# Introduzione

1. **Boh.** Queste sono cose che ho scritto 3 anni fa per preparare l'esame di Solá Conde, non ho ricontrollato assolutamente nulla, quindi potrebbe essere pieno di errori, ma magari può servire a qualcuno(?) —Cesare

# Insiemistica di Base

1. **Insiemi ed appartenenza.** I concetti di insieme e di appartenenza sono concetti primitivi, non si definiscono. Scriveremo $x \in \mathbb{X}$ per indicare che l'elemento $x$ appartiene all'insieme $\mathbb{X}$ e $x \notin \mathbb{X}$ per indicare che $x$ non appartiene a $\mathbb{X}$.
2. **Quantificatori.** Il simbolo $\forall$ significa "per ogni", il simbolo $\exists$ significa "esiste". Per dire "esiste un unico" si usa $\exists!$. Solitamente i quantificatori vengono usati per enunciare proprietà che valgono su un insieme, ad esempio $\forall x \in \mathbb{X}$ vale $p(x)$.
3. **Definizione per elenco o per proprietà.** Un insieme $\mathbb{X}$ può essere definito per elenco, scrivendo tutti i suoi elementi, ad esempio $\mathbb{X} = \{1, 2, 3, 4, 6, 12\}$. Lo stesso insieme può essere definito per proprietà, ad esempio $\mathbb{X} = \{x : p(x)\}$ dove la proprietà $p(x)$ in questo caso è "$x$ è un intero positivo che divide 12".
4. **Sottoinsiemi.** Dato un insieme $\mathbb{X}$, un sottoinsieme di $\mathbb{X}$ è un qualunque insieme $\mathbb{Y}$ tale che $\forall y \in \mathbb{Y}$ si abbia $y \in \mathbb{X}$. Si indica scrivendo $\mathbb{Y} \subseteq \mathbb{X}$. Se $\mathbb{Y} \neq \mathbb{X}$, si può scrivere $\mathbb{Y} \subsetneq \mathbb{X}$. In particolare per ogni insieme $\mathbb{X}$ si ha $\mathbb{X} \subseteq \mathbb{X}$.
5. **Insieme vuoto.** L'insieme che non contiene nessun elemento si chiama insieme vuoto e si indica con $\emptyset$. Per ogni insieme $\mathbb{X}$ si ha che $\emptyset \subseteq \mathbb{X}$.
6. **Insieme delle parti.** Dato un insieme $\mathbb{X}$, si definisce insieme delle parti di $\mathbb{X}$, e si denota con $\mathcal{P}(\mathbb{X})$, l'insieme che contiene tutti i sottoinsiemi di $\mathbb{X}$, compresi $\emptyset$ e $\mathbb{X}$ stesso. Se $\mathbb{X}$ ha $n$ elementi, $\mathcal{P}(\mathbb{X})$ ne ha $2^n$.
7. **Operazioni tra insiemi.** Dati due insiemi $\mathbb{X}$ e $\mathbb{Y}$, si definisce unione di $\mathbb{X}$ e $\mathbb{Y}$ l'insieme $\mathbb{X} \cup \mathbb{Y}$ che contiene tutti e soli gli elementi che appartengono o a $\mathbb{X}$ o a $\mathbb{Y}$ oppure ad entrambi. Similmente si definisce intersezione di $\mathbb{X}$ e $\mathbb{Y}$ l'insieme $\mathbb{X} \cap \mathbb{Y}$ che contiene tutti e soli gli elementi che appartengono sia a $\mathbb{X}$ sia a $\mathbb{Y}$. Inoltre si definisce differenza di $\mathbb{X}$ e $\mathbb{Y}$ l'insieme $\mathbb{X} \setminus \mathbb{Y}$ che comprende tutti e soli gli elementi di $\mathbb{X}$ che non appartengono a $\mathbb{Y}$. Si ha che
$$(\mathbb{X} \setminus \mathbb{Y}) \cup (\mathbb{Y} \setminus \mathbb{X}) = (\mathbb{X} \cup \mathbb{Y}) \setminus (\mathbb{X} \cap \mathbb{Y}).$$
8. **Coppia ordinata e prodotto cartesiano.** Dati due insiemi $\mathbb{X}$ e $\mathbb{Y}$ e due elementi $x \in \mathbb{X}$ e $y \in \mathbb{Y}$, si definisce coppia ordinata l'elemento $(x, y)$, che è generalmente diverso da $(y, x)$. L'insieme di tutte le coppie ordinate di elementi di $\mathbb{X}$ e $\mathbb{Y}$ si chiama prodotto cartesiano di $\mathbb{X}$ e $\mathbb{Y}$ e si indica con $\mathbb{X} \times \mathbb{Y}$. Allo stesso modo l'insieme delle terne $(x, y, z)$ si indica con $\mathbb{X} \times \mathbb{Y} \times \mathbb{Z}$ e così via. Solitamente $\mathbb{X} \times \mathbb{X}$ si indica con $\mathbb{X}^2$, $\mathbb{X} \times \mathbb{X} \times \mathbb{X}$ si indica con $\mathbb{X}^3$ e in generale $\mathbb{X}^n$ è l'insieme delle $n$-uple ordinate di elementi di $\mathbb{X}$.
9. **Collezioni di insiemi.** Dato un insieme $\mathbb{X}$, un insieme di indici $\mathbb{I}$ e alcuni sottoinsiemi $\mathbb{Y}_i \subseteq \mathbb{X}$ (al variare di $i \in \mathbb{I}$), l'insieme $\{\mathbb{Y}_i : i \in \mathbb{I}\}$ è una collezione di sottoinsiemi di $\mathbb{X}$. Si possono definire unioni e intersezioni di collezioni di sottoinsiemi, definendo
$$\bigcup_{i \in \mathbb{I}} \mathbb{Y}_i \quad \text{e} \quad \bigcap_{i \in \mathbb{I}} \mathbb{Y}_i,$$
rispettivamente, l'insieme che contiene tutti e soli gli elementi contenuti in almeno uno degli $\mathbb{Y}_i$, e l'insieme che contiene tutti e soli gli elementi contenuti in ciascuno degli $\mathbb{Y}_i$.

# Relazioni e Funzioni

1. **Relazioni.** Dato un insieme $\mathbb{X}$, una relazione su $\mathbb{X}$ è un qualunque sottoinsieme $\mathcal{R} \subseteq \mathbb{X} \times \mathbb{X}$. Per dire che $(x, y) \in \mathcal{R}$ solitamente si scrive $x\mathcal{R}y$.
2. **Riflessività.** Una relazione si dice riflessiva se per ogni $x \in \mathbb{X}$ vale $x\mathcal{R}x$.
3. **Simmetria.** Una relazione si dice simmetrica se per ogni $x \in \mathbb{X}$ e per ogni $y \in \mathbb{X}$ vale che se $x\mathcal{R}y$ allora $y\mathcal{R}x$ (e chiaramente viceversa).
4. **Antisimmetria.** Una relazione si dice antisimmetrica se per ogni $x \in \mathbb{X}$ e per ogni $y \in \mathbb{X}$ vale che se $x\mathcal{R}y$ e $y\mathcal{R}x$ allora $x = y$. In altre parole, se $x \neq y$ può valere al massimo una tra $x\mathcal{R}y$ e $y\mathcal{R}x$ (eventualmente anche nessuna).
5. **Transitività.** Una relazione si dice transitiva se per ogni $x \in \mathbb{X}$, per ogni $y \in \mathbb{X}$ e per ogni $z \in \mathbb{X}$ se $x\mathcal{R}y$ e $y\mathcal{R}z$ si ha anche che $x\mathcal{R}z$.
6. **Relazioni di equivalenza.** Una relazione si dice di equivalenza se è riflessiva, simmetrica e transitiva. Di solito si indicano con $\sim$ al posto di $\mathcal{R}$.
7. **Relazioni d'ordine.** Una relazione si dice d'ordine se è riflessiva, antisimmetrica e transitiva. Di solito si indicano con $\leq$ al posto di $\mathcal{R}$. Se vale $x \leq y$ e $x \neq y$, si può usare la notazione $x < y$.
8. **Relazioni d'ordine totale.** Una relazione d'ordine si dice totale se per ogni $x \in \mathbb{X}$ e per ogni $y \in \mathbb{X}$ si ha che $x \leq y$ oppure $y \leq x$.
9. **Funzioni.** Una funzione (o applicazione, o mappa) $f$ da $\mathbb{X}$ a $\mathbb{Y}$, denotata con $f : \mathbb{X} \to \mathbb{Y}$, è un sottoinsieme $\mathcal{F} \subseteq \mathbb{X} \times \mathbb{Y}$ tale che per ogni $x \in \mathbb{X}$ esiste un unico $y \in \mathbb{Y}$ per cui $(x, y) \in \mathcal{F}$. Quell'unico $y$ associato al valore $x$ si denota con $y = f(x)$.
10. **Iniettività.** Una funzione $f : \mathbb{X} \to \mathbb{Y}$ si dice iniettiva se per ogni $x_1 \in \mathbb{X}$ e per ogni $x_2 \in \mathbb{X}$ si ha che $f(x_1) = f(x_2)$ implica $x_1 = x_2$ (in parole povere, ogni valore $y \in \mathbb{Y}$ viene assunto al massimo una volta).
11. **Surgettività.** Una funzione $f : \mathbb{X} \to \mathbb{Y}$ si dice surgettiva se per ogni $y \in \mathbb{Y}$ esiste $x \in \mathbb{X}$ tale che $f(x) = y$ (in parole povere, ogni valore $y \in \mathbb{Y}$ viene assunto almeno una volta).
12. **Bigettività.** Una funzione $f : \mathbb{X} \to \mathbb{Y}$ si dice bigettiva se è sia iniettiva sia bigettiva, cioè per ogni $y \in \mathbb{Y}$ esiste un unico $x \in \mathbb{X}$ tale che $f(x) = y$. Una funzione bigettiva si dice anche biunivoca oppure invertibile quest'ultimo termine deriva dal fatto che anche la $f^{-1} : \mathbb{Y} \to \mathbb{X}$ che a $f(x)$ associa $x$ è una funzione, detta funzione inversa di $f$.
13. **Insiemi infiniti.** Un insieme $\mathbb{X}$ si dice infinito se esiste $\mathbb{Y} \subsetneq \mathbb{X}$ e una bigezione tra $\mathbb{X}$ e $\mathbb{Y}$. In realtà basta che esista $f : \mathbb{Y} \to \mathbb{X}$ surgettiva oppure $f : \mathbb{X} \to \mathbb{Y}$ iniettiva.
14. **Insiemi finiti.** Un insieme $\mathbb{X}$ si dice finito se non è infinito. Intuitivamente, un insieme finito avrà un numero $n$ intero non negativo di elementi, cioè esiste una bigezione tra $\mathbb{X}$ e l'insieme $\{1, \ldots, n\}$ (che però non è ancora stato definito).
15. **Cardinalità di un insieme.** Dato un insieme $\mathbb{X}$, si definisce $\mathsf{card}(\mathbb{X}) = \infty$ se $\mathbb{X}$ è infinito, altrimenti $\mathsf{card}(\mathbb{X}) = n$ se $\mathbb{X}$ è finito e ha $n$ elementi.

# Lemma di Zorn

In tutta questa scheda, $\mathbb{X}$ sarà un insieme, $\leq$ una relazione d'ordine (non necessariamente totale) su $\mathbb{X}$ e $\mathbb{Y}$ sarà un sottoinsieme di $\mathbb{X}$.

1. **Limitatezza.** $\mathbb{Y}$ si dice limitato superiormente se esiste $m \in \mathbb{X}$ tale che $y \leq m$ per ogni $y \in \mathbb{Y}$. Similmente $\mathbb{Y}$ si dice limitato inferiormente se esiste $m \in \mathbb{X}$ tale che $m \leq y$ per ogni $y \in \mathbb{Y}$. Se $\mathbb{Y}$ è sia limitato superiormente sia inferiormente, si dice limitato.
2. **Massimi e minimi.** Un elemento $m \in \mathbb{Y}$ si dice massimo di $\mathbb{Y}$ se per ogni $y \in \mathbb{Y}$ si ha che $y \leq m$. Similmente un elemento $m \in \mathbb{Y}$ si dice minimo di $\mathbb{Y}$ se per ogni $y \in \mathbb{Y}$ si ha che $m \leq y$. Se il massimo di $\mathbb{Y}$ esiste, è unico. Infatti se $m_1$ ed $m_2$ fossero due massimi, si avrebbe $m_1 \leq m_2$ e $m_2 \leq m_1$, da cui per antisimmetria $m_1 = m_2$. Allo stesso modo anche il minimo, se esiste, è unico.
3. **Maggioranti e minoranti.** Un elemento $m \in \mathbb{X}$ si dice maggiorante di $\mathbb{Y}$ se per ogni $y \in \mathbb{Y}$ si ha che $y \leq m$. Similmente un elemento $m \in \mathbb{X}$ si dice minorante di $\mathbb{Y}$ se per ogni $y \in \mathbb{Y}$ si ha che $m \leq y$. Se un maggiorante appartiene a $\mathbb{Y}$, allora è anche il massimo di $\mathbb{Y}$, e così se un minorante appartiene a $\mathbb{Y}$, allora è anche il minimo di $\mathbb{Y}$.
4. **Elementi massimali e minimali.** Un elemento $m \in \mathbb{Y}$ si dice elemento massimale di $\mathbb{Y}$ se per ogni $y \in \mathbb{Y}$, $m \leq y$ implica $m = y$. Allo stesso modo un elemento $m \in \mathbb{Y}$ si dice minimale se per ogni $y \in \mathbb{Y}$, $y \leq m$ implica $y = m$. Se la relazione d'ordine è totale, ogni elemento massimale è un massimo ed ogni elemento minimale è un minimo. Questo però non è vero in generale, dato che un insieme può avere un numero arbitrariamente grande di elementi massimali e di elementi minimali.
5. **Catene.** Un sottoinsieme $\mathbb{Y} \subseteq \mathbb{X}$ si dice catena (rispetto alla relazione $\leq$) se è totalmente ordinato rispetto a $\leq$. Non è quindi necessario che $\mathbb{X}$ sia di per sé totalmente ordinato (in tale caso ogni sottoinsieme è una catena).
6. **Lemma di Zorn.** Sia $\mathbb{X}$ un insieme e sia $\leq$ una relazione d'ordine su $\mathbb{X}$. Se ogni catena di $\mathbb{X}$ ha un maggiorante, allora $\mathbb{X}$ ha un elemento massimale.
7. **Dimostrazione del lemma di Zorn.** Il lemma di Zorn non è banale, poiché è equivalente all'assioma della scelta, un assioma della teoria degli insiemi. Si può quindi considerare il lemma di Zorn come assioma.

# Numeri Naturali

1. **Idea intuitiva.** Intuitivamente $\mathbb{N} = \{0, 1, 2, \ldots\}$ contiene tutti i numeri naturali.
2. **Definizione.** Sia $\mathbb{X}$ un insieme infinito con una relazione d'ordine $\leq$. Supponiamo che ogni sottoinsieme non vuoto di $\mathbb{X}$ abbia un minimo, e che ogni sottoinsieme finito e non vuoto di $\mathbb{X}$ abbia un massimo. Vogliamo dimostrare che esiste un unico insieme con queste proprietà (a meno di rinominare gli elementi).
3. **Zero, successivo, precedente.** Sia $\mathbb{X}$ un qualsiasi insieme con le proprietà sopra elencate, e sia $\leq$ la sua relazione d'ordine. Esiste il minimo di $\mathbb{X}$ per la prima proprietà, che indicheremo con $0_{\mathbb{X}}$ o con $\mathsf{min}(\mathbb{X})$. Fissato un qualunque $x \in \mathbb{X}$, inoltre, esiste $\mathsf{min}(\{y \in \mathbb{X} : x < y\})$, cioè il minimo elemento più grande di $x$. Lo chiameremo successivo di $x$ e lo indicheremo con $\mathsf{s}(x)$. Inoltre per $x \neq 0_{\mathbb{X}}$ esiste anche $\max(\{y \in \mathbb{X} : y < x\})$, cioè il minimo elemento più piccolo di $x$. Per $x = 0_{\mathbb{X}}$ non esiste poiché non ci sono elementi minori di $0_{\mathbb{X}}$. Questo si chiama precedente di $x$ e sarà denotato da $\mathsf{p}(x)$.
4. **Lemma.** Per ogni $x \neq 0_{\mathbb{X}}$ si ha che $\mathsf{s}(\mathsf{p}(x)) = x$. Per ogni $x$ si ha che $\mathsf{p}(\mathsf{s}(x)) = x$.
5. **Principio di induzione.** Sia $\mathbb{X}$ un qualsiasi insieme con le proprietà sopra elencate, e sia $\leq$ la sua relazione d'ordine. Se un sottoinsieme $\mathbb{Y} \subseteq \mathbb{X}$ è tale che $0_{\mathbb{X}}$ appartiene a $\mathbb{Y}$ e se $x \in \mathbb{Y}$ allora $\mathsf{s}(x) \in \mathbb{Y}$, si ha che $\mathbb{X} = \mathbb{Y}$.
6. **Unicità.** Per mostrare che $\mathbb{X}$ è unico, mostriamo che presi comunque due insiemi $\mathbb{X}$ ed $\mathbb{Y}$ che rispettano le proprietà di definizione, esiste una funzione bigettiva $\psi : \mathbb{X} \to \mathbb{Y}$ che mantiene le proprietà di ordinamento, cioè tale che $\psi(x_1) \leq \psi(x_2)$ per ogni $x_1$ e $x_2$ in $\mathbb{X}$ tali che $x_1 \leq x_2$. Costruiamo la mappa $\psi$ imponendo che $\psi(0_{\mathbb{X}}) = 0_{\mathbb{Y}}$ e per $x \in \mathbb{X}$ si abbia che $\psi(\mathsf{s}(x)) = \mathsf{s}(\psi(x))$, dove $\mathsf{s}$ a sinistra è il successivo in $\mathbb{X}$ e $\mathsf{s}$ a destra è il successivo in $\mathbb{Y}$. Grazie al principio di induzione si ha che questa mappa è ben definita e bigettiva e conserva l'ordine.
7. **Naturali.** D'ora in poi chiameremo $\mathbb{N}$ l'insieme (unico) che soddisfa le proprietà sopra elencate, e sarà $0 = 0_{\mathbb{N}}$, $1 = \mathsf{s}(0)$, $2 = \mathsf{s}(1)$, ...
8. **Somma.** Possiamo definire la somma tra due naturali $a+b$ per induzione su $b$, definendo quindi $a + 0 = a$ per ogni $a \in \mathbb{N}$, e $a + \mathsf{s}(b) = \mathsf{s}(a + b)$ per ogni $a \in \mathbb{N}$ e per ogni $b \in \mathbb{N}$. In questo modo al posto di $\mathsf{s}(x)$ possiamo scrivere $x + 1$, poiché $\mathsf{s}(x) = x + \mathsf{s}(0) = x + 1$.
9. **Prodotto.** Possiamo definire il prodotto di due naturali $a \cdot b$ per induzione su $b$, ponendo $a \cdot 0 = 0$ per ogni $a \in \mathbb{N}$, e $a \cdot \mathsf{s}(b) = a \cdot b + a$ per ogni $a \in \mathbb{N}$ e per ogni $b \in \mathbb{N}$.

# Interi e Razionali

1. **Classi.** Sia $\mathbb{X}$ un insieme e $\sim$ una relazione di equivalenza su $\mathbb{X}$. Fissato un elemento $x \in \mathbb{X}$, si definisce la sua classe come

$$\mathsf{cl}(x) := \{y \in \mathbb{X} : y \sim x\} \subseteq \mathbb{X}.$$

2. **Insieme quoziente.** Dato $\mathbb{X}$ insieme e $\sim$ una relazione di equivalenza su $\mathbb{X}$, si definisce l'insieme quoziente di $\mathbb{X}$ su $\sim$ come l'insieme che contiene tutte le classi:

$$\mathbb{X}_{/\sim} := \{\mathsf{cl}(x) : x \in \mathbb{X}\} \subseteq \mathcal{P}(\mathbb{X}).$$

3. **Numeri interi.** Sia $\sim$ la relazione di equivalenza su $\mathbb{N}^2$ tale che $(x_1, y_1) \in \mathbb{N}^2$ è simile a $(x_2, y_2) \in \mathbb{N}^2$ se e solo se $x_1 + y_2 = x_2 + y_1$. È immediato verificare che rispetta le proprietà riflessiva, simmetrica e transitiva. Dato un qualunque $(x, y) \in \mathbb{N}^2$, si vede che o $x = y$, oppure esiste $k \in \mathbb{N} \setminus \{0\}$ tale che $(x, y) \sim (0, k)$, oppure esiste $k \in \mathbb{N} \setminus \{0\}$ tale che $(x, y) \sim (k, 0)$. Ora denoteremo con $0 := \mathsf{cl}(0, 0)$, $k := \mathsf{cl}(k, 0)$ e $-k := \mathsf{cl}(0, k)$ e chiameremo numeri interi gli elementi dell'insieme

$$\mathbb{Z} = \mathbb{N}^2_{/\sim} = \{0\} \cup \{k : k \in \mathbb{N} \setminus \{0\}\} \cup \{-k : k \in \mathbb{N} \setminus \{0\}\}.$$

4. **Operazioni sugli interi.** Si può verificare che $\mathbb{N} \subseteq \mathbb{Z}$ e le operazioni di somma e prodotto di $\mathbb{Z}$ sono estendibili a partire da quelle di $\mathbb{N}$. Inoltre si definisce anche la differenza $a - b$ con $a$ e $b$ interi, posta pari ad $(a) + (-b)$.

5. **Numeri razionali.** Sia $\sim$ la relazione di equivalenza su $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definita in modo tale che $(x_1, y_1) \in \mathbb{Z}^2$ con $y_1 \neq 0$ sia simile a $(x_2, y_2) \in \mathbb{Z}^2$ con $y_2 \neq 0$ se e solo se $x_1 \cdot y_2 = x_2 \cdot y_1$. Anche qui è immediato verificare che le proprietà riflessiva, simmetrica e transitiva sono rispettate. Denoteremo con $x/y := \mathsf{cl}(x, y)$ e con $\mathbb{Q}$ l'insieme dei numeri razionali e cioè

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})_{/\sim} = \{x/y : (x, y) \in \mathbb{Z}^2, y \neq 0\}.$$

6. **Operazioni sui razionali.** La somma, il prodotto e la differenza sono definiti estendendo quelli di $\mathbb{Z}$. Inoltre c'è anche l'operazione di quoziente, definendo $p/q$ con $p \in \mathbb{Q}$ e $q \in \mathbb{Q}$ con $q \neq 0$ in modo tale che se $p = x_1/y_1$ e $q = x_2/y_2$ allora $p/q = (x_1 y_2)/(x_2 y_1)$.

7. **Numeri reali.** La definizione di numeri reali è complicata, comunque ci interesserà sapere che esiste un insieme $\mathbb{R}$ su cui valgono tutte le stesse operazioni e ordinamento di $\mathbb{Q}$, in modo che $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

8. **Numeri complessi.** Dato $\mathbb{R}^2$, si definisce il prodotto nel modo seguente:

$$(x, y) \cdot (z, w) = (xz - yw, yz + xw).$$

   In questo caso $\mathbb{R}^2$ si indica con $\mathbb{C}$, e $(x, y) \in \mathbb{R}^2$ si indica con $x + iy$.

# Strutture Algebriche

1. **Operazioni interne.** Sia $\mathbb{X}$ un insieme. Un'operazione interna a $\mathbb{X}$ è una funzione $\mathcal{O} : \mathbb{X}^2 \to \mathbb{X}$. Solitamente si denota con $a \star b$ al posto di $\mathcal{O}(a, b)$.
2. **Commutatività.** L'operazione si dice commutativa se $a \star b = b \star a$ per ogni $a$ e $b$ in $\mathbb{X}$.
3. **Associatività.** L'operazione si dice associativa se $(a \star b) \star c = a \star (b \star c)$ per ogni scelta di $a$, $b$ e $c$ tra gli elementi di $\mathbb{X}$.
4. **Elemento neutro.** L'operazione si dice dotata di elemento neutro se esiste $e \in \mathbb{X}$ tale che per ogni $a \in \mathbb{X}$ si abbia $a \star e = e \star a = a$. L'elemento neutro è unico.
5. **Elemento inverso.** Un'operazione dotata di elemento neutro è detta dotata anche di elemento inverso se per ogni $a \in \mathbb{X}$ esiste $h(a) \in \mathbb{X}$ tale che $a \star h(a) = h(a) \star a = e$. Se l'operazione è associativa, l'elemento inverso è unico.
6. **Semigruppi.** Una coppia $(\mathbb{S}, \mathcal{O})$ dove $\mathcal{O}$ è un'operazione interna a $\mathbb{S}$ si dice semigruppo se $\mathcal{O}$ è associativa. Si dice invece semigruppo abeliano se $\mathcal{O}$ è associativa e commutativa.
7. **Monoidi.** Una coppia $(\mathbb{M}, \mathcal{O})$ dove $\mathcal{O}$ è un'operazione interna a $\mathbb{M}$ si dice monoide se $\mathcal{O}$ è associativa e dotata di elemento neutro. Si dice invece monoide abeliano se $\mathcal{O}$ è associativa, dotata di elemento neutro e commutativa.
8. **Gruppi.** Una coppia $(\mathbb{G}, \mathcal{O})$ dove $\mathcal{O}$ è un'operazione interna a $\mathbb{G}$ si dice gruppo se $\mathcal{O}$ è associativa, dotata di elemento neutro e di elemento inverso. Si dice invece gruppo abeliano se $\mathcal{O}$ è associativa, commutativa e dotata di elemento neutro e inverso.
9. **Anelli.** Una terna $(\mathbb{L}, \mathcal{O}_1, \mathcal{O}_2)$ dove $\mathcal{O}_1$ e $\mathcal{O}_2$ sono operazioni interne a $\mathbb{L}$ si dice anello se $(\mathbb{L}, \mathcal{O}_1)$ è un gruppo abeliano con elemento neutro $e$ e $(\mathbb{L} \setminus \{e\}, \mathcal{O}_2)$ è un monoide. Si dice invece anello abeliano se è un anello e l'operazione $\mathcal{O}_2$ è anche commutativa.
10. **Campi.** Una terna $(\mathbb{F}, \mathcal{O}_1, \mathcal{O}_2)$ dove $\mathcal{O}_1$ e $\mathcal{O}_2$ sono operazioni interne a $\mathbb{X}$ si dice campo se $(\mathbb{F}, \mathcal{O}_1)$ e $(\mathbb{F} \setminus \{e\}, \mathcal{O}_2)$ sono gruppi abeliani, dove $e$ è l'elemento neutro di $\mathcal{O}_1$.
11. **Sottoinsiemi.** Se un insieme $\mathbb{X}$ è un semigruppo, semigruppo abeliano, monoide, monoide abeliano, gruppo, gruppo abeliano, anello, anello abeliano oppure campo rispetto ad una operazione $\mathcal{O}_1$ oppure a due operazioni $\mathcal{O}_1$ e $\mathcal{O}_2$, e un sottoinsieme $\mathbb{Y} \subseteq \mathbb{X}$ è un insieme dello stesso tipo di $\mathbb{X}$ rispetto alla stessa o alle stesse operazioni interne di $\mathbb{X}$, allora $\mathbb{Y}$ si dice rispettivamente sottosemigruppo, sottosemigruppo abeliano, sottomonoide, sottomonoide abeliano, sottogruppo, sottogruppo abeliano, sottoanello, sottoanello abeliano oppure sottocampo di $\mathbb{X}$.

# Campi

1. **Caratteristica di un campo.** Sia $(\mathbb{F}, +, \cdot)$ un campo ($+$ e $\cdot$ sono i nomi dati alle operazioni, le quali potrebbero non essere somma e prodotto). Siano 0 e 1 gli elementi neutri di $+$ e $\cdot$ rispettivamente. Consideriamo la successione $1, 1+1, 1+1+1, \ldots$ Se gli elementi di questa successione sono tutti diversi da 0, allora si pone $\mathsf{char}(\mathbb{F}) = 0$. Se invece esiste un elemento uguale a zero, si considera il più piccolo numero $p \in \mathbb{N} \setminus \{0\}$ tale che $1 + \ldots + 1 = 0$ (dove il numero 1 è presente $p$ volte) e si pone $\mathsf{char}(\mathbb{F}) = p$.
2. **Campi finiti con $p$ elementi.** Sia $p \in \mathbb{P}$ un numero primo. Consideriamo la relazione di equivalenza $\sim$ su $\mathbb{Z}$ tale che $a \sim b$ se e solo se esiste $k \in \mathbb{Z}$ tale che $a = b + kp$. Allora sia
$$\mathbb{F}_p := \mathbb{Z}_{/\sim} = \{\mathsf{cl}(0), \mathsf{cl}(1), \ldots, \mathsf{cl}(p-1)\}.$$
Questo è un campo e ha un numero finito $p$ di elementi. Inoltre $\mathsf{char}(\mathbb{F}_p) = p$. Le operazioni di somma e moltiplicazione sono ben definite su $\mathbb{F}_p$, così come l'inversa per elementi diversi da $\mathsf{cl}(0)$.
3. **Campi algebricamente chiusi.** Un campo $\mathbb{F}$ si dice algebricamente chiuso se ogni polinomio a $p(t) \in \mathbb{F}[t]$ a coefficienti in $\mathbb{F}$ di grado $\mathsf{deg}(p) > 0$ ammette una radice in $\mathbb{F}$, cioè esiste $\zeta \in \mathbb{F}$ tale che $p(\zeta) = 0$. In particolare, se $\mathbb{F}$ è un campo algebricamente chiuso, ogni polinomio $p(t) \in \mathbb{F}[t]$ ammette esattamente $\mathsf{deg}(p)$ radici.
4. **Chiusura algebrica di un campo.** Sia $\mathbb{F}$ un campo. Si chiama chiusura algebrica di $\mathbb{F}$, e si indica con $\widehat{\mathbb{F}}$, il più piccolo campo algebricamente chiuso che contiene $\mathbb{F}$. Ad esempio, la chiusura algebrica di $\mathbb{R}$ è $\mathbb{C}$.

# Gruppi Simmetrici

1. **Permutazione.** Sia $n \geq 1$ un naturale. Una funzione $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ bigettiva si dice permutazione dell'insieme $\{1, \ldots, n\}$.
2. **Gruppo simmetrico.** L'insieme di tutte le permutazioni dell'insieme $\{1, \ldots, n\}$ è un gruppo rispetto all'operazione di composizione, e si chiama $n$-esimo gruppo simmetrico. Si indica solitamente con $\mathfrak{S}_n$. Se $n > 2$ il gruppo non è abeliano. Il numero di elementi dell'$n$-esimo gruppo simmetrico è $n! = n \cdot (n-1) \cdot \ldots \cdot 1$.
3. **Trasposizione.** Per $n \geq 2$, dati $i$ e $j$ distinti tra 1 ed $n$, si definisce la trasposizione $\tau_{ij} \in \mathfrak{S}_n$ come $\tau_{ij}(i) = j$, $\tau_{ij}(j) = i$ e $\tau_{ij}(k) = k$ per $k \neq i$ e $k \neq j$. In $\mathfrak{S}_n$ ci sono $n(n-1)/2$ trasposizioni diverse, considerando $\tau_{ij}$ e $\tau_{ji}$ come la stessa trasposizione.
4. **Composizione di trasposizioni.** Ogni permutazione $\sigma \in \mathfrak{S}_n$ con $n \geq 2$ si scrive come composizione di un certo numero (finito) di trasposizioni $\tau_{ij} \in \mathfrak{S}_n$.
5. **Il numero di trasposizioni necessarie non è fisso.** Data una permutazione $\sigma \in \mathfrak{S}_n$ con $n \geq 2$, si può scrivere in diversi (in realtà infiniti) modi come composizione di trasposizioni distinte in $\mathfrak{S}_n$. Però fissata $\sigma$, la parità del numero di trasposizioni necessarie per scrivere $\sigma$ come composizione di trasposizioni è fissa. Ci sono quindi permutazioni pari, che necessitano di un numero pari di trasposizioni, e permutazioni dispari, che necessitano di un numero dispari di trasposizioni.
6. **Segno di una permutazione.** Data $\sigma \in \mathfrak{S}_n$, si definisce $\mathsf{sgn}(\sigma)$ come $+1$ se $\sigma$ è una permutazione pari, e $-1$ se $\sigma$ è una permutazione dispari. Il segno di una permutazione si comporta bene con la composizione: il segno della composizione di due permutazioni è pari al prodotto dei segni delle due permutazioni.

# Spazi Vettoriali

1. **Spazio vettoriale.** Sia $(\mathbb{F}, +, \cdot)$ un campo. Un insieme $\mathbb{V}$ si dice spazio vettoriale su $\mathbb{F}$ rispetto a un'operazione interna $\mathcal{O}$ e un'operazione esterna $\mathcal{E} : \mathbb{F} \times \mathbb{V} \to \mathbb{V}$ se $(\mathbb{V}, \mathcal{O})$ è un gruppo abeliano, e l'operazione esterna soddisfa le seguenti proprietà: dette $a \oplus b$ l'operazione $\mathcal{O}(a, b)$ e $a \otimes b$ l'operazione $\mathcal{E}(a, b)$, si ha che queste operazioni soddisfano le proprietà cosiddette di distributività, pseudodistributività, pseudoassociatività e neutralità dell'elemento neutro.
2. **Distributività.** L'operazione $\oplus$ si dice distributiva rispetto a $\otimes$ se per ogni $k \in \mathbb{F}$ e per ogni $v_1$ e $v_2$ in $\mathbb{V}$ si ha che
$$k \otimes (v_1 \oplus v_2) = (k \otimes v_1) \oplus (k \otimes v_2).$$
3. **Pseudodistributività.** L'operazione $\otimes$ si dice pseudodistributiva rispetto a $+$ se per ogni $k_1$ e $k_2$ in $\mathbb{F}$ e per ogni $v \in \mathbb{V}$ si ha che
$$(k_1 + k_2) \otimes v = (k_1 \otimes v) \oplus (k_2 \otimes v).$$
4. **Pseudoassociatività.** Le operazioni $\otimes$ e $\cdot$ si dicono pseudoassociative se per ogni $k_1$ e $k_2$ in $\mathbb{F}$ e per ogni $v \in \mathbb{V}$ si ha che
$$k_1 \otimes (k_2 \otimes v) = (k_1 \cdot k_2) \otimes v.$$
5. **Neutralità dell'elemento neutro.** Si dice che l'elemento neutro dell'operazione $\cdot$ di $\mathbb{F}$ (che indicheremo con 1) è neutrale per l'operazione $\otimes$ se per ogni $v \in \mathbb{V}$ si ha che
$$1 \otimes v = v.$$
6. **Nomi delle operazioni.** L'operazione $\oplus$ si denota solitamente con $+$ ed è detta somma. L'operazione $\otimes$ si denota solitamente con $\cdot$ ed è detta prodotto per scalare. Gli elementi di $\mathbb{F}$ infatti sono chiamati scalari, mentre gli elementi di $\mathbb{V}$ vettori.
7. **Sottospazi vettoriali.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ e $\mathbb{U}$ un altro spazio vettoriale su $\mathbb{F}$ tale che $\mathbb{U} \subseteq \mathbb{V}$. Allora $\mathbb{U}$ si dice sottospazio vettoriale di $\mathbb{V}$.
8. **Spazio vettoriale banale.** Sia 0 l'elemento neutro dell'operazione $\mathcal{O}$ in $\mathbb{V}$ (spazio vettoriale su $\mathbb{F}$). Allora l'insieme $\{0\}$ è uno spazio vettoriale su $\mathbb{F}$, sottospazio di $\mathbb{V}$. Ogni sottospazio vettoriale $\mathbb{U}$ di $\mathbb{V}$ è tale che $\{0\} \subseteq \mathbb{U} \subseteq \mathbb{V}$.
9. **Ordinamento dei sottospazi vettoriali.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$. Allora l'insieme dei sottospazi vettoriali di $\mathbb{V}$ è (parzialmente) ordinato rispetto alla relazione d'ordine $\subseteq$, ed esistono un massimo $\mathbb{V}$ ed un minimo $\{0\}$.
10. **Spazio delle $n$-uple.** Sia $n \geq 1$ un naturale e sia $\mathbb{F}$ un campo. Allora $\mathbb{F}^n$ è uno spazio vettoriale su $\mathbb{F}$. La somma e il prodotto per scalari sono intesi termine a termine.

# Applicazioni Lineari

1. **Linearità.** Siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali sullo stesso campo $\mathbb{F}$. Una funzione $f : \mathbb{V} \to \mathbb{W}$ si dice lineare se per ogni coppia di vettori $v_1$ e $v_2$ in $\mathbb{V}$ si ha che
$$f(v_1 + v_2) = f(v_1) + f(v_2)$$
e per ogni $k \in \mathbb{F}$ e per ogni $v \in \mathbb{V}$ si ha che
$$f(k \cdot v) = k \cdot f(v).$$
2. **Isomorfismi tra spazi vettoriali.** Siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali sullo stesso campo $\mathbb{F}$. Se esiste una funzione $\psi : \mathbb{V} \to \mathbb{W}$ lineare e bigettiva, allora gli spazi $\mathbb{V}$ e $\mathbb{W}$ si dicono isomorfi e $\psi$ è detta isomorfismo tra spazi vettoriali.
3. **Combinazione lineare.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$, $\mathbb{I}$ un insieme (di indici) e $\mathbb{J} \subseteq \mathbb{V}$ con $\mathbb{J} = \{v_i : i \in \mathbb{I}\}$. Una combinazione lineare di questi vettori è una somma finita di loro multipli, cioè una scrittura del tipo
$$\sum_{j=1}^{n} k_{i_j} v_{i_j} = k_{i_1} v_{i_1} + \ldots + k_{i_n} v_{i_n}$$
con $\{i_1, \ldots, i_n\} \subseteq \mathbb{I}$ e $k_{i_j} \in \mathbb{F}$ per ogni $j$ da 1 a $n$. In un altro modo, si può scrivere
$$\sum_{i \in \mathbb{I}} k_i v_i, \text{ con } k_i \in \mathbb{F} \text{ e } k_i = 0 \text{ per quasi tutti gli } i,$$
dove "per quasi tutti gli $i$" significa "per tutti gli $i$ tranne che al più un numero finito".
4. **Indipendenza lineare.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$, $\mathbb{I}$ un insieme (di indici) e $\mathbb{J} = \{v_i : i \in \mathbb{I}\} \subseteq \mathbb{V}$. Gli elementi di $\mathbb{J}$ si dicono linearmente indipendenti se l'unica loro combinazione lineare nulla è quella con tutti i coefficienti pari a 0, cioè se
$$\sum_{i \in \mathbb{I}} k_i v_i = 0, \text{ con } k_i \in \mathbb{F} \text{ e } k_i = 0 \text{ per quasi tutti gli } i,$$
allora $k_i = 0$ per ogni $i \in \mathbb{I}$. Similmente, dei vettori si dicono linearmente dipendenti se non sono linearmente dipendenti (cioè se esiste almeno una combinazione lineare di quei vettori che sia nulla e con i coefficienti non tutti nulli).
5. **Un altro modo di vedere la linearità.** Le combinazioni lineari sono un tratto caratteristico degli spazi vettoriali. Le applicazioni vettoriali sono le funzioni tra spazi vettoriali che preservano le combinazioni lineari, cioè $f$ è lineare se e solo se
$$f\left(\sum_{i \in \mathbb{I}} k_i v_i\right) = \sum_{i \in \mathbb{I}} k_i f(v_i),$$
con $k_i \in \mathbb{F}$ e $k_i = 0$ per quasi tutti gli $i$. Gli isomorfismi tra spazi vettoriali sono quindi funzioni bigettive che preservano la struttura di spazio vettoriale.

# Sottospazi Generati

1. **Sottospazi generati.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ e sia $\mathbb{I}$ un insieme. Consideriamo l'insieme $\mathbb{J} \subseteq \mathbb{V}$ con $\mathbb{J} = \{v_i : i \in \mathbb{I}\}$. L'insieme di tutte le combinazioni lineari di elementi di $\mathbb{J}$ si chiama sottospazio vettoriale generato da $\mathbb{J}$, e si indica con $\mathsf{span}(\mathbb{J})$. Si può verificare che $\mathsf{span}(\mathbb{J})$ è il più piccolo sottospazio vettoriale di $\mathbb{V}$ contenente $\mathbb{J}$.
2. **Sottospazio generato dall'insieme vuoto.** Abbiamo definito $\mathsf{span}(\mathbb{J})$ ma nel farlo abbiamo supposto che $\mathbb{J} \neq \emptyset$. La definizione si può estendere ponendo $\mathsf{span}(\emptyset) = \{0\}$, cioè il più piccolo sottospazio vettoriale di $\mathbb{V}$.
3. **Lineare indipendenza di un elemento.** Sia $\mathbb{V}$ uno spazio vettoriale su un campo $\mathbb{F}$ e sia $\mathbb{J} = \{v\} \subseteq \mathbb{V}$ (cioè, $\mathbb{J}$ contiene un solo elemento). Allora $\mathbb{J}$ è linearmente indipendente se e solo se $v \neq 0$. Infatti per essere linearmente indipendente deve valere che se $kv = 0$ allora $k = 0$, e questo è vero per ogni vettore $v \neq 0$.
4. **Rimuovere un elemento da un insieme linearmente dipendente.** Sia $\mathbb{V}$ uno spazio vettoriale su un campo $\mathbb{F}$ e sia $\mathbb{I}$ un insieme e $\mathbb{J} = \{v_i : i \in \mathbb{I}\}$. Allora $\mathbb{J}$ è linearmente dipendente se e solo se esiste un $j \in \mathbb{I}$ tale che $\mathsf{span}(\mathbb{J}) = \mathsf{span}(\mathbb{J} \setminus \{v_j\})$. In parole povere, un insieme è linearmente dipendente se e solo se esiste un suo elemento che è combinazione lineare degli altri.
5. **Aggiungere un elemento ad un insieme linearmente indipendente.** Sia $\mathbb{V}$ uno spazio vettoriale su un campo $\mathbb{F}$ e sia $\mathbb{I}$ un insieme e $\mathbb{J} = \{v_i : i \in \mathbb{I}\}$ linearmente indipendente. Allora se $v \in \mathbb{V}$ e $v \notin \mathsf{span}(\mathbb{J})$, anche $\mathbb{J} \cup \{v\}$ è linearmente indipendente. Infatti non è possibile che $\mathbb{J} \cup \{v\}$ sia linearmente dipendente, perché vorrebbe dire o che $\mathbb{J}$ non era linearmente indipendente oppure che $v \in \mathsf{span}(\mathbb{J})$.

# Teorema di Esistenza di una Base

1. **Base.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$. Un sottoinsieme $\mathbb{B} \subseteq \mathbb{V}$ si dice base di $\mathbb{V}$ se è linearmente indipendente e $\mathsf{span}(\mathbb{B}) = \mathbb{V}$.
2. **Esistenza delle basi.** Consideriamo l'insieme dei sottoinsiemi linearmente indipendenti di $\mathbb{V}$. Questo insieme è ordinato parzialmente secondo l'inclusione $\subseteq$. Ogni catena di questo insieme ha un maggiorante poiché presa una catena (cioè un insieme totalmente ordinato di sottoinsiemi linearmente indipendenti di $\mathbb{V}$) l'unione di tutti gli insiemi che formano la catena contiene ovviamente tutti quegli insiemi e inoltre è linearmente indipendente poiché se non lo fosse dovrebbe esistere un insieme facente parte della catena e non linearmente indipendente. Quindi ogni catena ha un maggiorante e per il lemma di Zorn esiste un elemento massimale dell'insieme dei sottoinsiemi di $\mathbb{V}$ linearmente indipendenti. Sia $\mathbb{B}$ questo elemento massimale. Se $\mathbb{B}$ non fosse una base si avrebbe che $\mathsf{span}(\mathbb{B}) \neq \mathbb{V}$ e quindi esisterebbe $v \in \mathbb{V}$ con $v \notin \mathsf{span}(\mathbb{B})$, quindi si potrebbe aggiungere $v$ a $\mathbb{B}$ ottenendo che $\mathbb{B} \cup \{v\}$ è linearmente indipendente, assurdo perché $\mathbb{B}$ era un elemento massimale dell'insieme dei sottoinsiemi di $\mathbb{V}$ linearmente indipendenti.
3. **Equivalenza con il lemma di Zorn.** Il teorema di esistenza di una base è equivalente al lemma di Zorn (e quindi è equivalente anche all'assioma della scelta).
4. **Scrittura univoca.** Sia $\mathbb{V} \neq \{0\}$ uno spazio vettoriale sul campo $\mathbb{F}$. $\mathbb{B}$ è una base di $\mathbb{V}$ se e solo se ogni elemento di $\mathbb{V}$ si scrive in modo unico come combinazione lineare di elementi di $\mathbb{B}$. Infatti $\mathbb{V} = \mathsf{span}(\mathbb{B})$ se e solo se ogni elemento di $\mathbb{V}$ si può scrivere (in almeno un modo) come combinazione lineare di elementi di $\mathbb{B}$; e $\mathbb{B}$ è linearmente indipendente se e solo se ogni elemento di $\mathbb{V}$ si può scrivere al massimo in un modo come combinazione lineare di elementi di $\mathbb{B}$, perché se si potesse scrivere in più di un modo diverso la differenza tra questi sarebbe una combinazione lineare di elementi di $\mathbb{B}$ uguale a 0 e ma non con tutti i coefficienti uguali a 0.
5. **Coordinate rispetto ad una base.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$ e sia $\mathbb{B}$ una base con $n$ elementi. Allora esiste un isomorfismo $\psi : \mathbb{V} \to \mathbb{F}^n$. Dato un vettore $v \in \mathbb{V}$, $\psi(v)$ si chiamano coordinate di $v$ rispetto alla base $\mathbb{B}$. Basi diverse producono isomorfismi diversi e quindi generalmente coordinate diverse.
6. **Delta di Kronecker.** Sia $\mathbb{I}$ un insieme (di indici) e siano $i$ e $j$ due indici qualunque. Si pone
$$\delta_{ij} = \begin{cases} 1 \text{ se } i = j; \\ 0 \text{ se } i \neq j. \end{cases}$$
Questa si chiama delta di Kronecker.
7. **Base canonica.** Dato lo spazio vettoriale $\mathbb{F}^n$, consideriamo gli elementi $e_i$ (per $i$ da 1 ad $n$) che come $j$-esima componente hanno $\delta_{ij}$ (per $j$ da 1 ad $n$). In altre parole $e_i$ è la $n$-upla di scalari in $\mathbb{F}$ composta da solo zeri tranne un 1 in $i$-esima posizione. L'insieme $\{e_1, \ldots, e_n\}$ si chiama base canonica di $\mathbb{F}^n$.

# Teorema di Steinitz

1. **Da un insieme che genera lo spazio intero ad una base.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ e sia $\mathbb{J} \subseteq \mathbb{V}$ con un numero finito di elementi e tale che $\mathsf{span}(\mathbb{J}) = \mathbb{V}$. Allora esiste $\mathbb{B} \subseteq \mathbb{J}$ base di $\mathbb{V}$. Infatti da $\mathbb{J}$ si può rimuovere di volta in volta un vettore fino a trovare un insieme linearmente indipendente $\mathbb{B}$, tenendo comunque $\mathsf{span}(\mathbb{J}) = \mathsf{span}(\mathbb{B})$.
2. **Sostituire un vettore in una base.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ e siano $\mathbb{B}$ una base di $\mathbb{V}$ e $u \neq 0$ un vettore di $\mathbb{V}$. Allora esiste un vettore $v_j \in \mathbb{B}$ tale che $\mathbb{B} \setminus \{v_j\} \cup \{u\}$ è una base di $\mathbb{V}$. Infatti scrivendo $u$ come combinazione lineare di elementi di $\mathbb{B}$, ce ne sarà almeno uno (detto $v_j$) con coefficiente $k_j$ non nullo, e a questo punto si può rimuovere e sostituire con $u$ ottenendo sempre una base.
3. **Teorema di Steinitz.** Sia $\mathbb{V}$ uno spazio vettoriale su un campo $\mathbb{F}$ e sia $\mathbb{B}$ una base di $\mathbb{V}$ con $n$ elementi. Sia $\mathbb{J} \subseteq \mathbb{V}$ un insieme linearmente indipendente con $m$ elementi. Allora esiste un sottoinsieme $\mathbb{J}' \subseteq \mathbb{B}$ con $m$ elementi e tale che $\mathbb{B} \setminus \mathbb{J}' \cup \mathbb{J}$ sia una base di $\mathbb{V}$. Inoltre otteniamo $m \leq n$, quindi ogni insieme linearmente indipendente ha meno elementi di una base. Per dimostrare il teorema di Steinitz bisogna applicare $m$ volte la sostituzione di un vettore in una base, stando attenti a non sostituire un elemento di $\mathbb{J}$ con un altro elemento di $\mathbb{J}$ già precedentemente sostituito. È sempre possibile evitare che accada qualcosa del genere poiché $\mathbb{J}$ è linearmente indipendente e quindi se i coefficienti $k_j$ davanti agli elementi di $\mathbb{B}$ fossero tutti nulli si avrebbe una contraddizione.
4. **Ogni base ha la stessa cardinalità.** Se prendiamo due basi finite $\mathbb{B}$ e $\mathbb{B}'$ di $\mathbb{V}$ otteniamo $\mathsf{card}(\mathbb{B}') \leq \mathsf{card}(\mathbb{B})$ e $\mathsf{card}(\mathbb{B}) \leq \mathsf{card}(\mathbb{B}')$ da cui $\mathsf{card}(\mathbb{B}) = \mathsf{card}(\mathbb{B}')$ e quindi ogni base di $\mathbb{V}$ ha la stessa cardinalità.
5. **Dimensione di uno spazio vettoriale.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$, e sia $\mathbb{B}$ una base di $\mathbb{V}$. Allora se $\mathbb{B}$ ha infiniti elementi si pone $\mathsf{dim}(\mathbb{V}) = \infty$, mentre se $\mathbb{B}$ ha un numero finito $n$ di elementi si pone $\mathsf{dim}(\mathbb{V}) = n$. In altre parole stiamo definendo la dimensione di uno spazio vettoriale come pari alla cardinalità di una sua base, visto che si ha sempre $\mathsf{dim}(\mathbb{V}) = \mathsf{card}(\mathbb{B})$. La definizione è ben posta poiché sappiamo che ogni base ha la stessa cardinalità.
6. **Da un insieme linearmente indipendente ad una base.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ di dimensione finita e sia $\mathbb{J} \subseteq \mathbb{V}$ un sottoinsieme linearmente indipendente con $m$ elementi. Per il teorema di Steinitz esiste una base $\mathbb{B}$ tale che $\mathbb{J} \subseteq \mathbb{B}$.
7. **Numero di elementi di una base.** Un'altra conseguenza del teorema di Steinitz è che, se $\mathbb{V}$ è uno spazio vettoriale su $\mathbb{F}$ di dimensione finita, ogni sottoinsieme linearmente indipendente con $\mathsf{dim}(\mathbb{V})$ elementi è una base, così come ogni sottoinsieme con $\mathsf{dim}(\mathbb{V})$ elementi che genera $\mathbb{V}$ è una base.
8. **Dimensione di un sottospazio.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ di dimensione finita e sia $\mathbb{U} \subseteq \mathbb{V}$ un sottospazio. Allora $\mathsf{dim}(\mathbb{U}) \leq \mathsf{dim}(\mathbb{V})$, con uguaglianza solo se $\mathbb{U} = \mathbb{V}$.

# Formula di Grassmann

1. **Intersezione finita di sottospazi.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$, e siano $\mathbb{U}_1$ e $\mathbb{U}_2$ due sottospazi di $\mathbb{V}$. Allora $\mathbb{U}_1 \cap \mathbb{U}_2$ è un sottospazio di $\mathbb{V}$. Infatti preso un qualsiasi sottoinsieme $\mathbb{J} \subseteq \mathbb{U}_1 \cap \mathbb{U}_2$, di sicuro $\mathbb{J} \subseteq \mathbb{U}_1$ e $\mathbb{J} \subseteq \mathbb{U}_2$, quindi $\mathsf{span}(\mathbb{J}) \subseteq \mathbb{U}_1$ e $\mathsf{span}(\mathbb{J}) \subseteq \mathbb{U}_2$, e dunque $\mathsf{span}(\mathbb{J}) \subseteq \mathbb{U}_1 \cap \mathbb{U}_2$.
2. **Intersezione qualunque di sottospazi.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$, $\mathbb{I}$ un insieme e $\{\mathbb{U}_i : i \in \mathbb{I}\}$ un insieme di sottospazi. Allora l'intersezione di tutti gli $\mathbb{U}_i$ è un sottospazio di $\mathbb{V}$.
3. **Unione di sottospazi.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$ e siano $\mathbb{U}_1$ e $\mathbb{U}_2$ due sottospazi di $\mathbb{V}$. Allora generalmente $\mathbb{U}_1 \cup \mathbb{U}_2$ non è un sottospazio vettoriale di $\mathbb{V}$.
4. **Somma finita di sottospazi.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$ e siano $\mathbb{U}_1$ e $\mathbb{U}_2$ due sottospazi di $\mathbb{V}$. Allora
$$\mathbb{U}_1 + \mathbb{U}_2 := \{u_1 + u_2 : u_1 \in \mathbb{U}_1 \text{ e } u_2 \in \mathbb{U}_2\}$$
è un sottospazio di $\mathbb{V}$, ed è il più piccolo sottospazio di $\mathbb{V}$ che contiene $\mathbb{U}_1 \cup \mathbb{U}_2$.
5. **Somma qualunque di sottospazi.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$, $\mathbb{I}$ un insieme e $\{\mathbb{U}_i : i \in \mathbb{I}\}$ un insieme di sottospazi. Allora la somma di tutti gli $\mathbb{U}_i$, definita come sopra, è un sottospazio di $\mathbb{V}$, ed è il più piccolo sottospazio di $\mathbb{V}$ che contiene l'unione di tutti gli $\mathbb{U}_i$.
6. **Somma diretta di sottospazi.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$ e siano $\mathbb{U}_1$ e $\mathbb{U}_2$ due sottospazi di $\mathbb{V}$ con $\mathbb{U}_1 \cap \mathbb{U}_2 = \{0\}$. Allora $\mathbb{U}_1 + \mathbb{U}_2$ è una somma diretta, cioè dato un qualsiasi elemento $u \in \mathbb{U}_1 + \mathbb{U}_2$ esistono unici $u_1 \in \mathbb{U}_1$ e $u_2 \in \mathbb{U}_2$ tali che $u = u_1 + u_2$. La somma diretta di $\mathbb{U}_1$ e $\mathbb{U}_2$ si indica con $\mathbb{U}_1 \oplus \mathbb{U}_2$.
7. **Formula di Grassmann.** Sia $\mathbb{V}$ uno spazio vettoriale di dimensione finita sul campo $\mathbb{F}$ e siano $\mathbb{U}_1$ e $\mathbb{U}_2$ due sottospazi di $\mathbb{V}$. Allora
$$\mathsf{dim}(\mathbb{U}_1 + \mathbb{U}_2) + \mathsf{dim}(\mathbb{U}_1 \cap \mathbb{U}_2) = \mathsf{dim}(\mathbb{U}_1) + \mathsf{dim}(\mathbb{U}_2).$$
Questo si dimostra considerando una base di $\mathbb{U}_1 \cap \mathbb{U}_2$, usando Steinitz per completarla ad una base prima di $\mathbb{U}_1$ e poi di $\mathbb{U}_2$, e mostrando infine che l'unione di queste basi è una base di $\mathbb{U}_1 + \mathbb{U}_2$.
8. **Spazio vettoriale quoziente.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$ e $\mathbb{U}$ un sottospazio vettoriale di $\mathbb{V}$. Sia $\sim$ la relazione di equivalenza su $\mathbb{V}$ definita in modo tale che $v_1 \sim v_2$ se e solo se $v_1 - v_2 \in \mathbb{U}$. Allora $\mathbb{V}/\mathbb{U} := \mathbb{V}_{/\sim}$ è uno spazio vettoriale su $\mathbb{F}$, e se $\mathbb{V}$ ha dimensione finita allora
$$\mathsf{dim}(\mathbb{V}/\mathbb{U}) = \mathsf{dim}(\mathbb{V}) - \mathsf{dim}(\mathbb{U}).$$

# Matrici

1. **Matrici.** Si dice matrice di dimensioni $n \times m$ una tabella di numeri con $n$ righe ed $m$ colonne. Solitamente con $m_{ij}$ si indica il numero scritto nella riga $i$-esima e colonna $j$-esima della matrice M. L'insieme di tutte le matrici di dimensioni $n \times m$ a coefficienti in un campo $\mathbb{F}$ è uno spazio vettoriale su $\mathbb{F}$, e si indica con $\mathcal{M}_{n\times m}(\mathbb{F})$. Si ha che
$$\mathsf{dim}(\mathcal{M}_{n\times m}(\mathbb{F})) = n \cdot m.$$

2. **Prodotto tra matrici.** Siano $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$ e $\mathrm{B} \in \mathcal{M}_{m\times k}(\mathbb{F})$. Allora si definisce prodotto tra la matrice $\mathrm{A} = \{a_{ij}\}$ e la matrice $\mathrm{B} = \{b_{jr}\}$ la matrice $\mathrm{C} = \{c_{ir}\}$ con
$$c_{ir} = \sum_{j=1}^{m} a_{ij} b_{jr}.$$
In particolare $\mathrm{C} \in \mathcal{M}_{n\times k}(\mathbb{F})$. Solitamente si indica $\mathrm{C} = \mathrm{A} \cdot \mathrm{B}$. Da questo segue che se le matrici A e B sono delle matrici $n \times n$, anche il loro prodotto è una matrice $n \times n$.

3. **Matrice identica.** Dato $m \geq 1$ si definisce matrice identica $m \times m$ la matrice $\mathrm{Id} \in \mathcal{M}_{m\times m}(\mathbb{F})$ dove $\mathrm{Id} = \{\delta_{ij}\}$ (delta di Kronecker). Per ogni matrice $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$ e $\mathrm{B} \in \mathcal{M}_{m\times k}(\mathbb{F})$ si ha
$$\mathrm{A} \cdot \mathrm{Id} = \mathrm{A}, \qquad \mathrm{Id} \cdot \mathrm{B} = \mathrm{B}.$$

4. **Matrici invertibili e inverse.** Data $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$, si dice invertibile se esiste una sua matrice inversa, cioè se esiste $\mathrm{B} \in \mathcal{M}_{m\times n}(\mathbb{F})$ tale che
$$\mathrm{A} \cdot \mathrm{B} = \mathrm{Id}, \qquad \mathrm{B} \cdot \mathrm{A} = \mathrm{Id},$$
dove la prima Id è la matrice identica $n \times n$ e la seconda Id è la matrice identica $m \times m$. Solitamente si indica B con $\mathrm{A}^{-1}$.

5. **Matrici diagonali e triangolari.** Una matrice $\mathrm{D} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice diagonale se scritto $\mathrm{D} = \{d_{ij}\}$ si ha $d_{ij} = 0$ per $i \neq j$. Una matrice $\mathrm{T} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice triangolare superiore se scritto $\mathrm{T} = \{t_{ij}\}$ si ha $t_{ij} = 0$ per $i > j$. Una matrice $\mathrm{T} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice triangolare inferiore se scritto $\mathrm{T} = \{t_{ij}\}$ si ha $t_{ij} = 0$ per $i < j$. Gli insiemi delle matrici diagonali, triangolari superiori e triangolari inferiori sono sottospazi vettoriali di $\mathcal{M}_{n\times n}(\mathbb{F})$, di dimensioni $n$, $(n^2+n)/2$ ed $(n^2+n)/2$ rispettivamente.

6. **Matrici nihilpotenti.** Una matrice $\mathrm{N} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice nihilpotente se esiste un $r \geq 1$ tale che $\mathrm{N}^r = 0$, cioè $\mathrm{N} \cdot \ldots \cdot \mathrm{N}$ (il prodotto di $r$ volte la matrice) è la matrice nulla, con tutti i coefficienti uguali a 0.

7. **Lemma.** Se $\mathrm{N} \in \mathcal{M}_{n\times n}(\mathbb{F})$ è nihilpotente, $\mathrm{Id} - \mathrm{N}$ è invertibile. Infatti
$$(\mathrm{Id} - \mathrm{N}) \cdot (\mathrm{Id} + \mathrm{N} + \mathrm{N}^2 + \ldots + \mathrm{N}^{r-1}) = \mathrm{Id}.$$

# Trasposizione di Matrici

1. **Matrici trasposte.** Sia $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$ una matrice, $\mathrm{A} = \{a_{ij}\}$. Si definisce matrice trasposta di A, scritto $\mathrm{A}^t$, la matrice in $\mathcal{M}_{m\times n}(\mathbb{F})$ con $\mathrm{A}^t = \{a_{ji}\}$.

2. **Proprietà della trasposizione.** La matrice trasposta della somma tra due matrici è la somma delle due trasposte:

$$(\mathrm{A} + \mathrm{B})^t = \mathrm{A}^t + \mathrm{B}^t.$$

   La matrice trasposta del prodotto tra due matrici A e B è il prodotto tra le due matrici trasposte scambiate di posto:

$$(\mathrm{A} \cdot \mathrm{B})^t = \mathrm{B}^t \cdot \mathrm{A}^t.$$

   Quindi la trasposta di una matrice invertibile è invertibile e la sua inversa è la trasposta dell'inversa:

$$(\mathrm{A}^{-1})^t = (\mathrm{A}^t)^{-1}.$$

   La trasposta della trasposta di una matrice è la matrice stessa:

$$(\mathrm{A}^t)^t = \mathrm{A}.$$

3. **Proprietà delle matrici mantenute dalla trasposizione.** Matrici diagonali, triangolari superiori, triangolari inferiori e nihilpotenti vanno rispettivamente in matrici diagonali, triangolari inferiori, triangolari superiori e nihilpotenti tramite trasposizione.

4. **Matrici simmetriche.** Una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice simmetrica se $\mathrm{A}^t = \mathrm{A}$, o in altre parole scritto $\mathrm{A} = \{a_{ij}\}$ si ha $a_{ij} = a_{ji}$ per ogni $i$ e $j$. L'insieme delle matrici simmetriche $n \times n$ è un sottospazio vettoriale di $\mathcal{M}_{n\times n}(\mathbb{F})$, di dimensione $(n^2 + n)/2$ (la stessa dimensione del sottospazio delle matrici triangolari).

5. **Matrici antisimmetriche.** Una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice antisimmetrica se $\mathrm{A}^t = -\mathrm{A}$, o in altre parole scritto $\mathrm{A} = \{a_{ij}\}$ si ha $a_{ij} + a_{ji} = 0$ per ogni $i$ e $j$. In particolare $a_{ii} = 0$ per ogni $i$. L'insieme delle matrici antisimmetriche $n \times n$ è un sottospazio vettoriale di $\mathcal{M}_{n\times n}(\mathbb{F})$, di dimensione $(n^2 - n)/2$.

6. **Somma diretta tra matrici simmetriche ed antisimmetriche.** Sia $\mathcal{S}_{n\times n}(\mathbb{F})$ l'insieme delle matrici simmetriche $n \times n$ e sia $\mathcal{A}_{n\times n}(\mathbb{F})$ l'insieme delle matrici antisimmetriche $n \times n$. Allora siccome $\mathcal{S}_{n\times n}(\mathbb{F}) \cap \mathcal{A}_{n\times n}(\mathbb{F})$ comprende solo la matrice nulla, si ha che la somma di questi due sottospazi vettoriali di $\mathcal{M}_{n\times n}(\mathbb{F})$ è una somma diretta, e viste le dimensioni si ha che

$$\mathcal{S}_{n\times n}(\mathbb{F}) \oplus \mathcal{A}_{n\times n}(\mathbb{F}) = \mathcal{M}_{n\times n}(\mathbb{F}).$$

   Quindi ogni matrice $n \times n$ si può scrivere come somma di una matrice simmetrica e di una antisimmetrica. Scritta $\mathrm{M} \in \mathcal{M}_{n\times n}(\mathbb{F})$ come $\mathrm{M}_s + \mathrm{M}_a$ con $\mathrm{M}_s$ simmetrica e $\mathrm{M}_a$ antisimmetrica, $\mathrm{M}_s$ si dice parte simmetrica di M e $\mathrm{M}_a$ parte antisimmetrica di M.

# Algoritmo di Gauss

1. **Matrici elementari.** Si dicono matrici elementari alcune particolari matrici $n \times n$ che, moltiplicate per un'altra matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$, fanno delle operazioni sulle righe di A. Le matrici elementari fanno tre tipologie di operazioni: scambio, prodotto per scalare, e sottrazione di un multiplo di un'altra riga.
2. **Matrice di scambio.** Siano $a$ e $b$ due interi tra 1 ed $n$. Si definisce la matrice $\mathrm{S}_{ab} \in \mathcal{M}_{n\times n}(\mathbb{F})$ come la matrice $\{s_{ij}\}$ con $s_{ij} = 1$ quando $i = a$ e $j = b$, $s_{ij} = 1$ quando $i = b$ e $j = a$, e $s_{ij} = 1$ quando $i = j$ e $i \neq a$ e $i \neq b$, mentre invece $s_{ij} = 0$ in tutti gli altri casi. Questa matrice è la matrice che scambia la riga $a$-esima con la riga $b$-esima di una matrice. La matrice inversa di $\mathrm{S}_{ab}$ è $\mathrm{S}_{ab}$ stessa. La matrice $\mathrm{S}_{aa}$ è l'identità.
3. **Matrice di prodotto per scalare.** Sia $a$ un intero tra 1 ed $n$ e sia $k \in \mathbb{F} \setminus \{0\}$. Si definisce allora la matrice $\mathrm{P}_a(k^{-1})$ come la matrice $\{p_{ij}\}$ con $p_{ij} = 1$ se $i = j$ e $i \neq a$, $p_{ij} = k^{-1}$ se $i = j = a$ e $p_{ij} = 0$ altrimenti. Questa matrice è la matrice che moltiplica tutti gli elementi della riga $a$-esima per uno stesso scalare $k^{-1}$. La matrice inversa di $\mathrm{P}_a(k^{-1})$ è $\mathrm{P}_a(k)$. La matrice $\mathrm{P}_a(1)$ è l'identità.
4. **Matrice di sottrazione di un multiplo di un'altra riga.** Siano $a$ e $b$ due interi distinti tra 1 ed $n$ e sia $k \in \mathbb{F}$. Si definisce la matrice $\mathrm{Z}_{ab}(-k)$ come la matrice $\{z_{ij}\}$ con $z_{ij} = 1$ per $i = j$, $z_{ij} = -k$ per $i = a$ e $j = b$, e $z_{ij} = 0$ altrimenti. Questa matrice è la matrice che alla riga $b$-esima toglie $k$ volte la riga $a$-esima. La matrice inversa di $\mathrm{Z}_{ab}(-k)$ è $\mathrm{Z}_{ab}(k)$. La matrice $\mathrm{Z}_{ab}(0)$ è l'identità.
5. **Matrici ridotte a gradini.** Una matrice $\mathrm{G} \in \mathcal{M}_{n\times m}(\mathbb{F})$ si dice ridotta a gradini se esiste un $r \in \mathbb{N}$ con $0 \leq r \leq n$ tale che, scritta $\mathrm{G} = \{g_{ij}\}$, si abbia $g_{ij} = 0$ se $i > r$ (cioè dalla $r+1$-esima riga in poi ci sono solo zeri), per ogni $i \leq r$ esista un $k(i) \in \{1, \ldots, m\}$ tale che $g_{ik(i)} \neq 0$ e per ogni $j < k(i)$ si abbia $g_{ij} = 0$. Inoltre dev'essere $k(1) < k(2) < \ldots < k(r)$. Gli elementi $g_{ik(i)}$ si chiamano pivot della matrice, e sono in numero $r$. Questo $r$ si chiama rango della matrice, e si indica con $\mathsf{rango}(\mathrm{G})$.
6. **Algoritmo di Gauss.** Data una matrice $\mathrm{M} \in \mathcal{M}_{n\times m}(\mathbb{F})$, esiste un algoritmo che la riduce a gradini tramite moltiplicazioni (a sinistra) per matrici elementari, cioè scambiando righe di M, moltiplicandole per scalari oppure sottraendo multipli di altre righe. Questo algoritmo si chiama algoritmo di Gauss, e assicura che partendo da una qualsiasi matrice M e moltiplicandola a sinistra per una quantità finita di matrici elementari (sia R il prodotto tra queste matrici elementari), allora $\mathrm{R} \cdot \mathrm{M}$ sarà ridotta a gradini.
7. **Rango di una matrice.** Abbiamo definito il rango per le matrici a gradini. In realtà il rango è definito per qualsiasi matrice $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$. Siano $v_1$, …, $v_n$ (appartenenti a $\mathbb{F}^m$) i vettori riga e siano $u_1$, …, $u_m$ (appartenenti a $\mathbb{F}^n$) i vettori colonna. Allora si definisce rango della matrice A la quantità

$$\mathsf{rango}(\mathrm{A}) := \mathsf{dim}(\mathsf{span}(v_1, \ldots, v_n)) = \mathsf{dim}(\mathsf{span}(u_1, \ldots, u_n)).$$

   In particolare, l'algoritmo di Gauss preserva il rango di una matrice, e quindi se M è una matrice e $\mathrm{G} = \mathrm{R} \cdot \mathrm{M}$ è ridotta con il metodo di Gauss, allora $\mathsf{rango}(\mathrm{G}) = \mathsf{rango}(\mathrm{M})$. Inoltre se $\mathrm{M} \in \mathcal{M}_{n\times m}(\mathbb{F})$, si ha per forza che $\mathsf{rango}(\mathrm{M}) \leq \mathsf{min}(n, m)$.

# Matrici Associate ad Applicazioni Lineari

1. **Le matrici sono lineari.** Sia $\mathbb{F}$ un campo, $\mathrm{M} \in \mathcal{M}_{n\times m}(\mathbb{F})$. Allora la funzione $f : \mathbb{F}^m \to \mathbb{F}^n$ che a $v \in \mathbb{F}^m$ associa $\mathrm{M}v \in \mathbb{F}^m$ è un'applicazione lineare. Il prodotto tra una matrice ed un vettore qui è definito pensando al vettore come se fosse una matrice colonna in $\mathcal{M}_{m\times 1}(\mathbb{F})$.
2. **Tutte le applicazioni lineari si scrivono con matrici.** Siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali di dimensione finita sullo stesso campo $\mathbb{F}$, con $\mathsf{dim}(\mathbb{V}) = m$ e $\mathsf{dim}(\mathbb{W}) = n$. Consideriamo una funzione lineare $f : \mathbb{V} \to \mathbb{W}$ e dimostriamo che si scrive sotto forma di matrice. Chiaramente possiamo supporre $\mathbb{V} = \mathbb{F}^m$ e $\mathbb{W} = \mathbb{F}^n$ (due spazi vettoriali con la stessa dimensione sono isomorfi). Sia $\{e_1, \ldots, e_m\}$ la base canonica di $\mathbb{F}^m$. Un elemento $x \in \mathbb{V}$ si scrive come
$$x = x_1 e_1 + \ldots + x_m e_m = \sum_{j=1}^{m} x_j e_j.$$
Inoltre, se $\{\widehat{e}_1, \ldots, \widehat{e}_n\}$ è la base canonica di $\mathbb{F}^n$, gli elementi $f(e_1)$, …, $f(e_m)$ si scrivono ciascuno come
$$f(e_j) = a_{1j}\widehat{e}_1 + \ldots + a_{nj}\widehat{e}_n = \sum_{i=1}^{n} a_{ij}\widehat{e}_i.$$
Dunque si ha che
$$f(x) = \sum_{j=1}^{m} x_j f(e_j) = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}x_j\widehat{e}_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{ij}x_j\right)\widehat{e}_i.$$
Quindi $f(x) = \mathrm{A}x$ dove $\mathrm{A} = \{a_{ij}\}$.
3. **Nucleo e nullità.** Sia $f : \mathbb{V} \to \mathbb{W}$ un'applicazione lineare. Si chiama nucleo di $f$, indicato con $\mathsf{ker}(f)$, l'insieme
$$\mathsf{ker}(f) := \{v \in \mathbb{V} : f(v) = 0\} \subseteq \mathbb{V}.$$
Il nucleo di $f$ è un sottospazio vettoriale di $\mathbb{V}$. La sua dimensione si chiama nullità:
$$\mathsf{null}(f) := \mathsf{dim}(\mathsf{ker}(f)).$$
4. **Immagine e rango.** Sia $f : \mathbb{V} \to \mathbb{W}$ un'applicazione lineare. Si chiama immagine di $f$, indicato con $\mathsf{img}(f)$, l'insieme
$$\mathsf{img}(f) := \{f(v) : v \in \mathbb{V}\} \subseteq \mathbb{W}.$$
L'immagine di $f$ è un sottospazio vettoriale di $\mathbb{W}$. La sua dimensione si chiama rango:
$$\mathsf{rango}(f) := \mathsf{dim}(\mathsf{img}(f)).$$
Il rango di un'applicazione è sempre pari al rango di ogni matrice associata (la matrice associata non è unica, dipende dalle scelte degli isomorfismi tra $\mathbb{V}$ e $\mathbb{F}^m$ e tra $\mathbb{W}$ e $\mathbb{F}^n$).

# Primo Teorema di Isomorfismo

1. **Proiezione canonica.** Siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali sul campo $\mathbb{F}$ e sia $f : \mathbb{V} \to \mathbb{W}$. L'insieme $\mathbb{V}/\mathsf{ker}(f)$ è un sottospazio vettoriale di $\mathbb{V}$, definito come l'insieme delle classi degli elementi di $\mathbb{V}$ tramite la relazione di equivalenza $\sim$ per cui $v_1 \sim v_2$ se e solo se $f(v_1) = f(v_2)$. La funzione

$$\pi : \mathbb{V} \to \mathbb{V}/\mathsf{ker}(f), \qquad \text{tale che} \qquad \pi(v) = \mathsf{cl}(v)$$

   è un'applicazione lineare chiamata proiezione canonica da $\mathbb{V}$ su $\mathbb{V}/\mathsf{ker}(f)$.

2. **Inclusione.** Nella stessa situazione, $\mathsf{img}(f)$ è un sottoinsieme di $\mathbb{W}$. La funzione lineare $\iota : \mathsf{img}(f) \to \mathbb{W}$ che manda un vettore $w$ in sé stesso è chiamata inclusione.

3. **Primo teorema di isomorfismo.** Siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali su $\mathbb{F}$ e sia $f : \mathbb{V} \to \mathbb{W}$ un'applicazione lineare. Allora esiste un isomorfismo

$$\psi : \mathbb{V}/\mathsf{ker}(f) \to \mathsf{img}(f)$$

   e inoltre si ha che $f(v) = \iota(\psi(\pi(v)))$ per ogni $v \in \mathbb{V}$.

4. **Descrizione dell'isomorfismo.** Definiamo l'isomorfismo $\psi$ come

$$\psi(\mathsf{cl}(v)) = f(v)$$

   per ogni $v \in \mathbb{V}$. È ben definito poiché se $\mathsf{cl}(v_1) = \mathsf{cl}(v_2)$ allora $f(v_1) = f(v_2)$. È lineare poiché $f$ è lineare, e inoltre $\mathsf{ker}(\psi) = \mathsf{ker}(f)$ e $\mathsf{img}(\psi) = \mathsf{img}(f)$, quindi è un isomorfismo.

5. **Teorema del rango e della nullità.** Dato che un isomorfismo tra due spazi vettoriali esiste quando gli spazi vettoriali hanno la stessa dimensione, otteniamo che

$$\mathsf{dim}(\mathbb{V}/\mathsf{ker}(f)) = \mathsf{dim}(\mathsf{img}(f)).$$

   Ora possiamo scrivere

$$\mathsf{dim}(\mathbb{V}/\mathsf{ker}(f)) = \mathsf{dim}(\mathbb{V}) - \mathsf{dim}(\mathsf{ker}(f))$$

   e ricordando i nomi della dimensione del nucleo e dell'immagine otteniamo

$$\mathsf{dim}(\mathbb{V}) = \mathsf{rango}(f) + \mathsf{null}(f),$$

   che si chiama teorema del rango e della nullità.

# Teorema di Rouché-Capelli

1. **Sistema lineare.** Si dice sistema lineare di $n$ equazioni in $m$ incognite un sistema del tipo
$$\begin{cases} a_{11}x_1 + \ldots + a_{1m}x_m = b_1 \\ \vdots \\ a_{n1}x_1 + \ldots + a_{nm}x_m = b_n \end{cases}$$
Possiamo considerare $x \in \mathbb{F}^m$ e $b \in \mathbb{F}^n$ due vettori, ma meglio considerarli come matrici aventi una sola colonna: $x \in \mathcal{M}_{m\times 1}(\mathbb{F})$ e $b \in \mathcal{M}_{n\times 1}(\mathbb{F})$. Detta inoltre $\mathrm{A} = \{a_{ij}\} \in \mathcal{M}_{n\times m}(\mathbb{F})$, il sistema si può riscrivere come
$$\mathrm{A}x = b.$$

2. **Soluzione del sistema.** Il sistema ha una soluzione unica se A è invertibile:
$$x = \mathrm{A}^{-1}b.$$
Se A non è invertibile, può non avere soluzioni oppure avere delle soluzioni dipendenti da un certo numero di parametri.

3. **Matrice completa del sistema.** Si definisce matrice completa del sistema, e si indica con $\mathrm{A}|b$, la matrice $n \times (m+1)$ che per prime $m$ colonne ha le colonne di A, e come $(m+1)$-esima colonna ha il vettore colonna $b$.

4. **Teorema di Rouché-Capelli.** Un sistema lineare $\mathrm{A} \cdot x = b$ ha soluzione se e solo se
$$\mathsf{rango}(\mathrm{A}) = \mathsf{rango}(\mathrm{A}|b).$$
Inoltre, la soluzione dipende da un certo numero di parametri pari a
$$m - \mathsf{rango}(\mathrm{A}),$$
e quindi la soluzione è unica se e solo se $\mathsf{rango}(\mathrm{A}) = m$.

5. **Dimostrazione.** Sia $f : \mathbb{F}^m \to \mathbb{F}^n$ la funzione che manda $x$ in $\mathrm{A}x$. Il sistema ha soluzione se e solo se $b \in \mathsf{img}(f)$, quindi se e solo se $\mathsf{img}(f) = \mathsf{img}(f) \cup \mathsf{span}(\{b\})$, quindi se e solo se
$$\mathsf{rango}(A) = \mathsf{dim}(\mathsf{img}(f)) = \mathsf{dim}(\mathsf{img}(f) \cup \mathsf{span}(\{b\}) = \mathsf{rango}(A|b).$$
Il numero di parametri è pari a $\mathsf{null}(f)$, che quindi per il teorema del rango e della nullità è
$$\mathsf{null}(f) = \mathsf{dim}(\mathbb{F}^m) - \mathsf{rango}(A) = m - \mathsf{rango}(A).$$

# Cambio di Base

1. **Matrice associata ad un'applicazione lineare rispetto ad una base.** Abbiamo visto che un'applicazione lineare $f : \mathbb{F}^m \to \mathbb{F}^n$ si scrive in modo unico come $f(v) = \mathrm{A}v$ dove $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$ è una matrice. Un'applicazione $f : \mathbb{V} \to \mathbb{W}$ (con $\mathsf{dim}(\mathbb{V}) = m$ e $\mathsf{dim}(\mathbb{W}) = n$) non ha un modo unico per essere scritta come $f(v) = \mathrm{A}v$, ma ha bisogno di essere proiettata tramite due isomorfismi. Siano $\mathbb{B}_\mathbb{V}$ e $\mathbb{B}_\mathbb{W}$ due basi di $\mathbb{V}$ e $\mathbb{W}$ rispettivamente, e siano $\psi_{\mathbb{B}_\mathbb{V}} : \mathbb{V} \to \mathbb{F}^m$ e $\psi_{\mathbb{B}_\mathbb{W}} : \mathbb{W} \to \mathbb{F}^n$ gli isomorfismi che ad un elemento $v \in \mathbb{V}$ o $w \in \mathbb{W}$ associano le sue coordinate rispetto alle basi $\mathbb{B}_\mathbb{V}$ o $\mathbb{B}_\mathbb{W}$ rispettivamente. Allora esiste un'unica matrice $\mathrm{A} \in \mathcal{M}_{n\times m}(\mathbb{F})$ tale che

$$f(v) = \psi^{-1}_{\mathbb{B}_\mathbb{W}} \left(\mathrm{A} \cdot \psi_{\mathbb{B}_\mathbb{V}}(v)\right).$$

   Le trasformazioni $\psi_{\mathbb{B}_\mathbb{V}}$ e $\psi_{\mathbb{B}_\mathbb{W}}$ possono essere viste a loro volta come matrici (rispettivamente $m \times m$ oppure $n \times n$).

2. **Matrici di cambio di base.** Sia $\mathbb{B}_1$ e $\mathbb{B}_2$ due basi di uno spazio vettoriale $\mathbb{V}$ di dimensione $m$. Allora un vettore $v \in \mathbb{V}$ ha delle coordinate $c_1(v) \in \mathbb{F}^m$ rispetto alla base $\mathbb{B}_1$ e delle coordinate $c_2(v) \in \mathbb{F}^m$ rispetto alla base $\mathbb{B}_2$. Per passare dalle coordinate $c_1$ alle coordinate $c_2$ si usa una matrice, costruita nel seguente modo: si scrivono i vettori di $\mathbb{B}_1$ in coordinate rispetto a $\mathbb{B}_2$, e si usano questi vettori come colonne della matrice T. Allora si ha che

$$\mathrm{T} \cdot c_1(v) = c_2(v)$$

   per ogni $v \in \mathbb{V}$. La matrice T si indica solitamente con $\mathrm{M}(\mathbb{B}_2\mathbb{B}_1)$, per indicare che è la matrice di cambio di base da $\mathbb{B}_1$ a $\mathbb{B}_2$. La matrice di cambio di base da $\mathbb{B}_2$ a $\mathbb{B}_1$ è $\mathrm{M}(\mathbb{B}_1\mathbb{B}_2)$ ed è l'inversa di $\mathrm{M}(\mathbb{B}_2\mathbb{B}_1)$.

3. **Tornando alla matrice associata ad un'applicazione lineare.** Sappiamo dunque che $f : \mathbb{V} \to \mathbb{W}$ può essere vista come una composizione di $\psi_{\mathbb{B}_\mathbb{V}} : \mathbb{V} \to \mathbb{F}^m$, $\mathrm{A} : \mathbb{F}^m \to \mathbb{F}^n$ e $\psi^{-1}_{\mathbb{B}_\mathbb{W}} : \mathbb{F}^n \to \mathbb{W}$. La funzione $\psi_{\mathbb{B}_\mathbb{V}}$ può essere vista come un cambio di base da $\mathbb{B}_\mathbb{V}$ alla base canonica $\mathbb{B}^m_C$ di $\mathbb{F}^m$. Allo stesso modo $\psi^{-1}_{\mathbb{B}_\mathbb{W}}$ può essere vista come un cambio di base dalla base canonica $\mathbb{B}^n_C$ di $\mathbb{F}^n$ alla base $\mathbb{B}_\mathbb{W}$. Quindi si ha che

$$f(v) = \mathrm{M}(\mathbb{B}_\mathbb{W}\mathbb{B}^n_C) \cdot \mathrm{A} \cdot \mathrm{M}(\mathbb{B}^m_C\mathbb{B}_\mathbb{V}) \cdot v.$$

4. **Caso di un endomorfismo.** Se $f$ è un endomorfismo (cioè è lineare e $\mathbb{V} = \mathbb{W}$), e $\mathbb{B} = \mathbb{B}_\mathbb{V} = \mathbb{B}_\mathbb{W}$, tutta questa formula si semplifica in

$$f(v) = \mathrm{M}^{-1} \cdot \mathrm{A} \cdot \mathrm{M} \cdot v,$$

   dove $\mathrm{M} = \mathrm{M}(\mathbb{B}^m_C\mathbb{B}_\mathbb{V})$ è la matrice che per colonne ha i vettori di $\mathbb{B}$ scritti in coordinate rispetto alla base canonica di $\mathbb{F}^m$.

# Dualità

1. **Spazio duale.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$. L'insieme delle mappe lineari da $\mathbb{V}$ in $\mathbb{F}$ si chiama spazio duale di $\mathbb{V}$, e si indica con

$$\mathbb{V}^\star := \{h : \mathbb{V} \to \mathbb{F},\ h \text{ lineare}\}.$$

   È uno spazio vettoriale su $\mathbb{F}$, con $\mathsf{dim}(\mathbb{V}^\star) = \mathsf{dim}(\mathbb{V})$.

2. **Base duale.** Sia $\mathbb{V}$ con dimensione finita pari a $n$, e sia $\{e_1, \ldots, e_n\}$ una base di $\mathbb{V}$. Allora la base duale di $\{e_1, \ldots, e_n\}$, base di $\mathbb{V}^\star$, è $\{\eta_1, \ldots, \eta_n\}$, dove $\eta_i(e_j) := \delta_{ij}$ (delta di Kronecker). È ben definita poiché una qualsiasi funzione lineare $h : \mathbb{V} \to \mathbb{F}$ è univocamente determinata una volta noti i valori $h(e_1)$, …, $h(e_n)$.

3. **Spazio biduale.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$, sia $\mathbb{V}^\star$ il suo spazio duale. Si definisce spazio biduale di $\mathbb{V}$ il duale di $\mathbb{V}^\star$, indicato con $(\mathbb{V}^\star)^\star$.

4. **Isomorfismo tra uno spazio e il suo biduale.** Sia $\mathbb{V}$ con $\mathsf{dim}(\mathbb{V})$ finita. Allora esiste un isomorfismo canonico tra $\mathbb{V}$ e $(\mathbb{V}^\star)^\star$ (che non dipende da nessuna base). Esistono isomorfismi tra $\mathbb{V}$ e $\mathbb{V}^\star$ oppure tra $\mathbb{V}^\star$ e $(\mathbb{V}^\star)^\star$, ma nessuno di questi è canonico (cioè ognuno di questi dipende da una certa base fissata). Sia $\psi : \mathbb{V} \to (\mathbb{V}^\star)^\star$ tale che $\psi(v)(h) = h(v)$ per ogni $h \in \mathbb{V}^\star$. Infatti $\psi(v)$ è una mappa lineare da $\mathbb{V}^\star$ in $\mathbb{F}$, quindi facendo così si definisce il suo valore per ogni $h \in \mathbb{V}^\star$. Questa mappa è ben definita, lineare e iniettiva, e quindi siccome $\mathsf{dim}(\mathbb{V})$ è finita, è anche surgettiva.

5. **Sottospazio ortogonale.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ di dimensione finita e sia $\mathbb{U}$ un suo sottospazio. Allora si definisce

$$\mathbb{U}^\perp := \{h \in \mathbb{V}^\star : h(w) = 0\ \forall w \in \mathbb{U}\}.$$

   Si ha che $\mathbb{U}^\perp$ è un sottospazio vettoriale di $\mathbb{V}^\star$. Inoltre $\psi : \mathbb{V} \to (\mathbb{V}^\star)^\star$ manda il sottospazio $\mathbb{U} \subseteq \mathbb{V}$ nel sottospazio $(\mathbb{U}^\perp)^\perp \subseteq (\mathbb{V}^\star)^\star$ e si ha che

$$\mathsf{dim}(\mathbb{U}) + \mathsf{dim}(\mathbb{U}^\perp) = \mathsf{dim}(\mathbb{V})$$

   per ogni $\mathbb{U}$ sottospazio vettoriale di $\mathbb{V}$.

# Potenza Esterna

1. **Forme.** Sia $\mathbb{V}$ uno spazio vettoriale sul campo $\mathbb{F}$ e sia $k \geq 1$ un intero. Si dice $k$-forma una mappa da $\mathbb{V}^k$ in $\mathbb{F}$. Una $k$-forma si dice multilineare se è lineare in ogni sua variabile, cioè fissando $k-1$ variabili come parametri, è una funzione lineare da $\mathbb{V}$ in $\mathbb{F}$. Una $k$-forma si dice alternata se è nulla ogniqualvolta due delle variabili sono uguali.
2. **Potenza esterna.** Si chiama $k$-potenza esterna di $\mathbb{V}^\star$ l'insieme delle $k$-forme multilineari ed alternate da $\mathbb{V}$ in $\mathbb{F}$. In simboli si indica con $\Lambda^k(\mathbb{V}^\star)$. È uno spazio vettoriale sul campo $\mathbb{F}$.
3. **Spazio duale.** Per $k = 1$ si ha che $\Lambda^1(\mathbb{V}^\star) = \mathbb{V}^\star$.
4. **Conseguenza dell'alternanza.** Sia $h \in \Lambda^k(\mathbb{V}^\star)$. Allora se scambio di posto due vettori il segno di $h$ cambia:
$$h(\ldots, v_i, \ldots, v_j, \ldots) = -h(\ldots, v_j, \ldots, v_i, \ldots).$$
Questo segue dall'alternanza e dalla multilinearità, e se $\mathsf{char}(\mathbb{F}) \neq 2$ è equivalente all'alternanza.
5. **Lineare indipendenza.** Sia $h \in \Lambda^k(\mathbb{V}^\star)$. Allora se $v_1$, …, $v_k$ sono linearmente dipendenti si ha che
$$h(v_1, \ldots, v_k) = 0.$$
Infatti se sono linearmente dipendenti ce n'è uno che si scrive come combinazione lineare degli altri, e poi per multilinearità ed alternanza si nota che deve fare 0.
6. **Potenze esterne con $k$ troppo elevato.** Per $k > \mathsf{dim}(\mathbb{V})$ si ha che $\Lambda^k(\mathbb{V}^\star) = \{0\}$. Infatti non esistono $k$ vettori di $\mathbb{V}^k$ linearmente indipendenti, e quindi per alternanza la funzione si annulla. Dunque per $k > \mathsf{dim}(\mathbb{V})$ si ha che $\mathsf{dim}(\Lambda^k(\mathbb{V}^\star)) = 0$.
7. **Base della potenza esterna.** Sia $\mathbb{B} = \{e_1, \ldots, e_n\}$ una base di $\mathbb{V}$. Allora un insieme di $k$ vettori, con $k \leq n$, si può scrivere come
$$v_j = a_{j1}e_1 + \ldots + a_{jn}e_n$$
per $j$ da 1 a $k$. Quindi per multilinearità ed alternanza una volta fissato il valore di $h(e_{i_1}, \ldots, e_{i_k})$ al variare di $i_1 < i_2 < \ldots < i_k$ in $\{1, \ldots, n\}$, è stabilito univocamente il valore di $h(v_1, \ldots, v_k)$. Quindi questa è una base di $\Lambda^k(\mathbb{V}^\star)$, e dunque
$$\mathsf{dim}(\Lambda^k(\mathbb{V}^\star)) = \binom{n}{k},$$
dove quest'ultimo è un coefficiente binomiale, definito come il numero di modi di scegliere $k$ elementi da un insieme di $n$.

# Mappe Indotte e Endomorfismi

1. **Mappa indotta sullo spazio duale.** Sia $\varphi : \mathbb{V} \to \mathbb{W}$ una mappa lineare. Si definisce mappa indotta da $\varphi$ sullo spazio duale la mappa $\varphi^\star : \mathbb{W}^\star \to \mathbb{V}^\star$ che ad ogni $h \in \mathbb{W}^\star$ associa la composizione di $h$ con $\varphi$, e quindi per ogni vettore $v \in \mathbb{V}$ si ha che
$$\varphi^\star(h(v)) = h(\varphi(v)).$$

2. **Mappa indotta sulla potenza esterna.** Sia $\varphi : \mathbb{V} \to \mathbb{W}$ una mappa lineare. Si definisce mappa indotta da $\varphi$ su $\Lambda^k$ la mappa $\varphi^\star : \Lambda^k(\mathbb{W}^\star) \to \Lambda^k(\mathbb{V}^\star)$ che associa ad ogni $h \in \Lambda^k(\mathbb{W}^\star)$ la composizione di $h$ con $\varphi$, e quindi per ogni $k$ vettori $v_1$, …, $v_k$ si ha che
$$\varphi(h(v_1, \dots, v_k)) = h(\varphi(v_1), \dots, \varphi(v_k)).$$
Questa è una generalizzazione della mappa indotta sul duale.

3. **Mappa indotta della composizione.** Siano $\mathbb{V}_1$, $\mathbb{V}_2$ e $\mathbb{V}_3$ tre spazi vettoriali sullo stesso campo $\mathbb{F}$, e siano $\varphi_{12} : \mathbb{V}_1 \to \mathbb{V}_2$ e $\varphi_{23} : \mathbb{V}_2 \to \mathbb{V}_3$ due mappe lineari. Allora la composizione di queste due mappe, $\varphi_{23} \circ \varphi_{12}$, è una funzione $\varphi_{13} : \mathbb{V}_1 \to \mathbb{V}_3$. La mappa indotta da $\varphi_{13}$ è pari a
$$\varphi_{13}^\star = (\varphi_{23} \circ \varphi_{12})^\star = \varphi_{12}^\star \circ \varphi_{23}^\star.$$

4. **Endomorfismo.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$, e sia $f : \mathbb{V} \to \mathbb{V}$ lineare. Allora $f$ si chiama endomorfismo di $\mathbb{V}$.

5. **Endomorfismi su spazi di dimensione 1.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ con $\mathsf{dim}(\mathbb{V}) = 1$. Allora dato un endomorfismo $f$ di $\mathbb{V}$ esiste $k \in \mathbb{F}$ tale che $f(v) = kv$ per ogni $v \in \mathbb{V}$. Infatti una volta fissato il valore di $f$ in un vettore $v_1 \neq 0$, la mappa è univocamente determinata.

6. **Mappe indotte dagli endomorfismi.** Sia $f : \mathbb{V} \to \mathbb{V}$ un endomorfismo. Allora la mappa indotta da $f$ su $\Lambda^k$ è un endomorfismo di $\Lambda^k(\mathbb{V}^\star)$.

# Determinanti

1. **Isomorfismo tra potenza esterna e campo.** Sia $\mathbb{V}$ uno spazio vettoriale di dimensione $n$ sul campo $\mathbb{F}$. Allora $\Lambda^n(\mathbb{V}^\star)$ ha dimensione 1, quindi esiste un isomorfismo $\psi : \Lambda^n(\mathbb{V}^\star) \to \mathbb{F}$. Consideriamo una base $\mathbb{B} = \{e_1, \dots, e_n\}$ di $\mathbb{V}$. Allora dati $n$ vettori $\{v_1, \dots, v_n\}$, questi si scrivono come

$$v_j = a_{j1}e_1 + \ldots + a_{jn}e_n.$$

Preso $h \in \Lambda^n(\mathbb{V}^\star)$, si ha che per multilinearità e per alternanza

$$h(v_1, \dots, v_n) = \sum_{\sigma \in \mathfrak{S}_n} \left( \mathsf{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i\sigma(i)} \right) h(e_1, \dots, e_n).$$

Quindi la mappa $\psi$ che ad $h \in \Lambda^n(\mathbb{V}^\star)$ associa il valore di $h(e_1, \dots, e_n)$ è un isomorfismo.

2. **Determinante di una matrice.** Data una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ con $\mathrm{A} = \{a_{ij}\}$, si definisce determinante di A il valore

$$\mathsf{det}(\mathrm{A}) := \sum_{\sigma \in \mathfrak{S}_n} \left( \mathsf{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i\sigma(i)} \right).$$

Il determinante ha tutte le proprietà delle $n$-forme multilineari alternate, in particolare se le righe o le colonne della matrice A sono linearmente dipendenti il determinante si annulla. In effetti A è invertibile se e solo se $\mathsf{det}(\mathrm{A}) \neq 0$.

3. **Determinante di matrici diagonali e triangolari.** Sia $\mathrm{T} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice diagonale, triangolare superiore oppure triangolare inferiore, e sia $\mathrm{T} = \{t_{ij}\}$. Allora

$$\mathsf{det}(\mathrm{T}) = t_{11} \cdot t_{22} \cdot \ldots \cdot t_{nn}.$$

4. **Determinante della matrice trasposta.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$. Allora

$$\mathsf{det}(\mathrm{A}^t) = \mathsf{det}(\mathrm{A}).$$

Questo deriva dal fatto che ogni permutazione $\sigma \in \mathfrak{S}_n$ ha una permutazione inversa.

5. **Determinante di una matrice $2 \times 2$.** Si ha che

$$\mathsf{det} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

6. **Regola di Sarrus per il determinante di una matrice $3 \times 3$.** Si ha che

$$\mathsf{det} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{array}{l} +a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} \end{array}.$$

# Teorema di Binet

1. **Determinante di un endomorfismo.** Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{F}$ con $\mathsf{dim}(\mathbb{V}) = n$, e sia $f$ un endomorfismo di $\mathbb{V}$. Questo endomorfismo induce una mappa $f^\star : \Lambda^n(\mathbb{V}^\star) \to \Lambda^n(\mathbb{V}^\star)$, che è quindi un endomorfismo di $\Lambda^n(\mathbb{V}^\star)$, che è uno spazio vettoriale di dimensione 1, quindi esiste un certo $k \in \mathbb{F}$ tale che $f^\star(h) = kh$ per ogni $h \in \Lambda^n(\mathbb{V}^\star)$. Si definisce il determinante di $f$ pari a

$$\mathsf{det}(f) := k = \frac{f^\star(h)}{h}.$$

   Questo è sempre pari al determinante della matrice associata a $f$, indipendentemente dalla base scelta.

2. **Teorema di Binet.** Siano A e B due matrici $n \times n$ sul campo $\mathbb{F}$. Allora si ha che

$$\mathsf{det}(\mathrm{A})\mathsf{det}(\mathrm{B}) = \mathsf{det}(\mathrm{AB}).$$

3. **Dimostrazione.** Se consideriamo i due endomorfismi $f_\mathrm{A} : \mathbb{F}^n \to \mathbb{F}^n$ e $f_\mathrm{B} : \mathbb{F}^n \to \mathbb{F}^n$ che hanno come matrici associate rispetto alla base canonica rispettivamente A e B, si ha che $f_A^\star(h) = \mathsf{det}(\mathrm{A})h$ e $f_B^\star(h) = \mathsf{det}(\mathrm{B})h$, quindi per la composizione si ha che

$$\mathsf{det}(\mathrm{A})\mathsf{det}(\mathrm{B})h = (f_\mathrm{B}^\star \circ f_\mathrm{A}^\star)(h) = (f_\mathrm{A} \circ f_\mathrm{B})^\star = \mathsf{det}(\mathrm{AB})h.$$

4. **Determinante della matrice inversa.** Dal teorema di Binet segue come corollario che, se A è invertibile,

$$\mathsf{det}(\mathrm{A}^{-1}) = \mathsf{det}(\mathrm{A})^{-1}.$$

5. **Gruppo lineare.** All'interno di $\mathcal{M}_{n\times n}(\mathbb{F})$ esiste un sottoinsieme $\mathbb{GL}_n(\mathbb{F})$ detto $n$-esimo gruppo lineare, formato da tutte e sole le matrici invertibili:

$$\mathbb{GL}_n(\mathbb{F}) := \{\mathrm{M} \in \mathcal{M}_{n\times n}(\mathbb{F}) : \mathsf{det}(\mathrm{M}) \neq 0\}.$$

   Questo è un gruppo rispetto al prodotto di matrici. Inoltre, considerando che $\mathbb{F} \setminus \{0\}$ è un gruppo rispetto al prodotto, si può riformulare il teorema di Binet dicendo che la funzione $\mathsf{det} : \mathbb{GL}_n(\mathbb{F}) \to \mathbb{F} \setminus \{0\}$ è un omomorfismo di gruppi, cioè preserva la struttura di gruppo, dato che $\mathsf{det}(\mathrm{AB}) = \mathsf{det}(\mathrm{A})\mathsf{det}(\mathrm{B})$.

# Laplace e Cramer

1. **Aggiunti di una matrice.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice. Consideriamo la matrice $\mathrm{A}_{ij} \in \mathcal{M}_{(n-1)\times(n-1)}(\mathbb{F})$ a cui sono stati tolte la riga $i$-esima e la colonna $j$-esima. Definiamo aggiunto il valore

$$\overline{a}_{ij} := (-1)^{i+j} \cdot \mathsf{det}(\mathrm{A}_{ij}).$$

   La matrice $n \times n$ formata dagli aggiunti si dice matrice aggiunta di A, e viene indicata con $\bar{\mathrm{A}} = \{\overline{a}_{ij}\}$.

2. **Teorema di Laplace.** Sia $\mathrm{A} = \{a_{ij}\}$ una matrice $n \times n$. Allora si ha che

$$\sum_{i=1}^{n} a_{ij}\overline{a}_{ij} = \mathsf{det}(\mathrm{A}) = \sum_{j=1}^{n} a_{ij}\overline{a}_{ij},$$

   dove quindi la somma a sinistra è intesa fissando la colonna $j$-esima, e la somma a destra è intesa fissando la riga $i$-esima.

3. **Formula dell'inversa.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice invertibile. Allora si ha che

$$\mathrm{A}^{-1} = \frac{1}{\mathsf{det}(\mathrm{A})}\bar{\mathrm{A}}^{t}.$$

4. **Regola di Cramer.** Consideriamo una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ invertibile e $b \in \mathbb{F}^n$. Allora il sistema

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

   ha una soluzione unica. La soluzione si può trovare esplicitamente: sia $\mathrm{A}_j$ la matrice ottenuta sostituendo al posto della $j$-esima colonna di A il vettore colonna $b$. Allora si ha che

$$x_1 = \frac{\mathsf{det}(\mathrm{A}_1)}{\mathsf{det}(\mathrm{A})}, \ldots, x_n = \frac{\mathsf{det}(\mathrm{A}_n)}{\mathsf{det}(\mathrm{A})}.$$

   Le matrici $\mathrm{A}_j$ qui non hanno nulla a che fare con le matrici $\mathrm{A}_{ij}$ che servivano per calcolare gli aggiunti prima.

# Polinomio Caratteristico

1. **Polinomio caratteristico di una matrice.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$. Allora si dice polinomio caratteristico di A il polinomio in $\mathbb{F}[\lambda]$ dato da

$$p_{\mathrm{A}}(\lambda) := \mathsf{det}(\mathrm{A} - \lambda\mathrm{Id}).$$

   Questo polinomio ha sempre grado $n$, e il suo coefficiente di testa è $(-1)^n$, il termine noto è $\mathsf{det}(\mathrm{A})$ e il coefficiente di grado $n-1$ è la traccia della matrice A, scritta $\mathsf{tr}(\mathrm{A})$ e definita come la somma dei numeri sulla diagonale (cioè $a_{11} + \ldots + a_{nn}$), mentre il coefficiente di grado 1 è la traccia di $\bar{\mathrm{A}}$. In altre parole

$$p_{\mathrm{A}}(\lambda) = (-\lambda)^n + \mathsf{tr}(\mathrm{A})(-\lambda)^{n-1} + \ldots + \mathsf{tr}(\bar{\mathrm{A}})(-\lambda) + \mathsf{det}(\mathrm{A}).$$

2. **Autovalori e autovettori.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice, $\lambda \in \mathbb{F}$ e $v \in \mathbb{F}^n$ con $v \neq 0$. Allora se

$$\mathrm{A}v = \lambda v,$$

   $\lambda$ si dice autovalore di A e $v$ si dice autovettore di A associato all'autovalore $\lambda$. Gli autovalori di una matrice A sono radici del polinomio caratteristico.

3. **Autospazi.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice e sia $\lambda$ un suo autovalore. Allora l'insieme dei $v \in \mathbb{F}^n$ tali che

$$\mathrm{A}v = \lambda v$$

   (cioè l'insieme degli autovettori associati a $\lambda$, con in più $v = 0$) si dice autospazio associato a $\lambda$. Si ha che l'autospazio associato a $\lambda$ è $\mathsf{ker}(\mathrm{A} - \lambda\mathrm{Id})$.

4. **Molteplicità di un autovalore.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice e sia $\lambda$ un suo autovalore. Si dice molteplicità algebrica di $\lambda$ la molteplicità di $\lambda$ pensato come radice del polinomio caratteristico. La molteplicità algebrica si indica con $\mathsf{ma}(\lambda)$. Inoltre si definisce la molteplicità geometrica di $\lambda$ come la dimensione dell'autospazio:

$$\mathsf{mg}(\lambda) := \mathsf{dim}(\mathsf{ker}(\mathrm{A} - \lambda\mathrm{Id})).$$

5. **Relazione tra le molteplicità.** Sia $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ una matrice e $\lambda$ un suo autovalore. Allora si ha che

$$1 \leq \mathsf{mg}(\lambda) \leq \mathsf{ma}(\lambda).$$

   Infatti che sia $1 \leq \mathsf{mg}(\lambda)$ è banale visto che $\lambda$ è un autovalore. Che $\mathsf{mg}(\lambda) \leq \mathsf{ma}(\lambda)$ segue dal fatto che si può considerare una base dell'autospazio di $\lambda$ e completarla con Steinitz ad una base di $\mathbb{F}^n$, e si vede banalmente che ci sono almeno $\mathsf{mg}(\lambda)$ radici pari a $\lambda$ nel polinomio caratteristico della matrice A vista dopo averla cambiata di base.

# Similarità e Diagonalizzazione

1. **Similarità tra matrici.** Due matrici A e B in $\mathcal{M}_{n\times n}(\mathbb{F})$ si dicono simili se esiste $\mathrm{M} \in \mathbb{GL}_n(\mathbb{F})$, cioè invertibile, tale che
$$\mathrm{MA} = \mathrm{BM}.$$
Si dimostra che la similarità $\sim$ è una relazione di equivalenza su $\mathcal{M}_{n\times n}(\mathbb{F})$.
2. **Similarità e polinomio caratteristico.** Se due matrici A e B sono simili, allora $p_{\mathrm{A}}(\lambda) = p_{\mathrm{B}}(\lambda)$. Infatti
$$\mathrm{M} \cdot (\mathrm{A} - \lambda\mathrm{Id}) = (\mathrm{B} - \lambda\mathrm{Id}) \cdot \mathrm{M},$$
da cui $\mathsf{det}(\mathrm{A} - \lambda\mathrm{Id}) = \mathsf{det}(\mathrm{B} - \lambda\mathrm{Id})$.
3. **Diagonalizzabilità.** Una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ si dice diagonalizzabile se è simile ad una matrice diagonale, cioè se esistono D diagonale e M invertibile tali che
$$\mathrm{A} = \mathrm{M}^{-1} \cdot \mathrm{D} \cdot \mathrm{M}.$$
Una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ è diagonalizzabile se e solo se esiste una base $\mathbb{B}$ di $\mathbb{F}^n$ composta da autovettori di A. Infatti poi basterebbe prendere come M la matrice di cambio di base dalla canonica a $\mathbb{B}$ e si avrebbe che
$$\mathrm{A} = \mathrm{M}^{-1} \cdot \mathrm{D} \cdot \mathrm{M}$$
con D matrice diagonale.
4. **Criterio di diagonalizzabilità.** Una matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ è diagonalizzabile se e solo se il suo polinomio caratteristico ha $n$ radici (questa condizione è superflua se $\mathbb{F}$ è algebricamente chiuso) e per ogni autovalore $\lambda$ si ha che $\mathsf{ma}(\lambda) = \mathsf{mg}(\lambda)$. Infatti l'insieme
$$\mathsf{ker}(\mathrm{A} - \lambda_1\mathrm{Id}) \oplus \ldots \oplus \mathsf{ker}(\mathrm{A} - \lambda_k\mathrm{Id}),$$
dove $\lambda_1, \ldots, \lambda_k$ sono i $k$ autovalori di A, ha come dimensione
$$\mathsf{mg}(\lambda_1) + \ldots + \mathsf{mg}(\lambda_k) \leq n,$$
e per essere uguale a $n$ (e cioè per essere vero che esista una base di $\mathbb{F}^n$ formata da autovettori di A) tutte le molteplicità geometriche devono coincidere con le rispettive molteplicità algebriche. Il fatto che la somma dei nuclei sia una somma diretta non è banale, e si dimostra per induzione.
5. **Autovalori distinti.** Se $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ ha $n$ autovalori distinti, è diagonalizzabile.
6. **Diagonalizzabilità di matrici nihilpotenti.** Le matrici nihilpotenti $\mathrm{N} \in \mathcal{M}_{n\times n}(\mathbb{F})$ hanno tutte polinomio caratteristico pari a
$$p_{\mathrm{N}}(\lambda) = (-\lambda)^n.$$
Una matrice nihilpotente inoltre è diagonalizzabile se e solo se è la matrice nulla: dev'essere $\mathsf{ker}(\mathrm{N}) = \mathbb{F}^n$ e quindi $\mathsf{rango}(\mathrm{N}) = 0$.

# Forma Canonica di Jordan

1. **Blocchi di Jordan e matrici di Jordan.** Si dice blocco di Jordan una matrice $\mathrm{B} \in \mathcal{M}_{r\times r}(\mathbb{F})$ con $b_{ij} = \lambda$ per $i = j$ e $b_{ij} = 1$ per $j = i + 1$ e $b_{ij} = 0$ altrimenti. Una matrice formata da blocchi di Jordan in diagonale e 0 altrove si dice matrice di Jordan.
2. **Teorema di Jordan.** Ogni matrice $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ è jordanizzabile, cioè esiste una matrice $\mathrm{J} \in \mathcal{M}_{n\times n}(\mathbb{F})$ di Jordan tale che A e J sono simili. La J si chiama forma canonica di Jordan di A. La matrice M tale che
$$\mathrm{A} = \mathrm{M}^{-1} \cdot \mathrm{J} \cdot \mathrm{M}$$
è la matrice di cambio di base dalla canonica ad una certa base $\mathbb{B}$, detta base di Jordan della matrice A.
3. **Jordanizzazione di matrici nihilpotenti.** Sia N una matrice nihilpotente. Allora tutti gli autovalori sono nulli, quindi ci sono solo blocchi di Jordan con 0 sulla diagonale. Il numero di blocchi è $\mathsf{dim}(\mathsf{ker}(\mathrm{N}))$, il numero di blocchi di dimensione almeno 2 è $\mathsf{dim}(\mathsf{ker}(\mathrm{N}^2)) - \mathsf{dim}(\mathsf{ker}(\mathrm{N}))$ e così via il numero di blocchi di dimensione almeno $j$ è $\mathsf{dim}(\mathsf{ker}(\mathrm{N}^j)) - \mathsf{dim}(\mathsf{ker}(\mathrm{N}^{j-1}))$. Quindi il numero di blocchi $j \times j$ è
$$-\mathsf{dim}(\mathsf{ker}(\mathrm{N}^{j-1})) + 2 \cdot \mathsf{dim}(\mathsf{ker}(\mathrm{N}^j)) - \mathsf{dim}(\mathsf{ker}(\mathrm{N}^{j+1})).$$
4. **Jordanizzazione di altre matrici.** Per le altre matrici $\mathrm{A} \in \mathcal{M}_{n\times n}(\mathbb{F})$ funziona analogamente. Dato un autovalore $\lambda$, il numero di blocchi di Jordan $j \times j$ con $\lambda$ sulla diagonale è
$$-\mathsf{dim}(\mathsf{ker}((\mathrm{A} - \lambda\mathrm{Id})^{j-1})) + 2 \cdot \mathsf{dim}(\mathsf{ker}((\mathrm{A} - \lambda\mathrm{Id})^j)) - \mathsf{dim}(\mathsf{ker}((\mathrm{A} - \lambda\mathrm{Id})^{j+1})).$$
5. **Trovare la base di Jordan.** Per trovare la base di Jordan bisogna trovare degli elementi per cui l'immagine della trasformazione sia quella desiderata.

# Spazi Affini

1. **Definizione via spostamento.** Sia $\mathbb{F}$ un campo e $\mathbb{V}$ uno spzio vettoriale su $\mathbb{F}$. Uno spazio affine $\mathbb{A}$ associato a $\mathbb{V}$ è un insieme dotato di una mappa $\varphi : \mathbb{A} \times \mathbb{A} \to \mathbb{V}$ tale che $\mathbb{A} \neq \emptyset$ e per ogni $P \in \mathbb{A}$ e ogni $v \in \mathbb{V}$ esista un unico $Q \in \mathbb{A}$ tale che $\varphi(P, Q) = v$; e inoltre per ogni $P$, $Q$ ed $R$ in $\mathbb{A}$ si abbia che
$$\varphi(P, Q) + \varphi(Q, R) + \varphi(R, P) = 0.$$
2. **Conseguenze.** Si ha che $\varphi(P, Q) = 0$ se e solo se $P = Q$, inoltre $\varphi(P, Q) + \varphi(Q, P) = 0$ per ogni $P$ e $Q$ in $\mathbb{A}$, e $\varphi(P, Q) = \varphi(R, S)$ se e solo se $\varphi(P, R) = \varphi(Q, S)$.
3. **Definizione via traslazione.** Sia $\mathbb{F}$ un campo e $\mathbb{V}$ uno spzio vettoriale su $\mathbb{F}$. Uno spazio affine $\mathbb{A}$ associato a $\mathbb{V}$ è un insieme dotato di una mappa $t : \mathbb{V} \times \mathbb{A} \to \mathbb{A}$ tale che $\mathbb{A} \neq \emptyset$ e per ogni $P \in \mathbb{A}$ e per ogni $Q \in \mathbb{A}$ esista un unico $v \in \mathbb{V}$ tale che $t(v, P) = Q$; e inoltre per ogni $P \in \mathbb{A}$ e per ogni $u$ e $v$ in $\mathbb{V}$ si ha che
$$t(u + v, P) = t(u, t(v, P)).$$
4. **Conseguenze.** Si ha che $t(v, P) = Q$ se e solo se $t(-v, Q) = P$. Inoltre le due definizioni di spazio affine sono equivalenti, ponendo $t(v, P) = Q$ se e solo se $\varphi(P, Q) = v$.
5. **Spazio vettoriale come spazio affine.** Prendendo $\mathbb{A} = \mathbb{V}$, $\varphi(u, v) = v - u$ e $t(u, v) = u + v$ si ottiene uno spazio affine associato a $\mathbb{V}$.
6. **Mappe affini (via spostamento).** Sia $\mathbb{F}$ un campo e siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali su $\mathbb{F}$, e siano $\mathbb{A}(\mathbb{V})$ e $\mathbb{A}(\mathbb{W})$ due spazi affini associati a $\mathbb{V}$ e a $\mathbb{W}$ rispettivamente. Allora se $\varphi_{\mathbb{V}}$ e $\varphi_{\mathbb{W}}$ sono le funzioni che definiscono $\mathbb{A}(\mathbb{V})$ e $\mathbb{A}(\mathbb{W})$, una funzione $F : \mathbb{A}(\mathbb{V}) \to \mathbb{A}(\mathbb{W})$ si dice mappa affine se esiste una funzione $f : \mathbb{V} \to \mathbb{W}$ lineare tale che
$$f(\varphi_{\mathbb{V}}(P, Q)) = \varphi_{\mathbb{W}}(F(P), F(Q)).$$
7. **Mappe affini (via traslazione).** Sia $\mathbb{F}$ un campo e siano $\mathbb{V}$ e $\mathbb{W}$ due spazi vettoriali su $\mathbb{F}$, e siano $\mathbb{A}(\mathbb{V})$ e $\mathbb{A}(\mathbb{W})$ due spazi affini associati a $\mathbb{V}$ e a $\mathbb{W}$ rispettivamente. Allora se $t_{\mathbb{V}}$ e $t_{\mathbb{W}}$ sono le funzioni che definiscono $\mathbb{A}(\mathbb{V})$ e $\mathbb{A}(\mathbb{W})$, una funzione $F : \mathbb{A}(\mathbb{V}) \to \mathbb{A}(\mathbb{W})$ si dice mappa affine se esiste una funzione $f : \mathbb{V} \to \mathbb{W}$ lineare tale che
$$t_{\mathbb{W}}(f(u), F(P)) = F(t_{\mathbb{V}}(u, P)).$$
8. **Spazio affine canonico.** Preso $\mathbb{V} = \mathbb{F}^n$, lo spazio affine associato a $\mathbb{V}$ si indica solitamente con $\mathbb{A}^n(\mathbb{F})$.

# Sottospazi Affini

1. **Sottospazio affine.** Sia $\mathbb{A}$ uno spazio affine associato ad uno spazio vettoriale $\mathbb{V}$ sul campo $\mathbb{F}$. Si definisce sottospazio affine un insieme del tipo

$$\{P + w : w \in \mathbb{U}\} \subseteq \mathbb{A}$$

dove $\mathbb{U} \subseteq \mathbb{V}$ è un sottospazio vettoriale detto giacitura del sottospazio affine, e $P \in \mathbb{A}$ è un punto. Questo sottospazio affine si indica solitamente con $(P + \mathbb{U})$, ed è uno spazio affine associato allo spazio vettoriale $\mathbb{U}$.

2. **Scambio.** Siano $P$ e $Q$ due punti di $\mathbb{A}$ e sia $\mathbb{U}$ un sottospazio di $\mathbb{V}$. Allora

$$P \in (Q + \mathbb{U}) \quad \Leftrightarrow \quad Q \in (P + \mathbb{U}).$$

3. **Intersezione.** Siano $P$ e $Q$ due punti di $\mathbb{A}$ e siano $\mathbb{U}$ e $\mathbb{W}$ due sottospazi di $\mathbb{V}$. Allora

$$(P + \mathbb{U}) \cap (Q + \mathbb{W}) \neq \emptyset \quad \Leftrightarrow \quad \varphi(P, Q) \in \mathbb{U} + \mathbb{W}.$$

Inoltre se $(P + \mathbb{U}) \cap (Q + \mathbb{W}) \neq \emptyset$ allora è un sottospazio affine. Infatti deve esistere un punto $R \in (P + \mathbb{U}) \cap (Q + \mathbb{W})$, e si ha che

$$(P + \mathbb{U}) \cap (Q + \mathbb{W}) = (R + (\mathbb{U} \cap \mathbb{W})).$$

4. **Somma.** Siano $P$ e $Q$ due punti di $\mathbb{A}$ e siano $\mathbb{U}$ e $\mathbb{W}$ due sottospazi di $\mathbb{V}$. Allora il più piccolo sottospazio affine che contiene sia $(P + \mathbb{U})$ sia $(Q + \mathbb{W})$, che indicheremo con

$$(P + \mathbb{U}) + (Q + \mathbb{W}),$$

ha giacitura pari a $\mathbb{U} + \mathbb{W}$ se $(P + \mathbb{U}) \cap (Q + \mathbb{W}) \neq \emptyset$; mentre invece ha giaciura pari a

$$\mathbb{U} + \mathbb{W} + \mathsf{span}(\varphi(P, Q))$$

nel caso in cui $(P + \mathbb{U}) \cap (Q + \mathbb{W}) = \emptyset$.

5. **Dimensione di uno spazio affine.** Si definisce la dimensione di uno spazio affine come pari alla dimensione dello spazio vettoriale a cui è associato. Se $(P + \mathbb{U})$ e $(Q + \mathbb{W})$ sono due sottospazi affini, e $(P + \mathbb{U}) \cap (Q + \mathbb{W}) \neq \emptyset$, si ha che

$$\mathsf{dim}(P + \mathbb{U}) + \mathsf{dim}(Q + \mathbb{W}) = \mathsf{dim}((P + \mathbb{U}) + (Q + \mathbb{W})) + \mathsf{dim}((P + \mathbb{U}) \cap (Q + \mathbb{W})).$$

Se invece $(P + \mathbb{U}) \cap (Q + \mathbb{W}) = \emptyset$, si ha che

$$\mathsf{dim}(P + \mathbb{U}) + \mathsf{dim}(Q + \mathbb{W}) = \mathsf{dim}((P + \mathbb{U}) + (Q + \mathbb{W})) - 1.$$

Per avere una formula sola, si può porre per definizione $\mathsf{dim}(\emptyset) = -1$.

# Trasformazioni Affini

1. **Trasformazione affine e affinità.** Una mappa affine $F : \mathbb{A}(\mathbb{V}) \to \mathbb{A}(\mathbb{W})$ si dice trasformazione affine se $\mathbb{V} = \mathbb{W}$. Si dice affinità se è bigettiva. Praticamente, le mappe affini sono l'equivalente affine delle applicazioni lineari, le trasformazioni affini degli endomorfismi, e le affinità degli automorfismi.
2. **Punti fissi.** Un punto $P \in \mathbb{A}(\mathbb{V})$ si dice punto fisso della trasformazione affine $F : \mathbb{A}(\mathbb{V}) \to \mathbb{A}(\mathbb{V})$ se $F(P) = P$.
3. **Trasformazioni del piano.** Le possibili trasformazioni del piano sono: traslazioni, riflessioni, proiezioni, dilatazioni, contrazioni, rotazioni, e trasformazioni di tipo shear 2d.
4. **Trasformazioni dello spazio.** Le possibili trasformazioni dello spazio sono: traslazioni, riflessioni, proiezioni, dilatazioni, contrazioni, rotazioni, trasformazioni di tipo shear 2d e trasformazioni di tipo shear 3d.
5. **Gruppo delle affinità.** L'insieme di tutte le affinità di uno spazio affine $\mathbb{A}$ è un gruppo rispetto alla composizione. La geometria affine studia le proprietà conservate dal gruppo delle affinità, così come la geometria lineare studia le proprietà conservate dal gruppo lineare (gruppo degli automorfismi di uno spazio vettoriale).
6. **Proprietà conservate dalle affinità.** L'immagine di un sottospazio affine è un sottospazio affine con stessa dimensione. Le rette vanno in rette, i piani in piani, e così via. Quindi una terna di punti allineati finisce in una terna di punti allineati. Due rette parallele vanno in due rette parallele con un'affinità. Due sottospazi che contengono uno stesso punto hanno come immagini due sottospazi che contengono l'immagine di quel punto. In particolare la concorrenza di rette viene mantenuta dalle affinità. Inoltre il rapporto semplice tra tre punti $P$, $Q$ ed $R$ allineati, definito come l'unico $k \in \mathbb{F}$ tale che
$$\varphi(P, R) = k \cdot \varphi(R, Q),$$
e indicato con $(P, Q; R)$, viene preservato dalle affinità (teorema di Talete).
7. **Caratterizzazione delle affinità.** Sia $\mathbb{F}$ un campo con $\mathsf{char}(\mathbb{F}) \neq 2$. Sia $\mathbb{A}$ uno spazio affine su $\mathbb{F}$ con $\mathsf{dim}(\mathbb{A}) < \infty$. Allora ogni mappa bigettiva $F : \mathbb{A} \to \mathbb{A}$ che conserva allineamenti e rapporti semplici è un'affinità.