. ■

Teorema Spettrale : Se A è una matrice simmetrica, ossia $A = {}^tA$, allora l'applicazione associata L_A è diagonalizzabile.

Lemma : Sia V uno spazio vettoriale di dimensione n sul campo $\mathbb{K}$ e sia $\varphi : V \to V$ un endomorfismo lineare, se φ ha n autovalori distinti, allora è diagonalizzabile.

Proposizione : Sia λ un autovalore, si ha che :

$$\text{molteplicità algebrica di } \lambda \geq \text{ molteplicità geometrica di } \lambda$$

Dimostrazione : Sia λ_0 un autovalore dell'endomorfismo T di uno spazio vettoriale V sul campo $\mathbb{K}$, siano $\mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_h\}$ una base per l'autospazio V_{λ_0} associato a λ_0. Sia F un completamento di V_{λ_0}, e sia $\mathcal{D} = \{\bar{v}_{h+1}, \bar{v}_{h+2} \ldots, \bar{v}_n\}$ una base per F. Consideriamo quindi la base per V, data da $\mathcal{E} = \mathcal{D} \cup \mathcal{B} = \{\bar{v}_1, \bar{v}_2 \ldots, \bar{v}_h + \bar{v}_{h+1}, \bar{v}_{h+2} \ldots, \bar{v}_n\}$, e consideriamo la matrice associata a T nella base $\mathcal{E}$, essa sarà divisa in 4 quadranti ed avrà la seguente forma :

$$M_{\mathcal{E},\mathcal{E}}(T) = \begin{bmatrix} \lambda_0 \cdot Id & | & X \\ --- & --- & --- \\ 0 & | & Y \end{bmatrix}$$

Dove X ed Y sono due matrici. Il polinomio caratteristico di tale applicazione su questa base sarà dato da

$$P_{\lambda_0}(T) = \det(M_{\mathcal{E},\mathcal{E}}(T) - \lambda_0 \cdot Id) = (\lambda_0 - \lambda)^h \cdot p(\lambda)$$

Dove $p(\lambda)$ è un altro polinomio in funzione di λ. Si noti come tale polinomio comprende il termine $(\lambda_0 - \lambda)^h$, dove h era la dimensione dell'autospazio associato a λ_0. Ne segue che la molteplicità algebrica è sempre maggiore o ugale alla molteplicità geometrica. ■

13 Complementi

Perché questa sezione? - Ci sono delle cose che durante il corso delle lezioni mi son perso, non ho voglia di aggiungerle agli appunti già scritti, potrei farlo in un futuro prossimo ma adesso non lo farò.

13.1 Sulla Teoria dei Gruppi e le Strutture Algebriche

13.1.1 Dimostrazione del Teorema di Eulero

Vogliamo dimostrare che $a^{\varphi(n)} = 1 \mod n$, prima di ciò, faccio un :
Osservazione cruciale : Se p è un numero primo che non divide a, allora :

$$a^{\varphi(p^k)} = 1 \mod p^k$$

Dimostrazione Osservazione cruciale : Procediamo per induzione su k.

- `Caso base` $k = 1$: $a^{\varphi}(p) = 1 \mod p \iff a^{p-1} = 1 \mod p$ e ciò è verificato in quanto è il caso del piccolo teorema di Fermat 4.4 .
- `Ipotesi induttiva` : $a^{\varphi(p^k)} = 1 \mod p^k$, che è equivalente a dire che $a^{\varphi(p^k)} = 1 + p^k \cdot t$ per qualche $t \in \mathbb{Z}$.
- `Passo induttivo` : Come prima cosa, mi rendo conto che :

  $$\varphi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p \cdot \varphi(p^k)$$

  Quindi :

  $$a^{\varphi(p^{k+1})} = a^{p \cdot \varphi(p^k)} = (a^{\varphi(p^k)})^p = \text{ ipotesi } = (1 + p^k \cdot t)^p$$

  Sviluppo il binomio :

  $$(1 + p^k \cdot t)^p = \sum_{i=0}^{p} \binom{p}{i} (p^k \cdot t)^i = (1 + p^k \cdot t)^p = \binom{p}{0} (p^k \cdot t)^0 + \sum_{i=1}^{p} \binom{p}{i} (p^k \cdot t)^i$$

  $$\binom{p}{0} (p^k \cdot t)^0 + \sum_{i=1}^{p} \binom{p}{i} (p^k \cdot t)^i = 1 + \sum_{i=1}^{p} \binom{p}{i} (p^k \cdot t)^i$$

  Vogliamo capire quanto fa questo risultato $\mod p^{k+1}$, osservo che $p^k \cdot t = 0 \mod p^{k+1}$, quindi :

  $$1 + \sum_{i=1}^{p} \binom{p}{i} (p^k \cdot t)^i \mod p^{k+1} \implies 1 + \sum_{i=1}^{p} \binom{p}{i} (0)^i \mod p^{k+1} = 1 + 0 = 1 \quad \blacksquare$$

Ora che ho dimostrato l'osservazione posso procedere con $a^{\varphi(n)} = 1 \mod n$, considero la fattorizzazione in primi di n, ossia $n = p_1^{h_1} \cdot p_2^{h_2} \dots p_s^{h_s}$, quindi $\varphi(n) = \varphi(p_1^{h_1} \cdot p_2^{h_2} \dots p_s^{h_s})$, ma so che φ è una funzione *moltiplicativa*, quindi $\dfrac{\varphi(n)}{\varphi(p_i^{h_i})} \in \mathbb{Z} \quad \forall i$. A questo punto, considero $a^{\varphi(p_i^{h_i})} = 1 \mod p_i^{h_i}$, per l'osservazione cruciale so che è uguale ad 1. Elevo ad entrambi i membri $\dfrac{\varphi(n)}{\varphi(p_i^{h_i})}$ ed ottengo :

$$(a^{\varphi(p_i^{h_i})})^{\frac{\varphi(n)}{\varphi(p_i^{h_i})}} = 1^{\frac{\varphi(n)}{\varphi(p_i^{h_i})}} \mod p_i^{h_i} \implies a^{\frac{\varphi(p_i^{h_i})\varphi(n)}{\varphi(p_i^{h_i})}} = 1 \mod p_i^{h_i} \implies a^{\varphi(n)} = 1 \mod p_i^{h_i}$$

Ma allora, per il teorema cinese , ho che :

$$\begin{cases} a^{\varphi(n)} = 1 \mod p_1^{h_1} \\ a^{\varphi(n)} = 1 \mod p_2^{h_2} \\ \vdots \\ a^{\varphi(n)} = 1 \mod p_s^{h_s} \end{cases} \implies a^{\varphi(n)} = 1 \mod (p_1^{h_1} \cdot p_2^{h_2} \dots p_s^{h_s}) = a^{\varphi(n)} = 1 \mod n \quad \blacksquare$$

13.1.2 Chiarimento sugli Ordini dei Gruppi

Sia G un gruppo, sia e l'elemento neutro di G e sia $g \in G$ un suo elemento. Consideriamo l'insieme $O = \{n \in \mathbb{N} | g^n = e\}$, l'**ordine** di g sarà $\min(O)$, ossia il numero naturale n più piccolo, per cui $g^n = e$. Ovviamente, non si considera lo zero. Diversamente, l'ordine di un gruppo, rappresenta la sua cardinalità. Se non esiste nessun $n \in \mathbb{N}$ per cui $g^n = e$, allora g ha ordine infinito.

- ordine di $g \in G := \min(\{n \in \mathbb{N} | g^n = e\})$
- ordine di $G := |G|$

Sia adesso G un gruppo **ciclico**, generato da g, ossia $G = \langle g \rangle$, allora si avrà che l'ordine di G, ossia la sua cardinalità, sarà identica all'ordine del generatore g. Diversamente, se un gruppo è finito ma non ciclico, la sua cardinalità non sarà correlata all'ordine di nessun elemento.

Tutti i gruppi ciclici finiti sono *isomorfi* a $\mathbb{Z}_n$

$\mathbb{Z}_n$ non ha un solo generatore, bensì, si ha che tutti gli elementi invertibili di $\mathbb{Z}_n$ sono generatori, ossia, tutti i numeri co-primi con n, ed ovviamente hanno tutti lo stesso ordine, che sarebbe la cardinalità di $\mathbb{Z}_n$.

Esempio : Si consideri il gruppo $(\mathbb{Z}_6, +)$ di elemento neutro 0, si noti come : il teorema di struttura

$$\mathbb{Z}_6 = \{[1], [2], [3], [4], [5], [6] \equiv [0]\}$$
$$\mathcal{U}(\mathbb{Z}_6) = \{[1], [5]\}$$

Si ricordi che siamo in notazione additiva! $g^k := g + g + g \cdots + g$ k-volte.

$$\langle 1 \rangle = \{1^1 = [1], 1^2 = [2], 1^3 = [3], 1^4 = [4], 1^5 = [5], 1^{\mathbf{6}} = 6 = [0]\}$$

$$\langle 5 \rangle = \{5^1 = [5], 5^2 = 10 = [4], 5^3 = 15 = [3], 5^4 = 20 = [2], 5^5 = 25 = [1], 5^{\mathbf{6}} = 30 = 6 = [0]\}$$

13.1.3 Dimostrazione del Teorema di Struttura dei Gruppi Ciclici

Ricordando che il teorema, enuncia :

1. Se G è ciclico, ogni suo sottogruppo è ciclico.
2. L'ordine di un sottogruppo di G divide l'ordine di G.
3. Se $G = \langle g \rangle$ e $o(g) = n$, allora, se k divide n, esiste un sottogruppo H di G tale che $H = \left\langle g^{\frac{n}{k}} \right\rangle$. Esiste una corrispondenza biunivoca fra i divisori di n ed i sottogruppi di G.
4. Se k divide n e h divide k, allora $\left\langle g^{\frac{n}{h}} \right\rangle$ è un sottogruppo di $\left\langle g^{\frac{n}{k}} \right\rangle$ ed anche di G.

Procediamo con la dimostrazione.

1. Sia H un sottogruppo di G, sappiamo che, se G è ciclico, esiste un isomorfismo $\varphi : G \to \mathbb{Z}$ oppure $\varphi : G \to \mathbb{Z}_n$. Si ha quindi che, $\varphi^{-1}(G) = \mathbb{Z}$, oppure $\varphi^{-1}(G) = \mathbb{Z}_n$, se H è un sottogruppo di G ed un isomorfismo mantiene le operazioni, $\varphi^{-1}(H)$ associa ad H un sottogruppo di $\mathbb{Z}$ o $\mathbb{Z}_n$. Quindi un sottogruppo di un gruppo ciclico, è isomorfo ad un sottogruppo di $\mathbb{Z}$ o $\mathbb{Z}_n$, essendo questi dei sottogruppi *ciclici*, allora anche H è ciclico.

2. Se G ha ordine n, ed è isomorfo a $\mathbb{Z}_n$, allora un suo sottogruppo H, per il punto (1), è isomorfo ad un sottogruppo di $\mathbb{Z}_n$, ossia H_d. L'ordine di H_d, che è identico all'ordine di H, divide n.

3. Sappiamo che $H \leq G$ è isomorfo a $H_d \leq \mathbb{Z}_n$, sappiamo che $d = \frac{n}{k}$, e che l'ordine di H_d è k. Ma allora $H = \langle g^d \rangle = \langle g^{\frac{n}{k}} \rangle$. Quindi, un qualsiasi sottogruppo di $\langle g \rangle$, è del tipo $\langle g^{\frac{n}{k}} \rangle$, e ne esistono in tanti quanti sono i divisori k di n.

4. $\langle g^{\frac{n}{k}} \rangle$ è un sottogruppo ciclico di ordine k di G, se esiste un h tale che h divide k, per il punto (3), esiste un sottogruppo di $\langle g^{\frac{n}{k}} \rangle$, dato da $\left\langle (g^{\frac{n}{k}})^{\frac{k}{h}} \right\rangle = \langle g^{\frac{n}{h}} \rangle$. Inoltre, si nota facilmente che h divide anche n, di fatto $\langle g^{\frac{n}{h}} \rangle$ è anche un sottogruppo di G. L'essere sottogruppi, stabilisce una relazione d'ordine parziale.

$\blacksquare$

13.1.4 Dimostrazione del Teorema Cinese del Resto

Riguardo il seguente sistema :

$$\begin{cases} x = c_1 \mod r_1 \\ x = c_2 \mod r_2 \\ \dots \\ x = c_s \mod r_s \end{cases}$$

Considero un numero $R = r_1 \cdot r_2 \dots r_s$, considero poi per ogni $k - esima$ equazione, il numero $R_k = {}^{R}/_{r_k}$, essendo che i valori $r_1, r_2 \dots, r_s$ sono co-primi fra loro, si avrà che R_k e r_k sono co-primi, ossia $MCD(R_k, r_k) = 1$.
Ricordando che le soluzioni di un equazione congruenziale $ax = b \mod n$ sono in numero $MCD(a, n)$, si avrà che l'equazione

$$R_k x = c_k \mod r_k$$

ammette un unica soluzione $\mod r_k$. Denotiamo tale soluzione $\bar{x}_k$, quindi si ha la seguente identità, per ogni equazione, $\bar{x}_k \cdot R_k = c_k \mod r_k$. Tornando al sistema quindi, abbiamo trovato una soluzione diversa per ogni equazione, ossia $\bar{x}_k \cdot R_k$. Si avrò quindi che

$$\begin{cases} x = c_1 \mod r_1 & \text{ha soluzione } \bar{x}_1 R_1 \\ x = c_2 \mod r_2 & \text{ha soluzione } \bar{x}_2 R_2 \\ \dots \\ x = c_s \mod r_s & \text{ha soluzione } \bar{x}_s R_s \end{cases}$$

Facciamo però un **osservazione cruciale**, sappiamo che $R_k = {}^{R}/_{r_k}$, ossia :

$\frac{r_1 \cdot r_2 \dots r_{k-1}, r_{k+1} \dots r_s}{r_k}$, ma ciò significa che, R_k, è multiplo di tutti gli argomenti dei moduli del sistema tranne che di r_k. Ciò significa che $R_i = 0 \mod r_k \quad \forall i \neq k$. Consideriamo quindi la seguente soluzione per il sistema $\bar{x} = \bar{x}_1 R_1 + \bar{x}_2 R_2 \dots \bar{x}_s R_s$:

$$\begin{cases} x_1 R_1 + \bar{x}_2 R_2 \dots \bar{x}_s R_s = c_1 \mod r_1 \\ x_1 R_1 + \bar{x}_2 R_2 \dots \bar{x}_s R_s = c_2 \mod r_2 \\ \dots \\ x_1 R_1 + \bar{x}_2 R_2 \dots \bar{x}_s R_s = c_k \mod r_k \\ \dots \\ x_1 R_1 + \bar{x}_2 R_2 \dots \bar{x}_s R_s = c_s \mod r_s \end{cases}$$

Ma per l'osservazione cruciale riguardo l'annullamento dei termini, ciò diventa :

$$\begin{cases} x_1 R_1 = c_1 \mod r_1 \\ \bar{x}_2 R_2 = c_2 \mod r_2 \\ \dots \\ x_k R_k = c_k \mod r_k \\ \dots \\ \bar{x}_s R_s = c_s \mod r_s \end{cases}$$

E sappiamo che queste sono soluzioni del sistema, ne deduciamo che $\bar{x} = \bar{x}_1 R_1 + \bar{x}_2 R_2 \dots \bar{x}_s R_s$ risolve il sistema, è quindi una soluzione (unica). ■