Schede riassuntive di Geometria 1

Alcuni accenni alla geometria di $\mathbb{R}^3$

Si definisce prodotto scalare la forma bilineare simmetrica unicamente determinata da $\langle \underline{e_i}, \underline{e_j} \rangle = \delta_{ij}$. Vale la seguente identità: $\langle (x, y, z), (x', y', z') \rangle = xx' + yy' + zz'$.

Inoltre $\langle \underline{a}, \underline{b} \rangle = |\underline{a}|\, |\underline{b}| \cos(\theta)$, dove θ è l'angolo compreso tra i due vettori. Due vettori $\underline{a}$, $\underline{b}$ si dicono ortogonali se e solo se $\langle \underline{a}, \underline{b} \rangle = 0$.

Si definisce prodotto vettoriale la forma bilineare alternante da $\mathbb{R}^3 \times \mathbb{R}^3$ in $\mathbb{R}^3$ tale che $\underline{e_1} \times \underline{e_2} = \underline{e_3}$, $\underline{e_2} \times \underline{e_3} = \underline{e_1}$, $\underline{e_3} \times \underline{e_1} = \underline{e_2}$ e $\underline{e_i} \times \underline{e_i} = \underline{0}$. Dati due vettori $\underline{(x, y, z)}$ e $\underline{(x', y', z')}$, si può determinarne il prodotto vettoriale informalmente come:

$$\begin{vmatrix} \underline{e_1} & \underline{e_2} & \underline{e_3} \\ x & y & z \\ x' & y' & z' \end{vmatrix}.$$

Vale l'identità $|\underline{a} \times \underline{b}| = |\underline{a}|\, |\underline{b}| \sin(\theta)$, dove θ è l'angolo con cui, ruotando di θ in senso antiorario $\underline{a}$, si ricade su $\underline{b}$. Due vettori $\underline{a}$, $\underline{b}$ si dicono paralleli se $\exists\, k \mid \underline{a} = k\underline{b}$, o equivalentemente se $\underline{a} \times \underline{b} = \underline{0}$. Altrettanto si può dire se $\langle \underline{a}, \underline{b} \rangle = |\underline{a}|\, |\underline{b}|$ (i.e. $\cos(\theta) = 1 \implies \theta = 0$).

Una retta in $\mathbb{R}^3$ è un sottospazio affine della forma $\underline{v} + \operatorname{Span}(\underline{r})$. Analogamente un piano è della forma $\underline{v} + \operatorname{Span}(\underline{x}, \underline{y})$.

Nella forma cartesiana, un piano è della forma $ax + by + cz = d$, dove (a, b, c) è detta normale del piano. Una retta è l'intersezione di due piani, e dunque è un sistema lineare di due equazioni di un piano. Due piani sono perpendicolari fra loro se e solo se le loro normali sono ortogonali. Due piani sono paralleli se e solo se le loro normali sono parallele. Il vettore $\underline{r}$ che genera lo Span di una retta che è intersezione di due piani può essere computato come prodotto vettoriale delle normali dei due piani.

Valgono le seguenti identità:

- $\underline{a} \times (\underline{b} \times \underline{c}) = \langle \underline{a}, \underline{c} \rangle\, \underline{b} - \langle \underline{a}, \underline{b} \rangle\, \underline{c}$ (*identità di Lagrange*),
- $\underline{a} \times (\underline{b} \times \underline{c}) + \underline{b} \times (\underline{c} \times \underline{a}) + \underline{c} \times (\underline{a} \times \underline{b}) = \underline{0}$ (*identità di Jacobi*).

Dati tre punti $\underline{a}$, $\underline{b}$, $\underline{c}$, il volume del parallelepipedo individuato da questi punti è:

$$\left| \det \begin{pmatrix} \underline{a} \\ \underline{b} \\ \underline{c} \end{pmatrix} \right| = |\langle \underline{a}, \underline{b} \times \underline{c} \rangle| .$$

Tre punti sono complanari se e solo se il volume di tale parallelpipedo è nullo (infatti questo è equivalente a dire che almeno uno dei tre punti si scrive come combinazione lineare degli altri due).

Proprietà generali di uno spazio vettoriale

Uno spazio vettoriale V su un campo $\mathbb{K}$ soddisfa i seguenti assiomi:

- $(V, +)$ è un gruppo abeliano,
- il prodotto esterno da $\mathbb{K} \times V$ in V è associativo rispetto agli scalari (i.e. $a(b\underline{v}) = (ab)\underline{v}$),
- $1_{\mathbb{K}} \cdot \underline{v} = \underline{v}$,
- il prodotto esterno è distributivo da ambo i lati (i.e. $(a + b)\underline{v} = a\underline{v} + b\underline{v}$ e $a(\underline{v} + \underline{w}) = a\underline{v} + a\underline{w}$.

Un insieme di vettori I si dice linearmente indipendente se una qualsiasi combinazione lineare di un suo sottinsieme finito è nulla se e solo se i coefficienti dei vettori sono tutti nulli. Si dice linearmente dipendente in caso contrario.

Un insieme di vettori G si dice generatore di V se ogni vettore di V si può scrivere come combinazione lineare di un numero finito di elementi di G, ossia se $V = \operatorname{Span}(G)$.

Una base è un insieme contemporaneamente linearmente indipendente e generatore di V. Equivalentemente una base è un insieme generatore minimale rispetto all'inclusione e un insieme linearmente indipendente massimale, sempre rispetto all'inclusione. Ogni spazio vettoriale, anche quelli non finitamente generati, ammettono una base. La dimensione della base è unica ed è il numero di elementi dell'insieme che è base.

Dato un insieme linearmente indipendente I in uno spazio di dimensione finita, tale insieme, data una base $\mathcal{B}$, può essere esteso a una base T che contiene I e che è completato da elementi di $\mathcal{B}$.

Analogamente, dato un insieme generatore finito G, da esso si può estrarre sempre una base dello spazio.

Uno spazio vettoriale fondato su un campo infinito con un insieme di vettori infinito non è mai unione finita di sottospazi propri. Un insieme linearmente indipendente di V con esattamente $\dim V$ elementi è una base di V. Analogamente, un insieme generatore di V con esattamente $\dim V$ elementi è una base di V.

Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base ordinata dello spazio vettoriale V.

- $\{\underline{0}\}$ e V sono detti sottospazi banali,
- lo Span di n vettori è il più piccolo sottospazio di V contenenti tali vettori,
- $\operatorname{Span}(\mathcal{B}) = V$,
- $\operatorname{Span}(\varnothing) = \{\underline{0}\}$,
- dato X generatore di V, $X \setminus \{\underline{x_0}\}$ genera $V \iff \underline{x_0} \in \operatorname{Span}(X \setminus \{\underline{x_0}\})$,
- $X \subseteq Y$ è un sottospazio di $Y \iff \operatorname{Span}(X) = X$,
- $\operatorname{Span}(X) \subseteq Y \iff X \subseteq Y$, se Y è uno spazio,
- $\operatorname{Span}(\operatorname{Span}(A)) = \operatorname{Span}(A)$,
- se I è un insieme linearmente indipendente di V, allora $|I| \leq \dim V$,
- se G è un insieme generatore di V, allora $|G| \geq \dim V$,
- $[\underline{v}]_{\mathcal{B}}$ è la rappresentazione di $\underline{v}$ nella base ordinata $\mathcal{B}$, ed è un vettore di $\mathbb{K}^n$ che alla coordinata i-esima associa il coefficiente di $\underline{v_i}$ nella combinazione lineare di $\underline{v}$ nella base $\mathcal{B}$,
- la rappresentazione nella base $\mathcal{B}$ è sempre unica ed esiste sempre (è quindi un isomorfismo tra V e $\mathbb{K}^n$),
- si definisce base canonica di $\mathbb{K}^n$ la base $e = \{\underline{e_1}, \ldots, \underline{e_n}\}$, dove $\underline{e_i}$ è un vettore con tutte le coordinate nulle, eccetto per la i-esima, che è pari ad 1 (pertanto $\dim \mathbb{K}^n = n$),
- una base naturale di $M(m, n, \mathbb{K})$ è data da $\mathcal{B} = \{E_{11}, E_{12}, \ldots, E_{1n}, \ldots, E_{mn}\}$, dove E_{ij} è una matrice con tutti gli elementi nulli, eccetto quello nel posto (i, j), che è pari ad 1 (dunque $\dim M(m, n, \mathbb{K}) = mn$),
- le matrici A di taglia n tali che $A^\top = A$ formano il sottospazio $\operatorname{Sym}(n, \mathbb{K})$ di $M(n, \mathbb{K})$, detto sottospazio delle matrici simmetriche, la cui base naturale è data da $\mathcal{B}' = \{E_{ij} + E_{ji} \in \mathcal{B} \mid i < j\} \cup \{E_{ij} \in \mathcal{B} \mid i = j\}$, dove $\mathcal{B}$ è la base naturale di $M(m, n, \mathbb{K})$ (dunque $\dim \operatorname{Sym}(n, \mathbb{K}) = \frac{n(n+1)}{2}$),
- le matrici A di taglia n tali che $A^\top = -A$ formano il sottospazio $\Lambda(n, \mathbb{K})$ di $M(n, \mathbb{K})$, detto sottospazio delle matrici antisimmetriche, la cui base naturale è data da $\mathcal{B}' = \{E_{ij} - E_{ji} \in \mathcal{B} \mid i < j\}$, dove $\mathcal{B}$ è la base naturale di $M(m, n, \mathbb{K})$ (dunque $\dim \Lambda(n, \mathbb{K}) = \frac{n(n-1)}{2}$),
- poiché $\operatorname{Sym}(n, \mathbb{K}) \cap \Lambda(n, \mathbb{K}) = \{\underline{0}\}$ e $\dim \operatorname{Sym}(n, \mathbb{K}) + \dim \Lambda(n, \mathbb{K}) = \dim M(n, \mathbb{K})$, vale che $M(n, \mathbb{K}) = \operatorname{Sym}(n, \mathbb{K}) \oplus \Lambda(n, \mathbb{K})$,
- una base naturale di $\mathbb{K}[x]$ è data da $\mathcal{B} = \{x^n \mid n \in \mathbb{N}\}$, mentre una di $\mathbb{K}_t[x]$ è data da $\mathcal{B} \cap \mathbb{K}_t[x] = \{x^n \mid n \in \mathbb{N} \land n \leq t\}$ (quindi $\dim \mathbb{K}[x] = \infty$ e $\dim \mathbb{K}_t[x] = t + 1$),
- una base naturale di $\mathbb{K}$ è $1_{\mathbb{K}} = \{1_{\mathbb{K}}\}$ (quindi $\dim \mathbb{K} = 1$),
- un sottospazio di dimensione 1 si definisce *retta*, uno di dimensione 2 *piano*, uno di dimensione 3 *spazio*, e, infine, uno di dimensione $n - 1$ un iperpiano,
- un iperpiano Π è sempre rappresentabile da un'equazione cartesiana nelle coordinate della rappresentazione della base (infatti ogni iperpiano è il kernel di un funzionale $f \in V^*$, e $M^{\mathcal{B}}_{1_{\mathbb{K}}}(f)\, [\underline{v}]_{\mathcal{B}} = 0$ è l'equazione cartesiana; è sufficiente prendere una base di Π e completarla a base di V con un vettore $\underline{t}$, considerando infine $\operatorname{Ker} \underline{t}^*$).

Applicazioni lineari, somme dirette, quozienti e prodotti diretti

Un'applicazione da V in W si dice applicazione lineare se:

- $f(\underline{v}+\underline{w}) = f(\underline{v}) + f(\underline{w})$,
- $f(\alpha\underline{v}) = \alpha f(\underline{v})$.

Si definisce $\mathcal{L}(V,W) \subseteq W^V$ come lo spazio delle applicazioni lineari da V a W. Si definisce $\mathrm{End}(V)$ come lo spazio degli endomorfismi di V, ossia delle applicazioni lineari da V in V, dette anche operatori. Un'applicazione lineare si dice isomorfismo se è bigettiva. La composizione di funzioni è associativa.

Dato un sottospazio A di V, si definisce lo spazio quoziente V/A come l'insieme quoziente $V/\sim$ della relazione di equivalenza $\underline{a} \sim \underline{b} \iff a - b \in A$ dotato dell'usuale somma e prodotto esterno. Si scrive $[\underline{v}]_A$ come $\underline{v} + A$ e vale che $A = \underline{0} + A$. In particolare $\underline{v} + A = A \iff \underline{v} \in A$.

Siano $f : V \to W$, $h : V \to W$, $g : W \to Z$ tre applicazioni lineari. $\mathcal{B}_V$ e $\mathcal{B}_W$ sono due basi rispettivamente di V e W. In particolare sia $\mathcal{B}_V = \{\underline{v_1}, \ldots, \underline{v_n}\}$. Si ricorda che $\mathrm{rg}(f) = \dim \mathrm{Im}\, f$. Siano e ed e' le basi canoniche rispettivamente di $\mathbb{K}^n$ e $\mathbb{K}^m$.

- $f(\underline{0}_V) = \underline{0}_W$,
- $\mathrm{Ker}\, f = f^{-1}(\underline{0}_W)$ è un sottospazio di V,
- $\mathrm{Im}\, f = f(V)$ è un sottospazio di W,
- $\mathrm{Im}\, f = \mathrm{Span}(f(\underline{v_1}), \ldots, f(\underline{v_n}))$,
- f è iniettiva $\iff$ $\mathrm{Ker}\, f = \{\underline{0}\}$,
- $V/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$ (*primo teorema d'isomorfismo*),
- $\dim \mathrm{Ker}\, f + \dim \mathrm{Im}\, f = \dim V$ (*teorema del rango*, o formula delle dimensioni, valido se la dimensione di V è finita),
- $g \circ f$ è un'applicazione lineare da V in Z,
- la composizione di funzioni è associativa e distributiva da ambo i lati,
- $g \circ (\alpha f) = \alpha(g \circ f) = (\alpha g) \circ f$, se $\alpha \in \mathbb{K}$,
- $\mathrm{Ker}\, f \subseteq \mathrm{Ker}(g \circ f)$,
- $\mathrm{Im}(g \circ f) \subseteq \mathrm{Im}\, g$,
- $\dim \mathrm{Im}(g \circ f) = \dim \mathrm{Im}\, g|_{\mathrm{Im}\, f} = \dim \mathrm{Im}\, f - \dim \mathrm{Ker}\, g|_{\mathrm{Im}\, f} = \dim \mathrm{Im}\, f - \dim(\mathrm{Ker}\, g \cap \mathrm{Im}\, f)$ (è sufficiente applicare la formula delle dimensioni sulla composizione),
- $\dim \mathrm{Im}(g \circ f) \leq \min\{\dim \mathrm{Im}\, g, \dim \mathrm{Im}\, f\}$,
- $\dim \mathrm{Ker}(g \circ f) \leq \dim \mathrm{Ker}\, g + \dim \mathrm{Ker}\, f$ (è sufficiente applicare la formula delle dimensioni su $(g \circ f)|_{\mathrm{Ker}(g \circ f)}$),
- f iniettiva $\implies$ $\dim V \leq \dim W$,
- f surgettiva $\implies$ $\dim V \geq \dim W$,
- f isomorfismo $\implies$ $\dim V = \dim W$,
- $g \circ f$ iniettiva $\implies$ f iniettiva,
- $g \circ f$ surgettiva $\implies$ g surgettiva,
- f surgettiva $\implies$ $\mathrm{rg}(g \circ f) = \mathrm{rg}(g)$,
- g iniettiva $\implies$ $\mathrm{rg}(g \circ f) = \mathrm{rg}(f)$,
- $M^{\mathcal{B}_V}_{\mathcal{B}_W}(f) = \left([f(\underline{v_1})]_{\mathcal{B}_W} \mid \cdots \mid [f(\underline{v_n})]_{\mathcal{B}_W} \right)$ è la matrice associata a f sulle basi $\mathcal{B}_V$, $\mathcal{B}_W$,
- $M^V_W(f+h) = M^V_W(f) + M^V_W(h)$,
- $M^V_Z(g \circ f) = M^W_Z(g) M^V_W(f)$,
- data $A \in M(m,n,\mathbb{K})$, sia $f_A : \mathbb{K}^n \to \mathbb{K}^m$ tale che $f_A(\underline{x}) = A\underline{x}$, allora $M^e_{e'}(f_A) = A$,
- f è completamente determinata dai suoi valori in una qualsiasi base di V ($M^{\mathcal{B}_V}_{\mathcal{B}_W}$ è un isomorfismo tra $\mathcal{L}(V,W)$ e $M(\dim W, \dim V, \mathbb{K})$),
- $\dim \mathcal{L}(V,W) = \dim V \cdot \dim W$ (dall'isomorfismo di sopra),
- $[\,]^{-1}_{\mathcal{B}_W} \circ M^{\mathcal{B}_V}_{\mathcal{B}_W}(f) \circ [\,]_{\mathcal{B}_V} = f$,
- $[f(\underline{v})]_{\mathcal{B}_W} = M^{\mathcal{B}_V}_{\mathcal{B}_W}(f) \cdot [\underline{v}]_{\mathcal{B}_V}$,
- $\mathrm{Im}(f) = [\,]^{-1}_{\mathcal{B}_W}\left(\mathrm{Im}\, M^{\mathcal{B}_V}_{\mathcal{B}_W}(f)\right)$
- $\mathrm{rg}(f) = \mathrm{rg}\left(M^{\mathcal{B}_V}_{\mathcal{B}_W}(f)\right)$,
- $\mathrm{Ker}(f) = [\,]^{-1}_{\mathcal{B}_V}\left(\mathrm{Ker}\, M^{\mathcal{B}_V}_{\mathcal{B}_W}(f)\right)$,
- $\dim \mathrm{Ker}(f) = \dim \mathrm{Ker}\, M^{\mathcal{B}_V}_{\mathcal{B}_W}(f)$.

Siano $\mathcal{B}'_V$, $\mathcal{B}'_W$ altre due basi rispettivamente di V e W. Allora vale il *teorema del cambiamento di base*:

$$M^{\mathcal{B}'_V}_{\mathcal{B}'_W}(f) = M^{\mathcal{B}_W}_{\mathcal{B}'_W}(id_W)\, M^{\mathcal{B}_V}_{\mathcal{B}_W}(f)\, M^{\mathcal{B}'_V}_{\mathcal{B}_V}(id_V).$$

Siano A e B due sottospazi di V. $\mathcal{B}_A$ e $\mathcal{B}_B$ sono due basi rispettivamente di A e B.

- $A + B = \{\underline{a} + \underline{b} \in V \mid \underline{a} \in A, \underline{b} \in B\}$ è un sottospazio,
- $\dim(A+B) = \dim A + \dim B - \dim(A \cap B)$ (*formula di Grassmann*),
- A e B sono in somma diretta $\iff$ $A \cap B = \{\underline{0}\}$ $\iff$ ogni elemento di $A + B$ si scrive in modo unico come somma di $\underline{a} \in A$ e $\underline{b} \in B$ $\iff$ $\dim(A+B) = \dim A + \dim B$ (in tal caso si scrive $A + B = A \oplus B$),
- $\dim V/A = \dim V - \dim A$ (è sufficiente applicare il teorema del rango alla proiezione al quoziente),
- $\dim V \times W = \dim V + \dim W$ ($\mathcal{B}_V \times \{\underline{0}_W\} \cup \{\underline{0}_V\} \times \mathcal{B}_W$ è una base di $V \times W$).

Si definisce *immersione* da V in $V \times W$ l'applicazione lineare i_V tale che $i_V(\underline{v}) = (\underline{v}, \underline{0})$. Si definisce *proiezione* da $V \times W$ in V l'applicazione lineare p_V tale che $p_V(\underline{v}, \underline{w}) = \underline{v}$. Analogamente si può fare con gli altri spazi del prodotto cartesiano.

Si dice che B è un supplementare di A se $V = A \oplus B \iff \dim A + \dim B = \dim V \wedge A \cap B = \{\underline{0}\}$. Il supplementare non è per forza unico. Per trovare un supplementare di A è sufficiente completare $\mathcal{B}_A$ ad una base $\mathcal{B}$ di V e considerare $\mathrm{Span}(\mathcal{B} \setminus \mathcal{B}_A)$.

Proprietà generali delle matrici

Si dice che una matrice $A \in M(n,\mathbb{K})$ è singolare se $\det(A) = 0$, o equivalentemente se non è invertibile. Compatibilmente, si dice che una matrice $A \in M(n,\mathbb{K})$ è non singolare se $\det(A) \neq 0$, ossia se A è invertibile.

Si definisce la matrice trasposta di $A \in M(m,n,\mathbb{K})$, detta $A^\top$, in modo tale che $A_{ij} = A^\top_{ji}$.

- $(AB)^\top = B^\top A^\top$,
- $(A+B)^\top = A^\top + B^\top$,
- $(\lambda A)^\top = \lambda A^\top$,
- $(A^\top)^\top = A$,
- se A è invertibile, $(A^\top)^{-1} = (A^{-1})^\top$,
- $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)\left(\begin{array}{c|c} E & F \\ \hline G & H \end{array}\right) = \left(\begin{array}{c|c} AE+BG & AF+BH \\ \hline CE+DG & CF+DH \end{array}\right)$.

Siano $A \in M(m,n,\mathbb{K})$ e $B \in M(n,m,\mathbb{K})$.

Si definisce $\mathrm{GL}(n,\mathbb{K})$ come il gruppo delle matrici di taglia n invertibili sulla moltiplicazione matriciale. Si definisce triangolare superiore una matrice i cui elementi al di sotto della diagonale sono nulli, mentre si definisce triangolare inferiore una matrice i cui elementi nulli sono quelli al di sopra della diagonale.

Si definiscono

$$Z(M(n,\mathbb{K})) = \{A \in M(n,\mathbb{K}) \mid AB = BA \;\forall\, B \in M(n,\mathbb{K})\},$$

ossia l'insieme delle matrici che commutano con tutte le altre matrici, e

$$Z_{\mathrm{GL}}(M(n,\mathbb{K})) = \{A \in M(n,\mathbb{K}) \mid AB = BA \;\forall\, B \in \mathrm{GL}(n,\mathbb{K})\},$$

ovvero l'insieme delle matrici che commutano con tutte le matrici di $\mathrm{GL}(n,\mathbb{K})$.

Si definisce $\mathrm{tr} \in M(m,\mathbb{K})^*$ come il funzionale che associa ad ogni matrice la somma degli elementi sulla sua diagonale.

- $\mathrm{tr}(A^\top) = \mathrm{tr}(A)$,
- $\mathrm{tr}(AB) = \mathrm{tr}(BA)$,
- $Z(M(n,\mathbb{K})) = \mathrm{Span}(I_n)$,
- $Z_{\mathrm{GL}}(M(n,\mathbb{K})) = \mathrm{Span}(I_n)$.

Sia $A \in M(n, \mathbb{K})$. Sia $C_A \in \operatorname{End}(M(n, \mathbb{K}))$ definito in modo tale che $C_A(B) = AB - BA$. Allora $\operatorname{Ker} C_A = M(n, \mathbb{K}) \iff A \in \operatorname{Span}(I_n)$. Siano I un insieme di n^2 indici distinti, allora l'insieme

$$T = \left\{A^i \mid i \in I\right\}$$

è linearmente dipendente (è sufficiente notare che se così non fosse, se $A \notin \operatorname{Span}(I_n)$, tale T sarebbe base di $M(n, \mathbb{K})$, ma così $\operatorname{Ker} C_A = M(n, \mathbb{K}) \implies A \in \operatorname{Span}(I_n)$, $\lightning$, e che se $A \in \operatorname{Span}(I_n)$, T è chiaramente linearmente dipendente).

In generale esiste sempre un polinomio $p(X) \in \mathbb{K}[x]$ di grado n tale per cui $p(A) = 0$, dove un tale polinomio è per esempio il polinomio caratteristico di p, ossia $p(\lambda) = \det(\lambda I_n - A)$ (*teorema di Hamilton-Cayley*).

Rango di una matrice

Si definisce rango di una matrice A il numero di colonne linearmente indipendenti di A. Siano A, $B \in M(m, n, \mathbb{K})$.

- $\operatorname{rg}(A) = \operatorname{rg}(A^\top)$ (i.e. il rango è lo stesso se calcolato sulle righe invece che sulle colonne),
- $\operatorname{rg}(A) \leq \min\{m, n\}$ (come conseguenza dell'affermazione precedente),
- $\operatorname{rg}(A + B) \leq \operatorname{rg}(A) + \operatorname{rg}(B) \impliedby \operatorname{Im}(A + B) \subseteq \operatorname{Im}(A) + \operatorname{Im}(B)$,
- $\operatorname{rg}(A + B) = \operatorname{rg}(A) + \operatorname{rg}(B) \implies \operatorname{Im}(A + B) = \operatorname{Im}(A) \oplus \operatorname{Im}(B)$ (è sufficiente applicare la formula di Grassmann),
- $\operatorname{rg}(A)$ è il minimo numero di matrici di rango uno che sommate restituiscono A (è sufficiente usare la proposizione precedente per dimostrare che devono essere almeno $\operatorname{rg}(A)$),
- $\operatorname{rg}(A) = 1 \implies \exists\, B \in M(m, 1, \mathbb{K})$, $C \in M(1, n, \mathbb{K}) \mid A = BC$ (infatti A può scriversi come $\left([c|c|c]\alpha_1 A^i \quad \cdots \quad \alpha_n A^i\right)$ per un certo $i \leq n$ tale che $A^i \neq \underline{0}$).

Siano $A \in M(m, n, \mathbb{K})$, $B \in M(n, k, \mathbb{K})$ e $C \in M(k, t, \mathbb{K})$.

- $\operatorname{rg}(AB) \geq \operatorname{rg}(A) + \operatorname{rg}(B) - n$ (*disuguaglianza di Sylvester* – è sufficiente usare la formula delle dimensioni ristretta alla composizione $f_A \circ f_B$),
- $\operatorname{rg}(ABC) \geq \operatorname{rg}(AB) + \operatorname{rg}(BC) - \operatorname{rg}(B)$ (*disuguaglianza di Frobenius*, di cui la proposizione precedente è un caso particolare con $B = I_n$ e $k = n$),
- $\operatorname{rg}(AB) = \operatorname{rg}(B) \impliedby \operatorname{Ker} A = \{\underline{0}\}$ (è sufficiente usare la formula delle dimensioni ristretta alla composizione $f_A \circ f_B$),
- $\operatorname{rg}(AB) = \operatorname{rg}(A) \impliedby f_B$ surgettiva (come sopra).

Sia $A \in M(n, \mathbb{K})$.

- se A è antisimmetrica e il campo su cui si fonda lo spazio vettoriale non ha caratteristica 2, allora $\operatorname{rg}(A)$ è pari,
- $\operatorname{rg}(A) = n \iff \dim \operatorname{Ker} A = 0 \iff \det(A) \neq 0 \iff$ A è invertibile,

Sistemi lineari, algoritmo di eliminazione di Gauss ed SD-equivalenza

Un sistema lineare di m equazioni in n variabili può essere rappresentato nella forma $A\underline{x} = B$, dove $A \in M(m, n, \mathbb{K})$, $\underline{x} \in \mathbb{K}^n$ e $B \in \mathbb{K}^m$. Un sistema lineare si dice omogeneo se $B = \underline{0}$. In tal caso l'insieme delle soluzioni del sistema coincide con $\operatorname{Ker} A = \operatorname{Ker} f_A$, dove $f_A : \mathbb{K}^n \to \mathbb{K}^m$ è l'applicazione lineare indotta dalla matrice A. Le soluzioni di un sistema lineare sono raccolte nel sottospazio affine $\underline{s} + \operatorname{Ker} A$, dove $\underline{s}$ è una qualsiasi soluzione del sistema completo.

- $A\underline{x} = B$ ammette soluzione se e solo se $B \in \operatorname{Span}(A^1, \ldots, A^n) \iff \operatorname{Span}(A^1, \ldots, A^n, B) = \operatorname{Span}(A^1, \ldots, A^n) \iff \dim \operatorname{Span}(A^1, \ldots, A^n, B) = \dim \operatorname{Span}(A^1, \ldots, A^n) \iff \dim \operatorname{Im}(A \mid B) = \dim \operatorname{Im} A \iff \operatorname{rg}(A \mid B) = \operatorname{rg}(A)$ (*teorema di Rouché-Capelli*),
- $A\underline{x} = B$, se la ammette, ha un'unica soluzione se e solo se $\operatorname{Ker} A = \{\underline{0}\} \iff \operatorname{rg} A = n$.

Si definiscono tre operazioni sulle righe di una matrice A:

1. l'operazione di scambio di riga,
2. l'operazione di moltiplicazione di una riga per uno scalare non nullo,
3. la somma di un multiplo non nullo di una riga ad un'altra riga distinta.

Queste operazioni non variano né $\operatorname{Ker} A$ né $\operatorname{rg}(A)$. Si possono effettuare le stesse medesime operazioni sulle colonne (variando tuttavia $\operatorname{Ker} A$, ma lasciando invariato $\operatorname{Im} A$ – e quindi $\operatorname{rg}(A)$). L'algoritmo di eliminazione di Gauss procede nel seguente modo:

1. se A ha una riga, l'algoritmo termina;
2. altrimenti si prenda la prima riga di A con il primo elemento non nullo e la si scambi con la prima riga di A (in caso non esista, si proceda all'ultimo passo),
3. per ogni riga di A con primo elemento non nullo, esclusa la prima, si sottragga un multiplo della prima riga in modo tale che la riga risultante abbia il primo elemento nullo,
4. si ripeta l'algoritmo considerando come matrice A la matrice risultante dall'algoritmo senza la prima riga e la prima colonna (in caso tale matrice non possa esistere, l'algoritmo termina).

Si definiscono *pivot* di una matrice l'insieme dei primi elementi non nulli di ogni riga della matrice. Il rango della matrice iniziale A è pari al numero di *pivot* della matrice risultante dall'algoritmo di eliminazione di Gauss. Una matrice che processata dall'algoritmo di eliminazione di Gauss restituisce sé stessa è detta matrice a scala.

Agendo solo attraverso operazioni per riga, l'algoritmo di eliminazione di Gauss non modifica $\operatorname{Ker} A$ (si può tuttavia integrare l'algoritmo con le operazioni per colonna, perdendo quest'ultimo beneficio).

Agendo su una matrice a scala con operazioni per riga considerando la matrice riflessa (ossia dove l'elemento $(1, 1)$ e (m, n) sono scambiati), si può ottenere una matrice a scala ridotta, ossia un matrice dove tutti i pivot sono 1 e dove tutti gli elementi sulle colonne dei pivot, eccetto i pivot stessi, sono nulli.

Si definisce:

$$I_r^{m \times n} = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right) \in M(m, n, \mathbb{K}).$$

Per ogni applicazione lineare $f : V \to W$, con $\dim V = n$ e $\dim W = m$ esistono due basi $\mathcal{B}_V$, $\mathcal{B}_W$ rispettivamente di V e W tale che $M_{\mathcal{B}_W}^{\mathcal{B}_V}(f) = I_r^{m \times n}$, dove $r = \operatorname{rg}(f)$ (è sufficiente completare con I a base di V una base di $\operatorname{Ker} f$ e poi prendere come base di W il completamento di $f(I)$ su una base di W).

Si definisce SD-equivalenza la relazione d'equivalenza su $M(m, n, \mathbb{K})$ indotta dalla relazione $A \sim_{SD} B \iff \exists\, P \in GL(m, \mathbb{K}),\ Q \in GL(n, \mathbb{K}) \mid A = PBQ$. L'invariante completo della SD-equivalenza è il rango: $\operatorname{rg}(A) = \operatorname{rg}(B) \iff A \sim_{SD} B$ (infatti $\operatorname{rg}(A) = r \iff A \sim_{SD} I_r^{m \times n}$ – è sufficiente applicare il cambio di base e sfruttare il fatto che esistono sicuramente due basi per cui f_A ha $I_r^{m \times n}$ come matrice associata).

Poiché $I_r^{m \times n}$ ha sempre rango r, l'insieme quoziente della SD-equivalenza su $M(m, n, \mathbb{K})$ è il seguente:

$$M(m, n, \mathbb{K})/\sim_{SD} = \left\{[\underline{0}], \left[I_1^{m \times n}\right], \ldots, \left[I_{\min\{m,n\}}^{m \times n}\right]\right\},$$

contenente esattamente $\min\{m, n\}$ elementi. L'unico elemento di $[\underline{0}]$ è $\underline{0}$ stesso.

La regola di Cramer

Qualora $m = n$ e A fosse invertibile (i.e. $\det(A) \neq 0$), per calcolare il valore di $\underline{x}$ si può applicare la regola di Cramer.

Si definisce:

$$A_i^* = \left([c|c|c|c|c]A^1 \quad \cdots \quad A^i \to B \quad \cdots \quad A^n\right),$$

dove si sostituisce alla i-esima colonna di A il vettore B. Allora vale la seguente relazione:

$$\underline{x} = \frac{1}{\det(A)}\begin{pmatrix}\det(A_1^*) \\ \vdots \\ \det(A_n^*)\end{pmatrix}.$$

L'inverso (generalizzato e non) di una matrice

Si definisce matrice dei cofattori di una matrice $A \in M(n, \mathbb{K})$ la seguente matrice:

$$\operatorname{Cof} A = \begin{pmatrix}\operatorname{Cof}_{1,1}(A) & \dots & \operatorname{Cof}_{1,n}(A) \\ \vdots & \ddots & \vdots \\ \operatorname{Cof}_{n,1}(A) & \dots & \operatorname{Cof}_{n,n}(A),\end{pmatrix},$$

dove, detta $A_{i,j}$ il minore di A ottenuto eliminando la i-esima riga e la j-esima colonna, si definisce il cofattore (o complemento algebrico) nel seguente modo:

$$\operatorname{Cof}_{i,j}(A) = (-1)^{i+j}\det(A_{i,j}).$$

Si definisce inoltre l'aggiunta classica:

$$\operatorname{adj}(A) = (\operatorname{Cof} A)^\top.$$

Allora, se A ammette un inverso (i.e. se $\det(A) \neq 0$), vale la seguente relazione:

$$A^{-1} = \frac{1}{\det(A)}\operatorname{adj}(A).$$

Quindi, per esempio, A^{-1} è a coefficienti interi $\iff \det(A) = \pm 1$.

Siano A, $B \in M(n, \mathbb{K})$.

- $\operatorname{adj}(AB) = \operatorname{adj}(B)\operatorname{adj}(A)$,
- $\operatorname{adj}(A^\top) = \operatorname{adj}(A)^\top$.

Si definisce inverso generalizzato di una matrice $A \in M(m, n, \mathbb{K})$ una matrice $X \in M(n, m, \mathbb{K}) \mid AXA = A$. Ogni matrice ammette un inverso generalizzato (è sufficiente considerare gli inversi generalizzati di $I_r^{m\times n}$ e la SD-equivalenza di A con $I_r^{m\times n}$, dove $\operatorname{rg}(A) = r$). Se $m = n$ ed A è invertibile, allora A^{-1} è l'unico inverso generalizzato di A. Gli inversi generalizzati di $I_r^{m\times n}$ sono della forma:

$$X = \left(\begin{array}{c|c} I_r & B \\ \hline C & D\end{array}\right) \in M(m, n, \mathbb{K}).$$

Endomorfismi e similitudine

Si definisce la similitudine tra matrici su $M(n, \mathbb{K})$ come la relazione di equivalenza determinata da $A \sim B \iff \exists\, P \in \mathrm{GL}(n, \mathbb{K}) \mid A = PBP^{-1}$. $A \sim B \implies \operatorname{rg}(A) = \operatorname{rg}(B)$, $\operatorname{tr}(A) = \operatorname{tr}(B)$, $\det(A) = \det(B)$, $P_\lambda(A) = P_\lambda(B)$ (invarianti *non completi* della similitudine). Vale inoltre che $A \sim B \iff A$ e B hanno la stessa forma canonica di Jordan, a meno di permutazioni dei blocchi di Jordan (invariante *completo* della similitudine). La matrice identità è l'unica matrice identica a sé stessa.

Sia $p \in \operatorname{End}(V)$. Si dice che un endomorfismo è un automorfismo se è un isomorfismo. Siano $\mathcal{B}$, $\mathcal{B}'$ due qualsiasi basi di V.

- p automorfismo $\iff p$ iniettivo $\iff p$ surgettivo (è sufficiente applicare la formula delle dimensioni),
- $M^{\mathcal{B}}_{\mathcal{B}'}(id_V)M^{\mathcal{B}'}_{\mathcal{B}}(id_V) = I_n$ (dunque entrambe le matrici sono invertibili e sono l'una l'inverso dell'altra),
- se p è un automorfismo, $M^{\mathcal{B}}_{\mathcal{B}'}(p^{-1}) = M^{\mathcal{B}'}_{\mathcal{B}}(p)^{-1}$,
- $M^{\mathcal{B}}_{\mathcal{B}}(p) = \underbrace{M^{\mathcal{B}'}_{\mathcal{B}}(id_V)}_{P}\, M^{\mathcal{B}'}_{\mathcal{B}'}(p)\, \underbrace{M^{\mathcal{B}}_{\mathcal{B}'}(id_V)}_{P^{-1}}$ (ossia $M^{\mathcal{B}}_{\mathcal{B}}(p) \sim M^{\mathcal{B}'}_{\mathcal{B}'}(p)$).

$M^{\mathcal{B}}_{\mathcal{B}'}(id_V)M^{\mathcal{B}'}_{\mathcal{B}}(id_V) = I_n$. Dunque entrambe le matrici sono invertibili. Inoltre $M^{\mathcal{B}}_{\mathcal{B}}(id_V) = I_n$.

Duale, biduale e annullatore

Si definisce duale di uno spazio vettoriale V lo spazio $V^* = \mathcal{L}(V, \mathbb{K})$, i cui elementi sono detti funzionali. Analogamente il biduale è il duale del duale di V: $V^{**} = (V^*)^* = \mathcal{L}(V^*, \mathbb{K})$.

Sia data una base $\mathcal{B} = \{\underline{v_1}, \dots, \underline{v_n}\}$ di uno spazio vettoriale V di dimensione n. Allora $\dim V^* = \dim \mathcal{L}(V, \mathbb{K}) = \dim V \cdot \dim \mathbb{K} = \dim V$. Si definisce il funzionale $\underline{v_i}^*$ come l'applicazione lineare univocamente determinata dalla relazione:

$$\underline{v_i}^*(\underline{v_j}) = \delta_{ij}.$$

Sia $\mathcal{B}^* = \{\underline{v_1}^*, \dots, \underline{v_n}^*\}$. Allora $\mathcal{B}^*$ è una base di V^*. Poiché V e V^* hanno la stesso dimensione, tali spazi sono isomorfi, sebbene non canonicamente. Ciononostante, V e V^{**} sono canonicamente isomorfi tramite l'isomorfismo:

$$\varphi^{**} : V \to V^{**},\ \underline{v} \mapsto \operatorname{val}|_{V^*},$$

che associa ad ogni vettore $\underline{v}$ la funzione di valutazione in una funzionale in $\underline{v}$, ossia:

$$\operatorname{val}|_{V^*} : V^* \to \mathbb{K},\ f \mapsto f(\underline{v}).$$

Sia $U \subseteq V$ un sottospazio di V. Si definisce il sottospazio di $\mathcal{L}(V, W)$:

$$\operatorname{Ann}_{\mathcal{L}(V,W)}(U) = \{f \in \mathcal{L}(V, W) \mid f(U) = \{\underline{0}\}\}.$$

Se V è a dimensione finita, la dimensione di $\operatorname{Ann}(U)$ è pari a $(\dim V - \dim U) \cdot \dim W$ (è sufficiente prendere una base di U, completarla a base di V e notare che $f(U) = \{\underline{0}\} \iff$ ogni valutazione in f degli elementi della base di U è nullo $\iff$ la matrice associata di f ha tutte colonne nulle in corrispondenza degli elementi della base di U).

Si scrive semplicemente $\operatorname{Ann}(U)$ quando $W = \mathbb{K}$ (ossia quando le funzioni sono funzionali di V). In tal caso $\dim \operatorname{Ann}(U) = \dim V - \dim U$.

- $\varphi^{**}(U) \subseteq \operatorname{Ann}(\operatorname{Ann}(U))$,
- se V è a dimensione finita, $\varphi^{**}(U) = U^{**} = \operatorname{Ann}(\operatorname{Ann}(U))$ (è sufficiente applicare la formula delle dimensioni $\varphi^{**}|_U$ e notare l'uguaglianza tra le due dimensioni),
- se V è a dimensione finita e W è un altro sottospazio di V, $U = W \iff \operatorname{Ann}(U) = \operatorname{Ann}(W)$ (è sufficiente considerare $\operatorname{Ann}(\operatorname{Ann}(U)) = \operatorname{Ann}(\operatorname{Ann}(W))$ e applicare la proposizione precedente, ricordandosi che φ^{**} è un isomorfismo, ed è dunque iniettivo).

Si definisce l'applicazione trasposta $^\top$ da $\mathcal{L}(V, W)$ a $\mathcal{L}(W^*, V^*)$ in modo tale che $f^\top(g) = g \circ f \in V^*$. Siano f, $g \in \mathcal{L}(V, W)$ e sia $h \in \mathcal{L}(W, Z)$.

- $(f + g)^\top = f^\top + g^\top$,
- $(\lambda f)^\top = \lambda f^\top$,
- se f è invertibile, $(f^{-1})^\top = (f^\top)^{-1}$,
- $(h \circ f)^\top = f^\top \circ h^\top$.

Siano $\mathcal{B}_V$, $\mathcal{B}_W$ due basi rispettivamente di V e di W. Allora vale la seguente relazione:

$$M^{\mathcal{B}_W^*}_{\mathcal{B}_V^*}(f^\top) = M^{\mathcal{B}_V}_{\mathcal{B}_W}(f)^\top.$$

Applicazioni multilineari

Sia $f : V_1 \times \ldots \times V_n \to W$ un'applicazione, dove V_i è uno spazio vettoriale $\forall\, i \leq n$, così come W. Tale applicazione si dice n-lineare ed appartiene allo spazio $\operatorname{Mult}(V_1 \times \ldots \times V_n, W)$, se è lineare in ogni sua coordinata, ossia se:

- $f(x_1, \dots, x_i + y_i, \dots, x_n) = f(x_1, \dots, x_i, \dots, x_n) + f(x_1, \dots, y_i, \dots, x_n)$,
- $f(x_1, \dots, \alpha x_i, \dots, x_n) = \alpha f(x_1, \dots, x_i, \dots, x_n)$.

Sia $W = \mathbb{K}$, e siano tutti gli spazi V_i fondati su tale campo: allora $\operatorname{Mult}(V_1 \times \ldots \times V_n, \mathbb{K})$ si scrive anche come $V_1^* \otimes \ldots \otimes V_n^*$, e tale spazio è detto prodotto tensoriale tra V_1, ..., V_n. Sia V_i di dimensione finita $\forall\, i \leq n$. Siano $\mathcal{B}_{V_i} = \left\{\underline{v_1^{(i)}}, \dots, \underline{v_{k_i}^{(i)}}\right\}$ base di V_i, dove $k_i = \dim V_i$. Si definisce l'applicazione n-lineare $\underline{v_{j_1}^{(1)}}^* \otimes \cdots \otimes \underline{v_{j_n}^{(n)}}^* \in \operatorname{Mult}(V_1 \times \ldots \times V_n, \mathbb{K})$ univocamente determinata dalla relazione:

$$\underline{v_{j_1}^{(1)}}^* \otimes \cdots \otimes \underline{v_{j_n}^{(n)}}^*(\underline{w_1}, \dots, \underline{w_n}) = \underline{v_{j_1}^{(1)}}^*(\underline{w_1}) \cdots \underline{v_{j_n}^{(n)}}^*(\underline{w_n}).$$

Si definisce l'insieme $\mathcal{B}_\otimes$ nel seguente modo:

$$\mathcal{B}_\otimes = \left\{ \underline{v_{j_1}^{(1)}}^* \otimes \cdots \otimes \underline{v_{j_n}^{(n)}}^* \mid 1 \leq j_1 \leq k_1, \ldots, 1 \leq j_n \leq k_n \right\}.$$

Poiché ogni applicazione n-lineare è univocamente determinata dai valori che assume ogni combinazione degli elementi delle basi degli spazi V_i, vi è un isomorfismo tra $\operatorname{Mult}(V_1 \times \ldots \times V_n, \mathbb{K})$ e $\mathbb{K}^{\mathcal{B}_{V_1} \times \cdots \times \mathcal{B}_{V_n}}$, che ha dimensione $\prod_{i=1}^n k_i = k$. Pertanto anche $\dim \operatorname{Mult}(V_1 \times \ldots \times V_n, \mathbb{K}) = k$. Poiché $\mathcal{B}_\otimes$ genera $\operatorname{Mult}(V_1 \times \ldots \times V_n, \mathbb{K})$ e i suoi elementi sono tanti quanto è la dimensione dello spazio, tale insieme è una base di $\operatorname{Mult}(V_1 \times \ldots \times V_n, \mathbb{K})$.

Se $V_i = V_1 = V \;\forall\, i \leq n$, si dice che $\operatorname{Mult}(V^n, \mathbb{K})$ è lo spazio delle forme n-lineari di V.

Applicazioni multilineari simmetriche

Sia V uno spazio di dimensione n. Una forma k-lineare f si dice simmetrica ed appartiene allo spazio $\operatorname{Sym}^k(V)$ se:

$$f(\underline{x_1}, \ldots, \underline{x_k}) = f(\underline{x_{\sigma(1)}}, \ldots, \underline{x_{\sigma(k)}}), \quad \forall\, \sigma \in S_k.$$

Poiché ogni applicazione n-lineare simmetrica è univocamente determinata dai valori che assume negli elementi della base disposti in modo non decrescente, $\dim \operatorname{Sym}^k(V) = \binom{n+k-1}{k}$.

Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V. Dato un insieme di indici non decrescente I, si definisce il prodotto simmetrico (o *prodotto vee*) $\underline{v_{i_1}}^* \vee \cdots \vee \underline{v_{i_k}}^*$ tra elementi della base come la forma k-lineare simmetrica determinata dalla relazione:

$$\underline{v_{i_1}}^* \vee \cdots \vee \underline{v_{i_k}}^* = \sum_{\sigma \in S_k} \underline{v_{i_{\sigma(1)}}}^* \otimes \cdots \otimes \underline{v_{i_{\sigma(k)}}}^*.$$

Si definisce l'insieme:

$$\mathcal{B}_{\mathrm{Sym}} = \left\{ \underline{v_{i_1}}^* \vee \cdots \vee \underline{v_{i_k}}^* \mid 1 \leq i_1 \leq \cdots \leq i_k \leq n \right\}.$$

L'insieme $\mathcal{B}_{\mathrm{Sym}}$ è sia generatore che linearmente indipendente su $\operatorname{Sym}^k(V)$, ed è dunque base. Allora $\dim \operatorname{Sym}^k(V) = \binom{n+k-1}{k}$.

Applicazioni multilineari alternanti

Sia V uno spazio di dimensione n. Una forma k-lineare f si dice alternante (o antisimmetrica) ed appartiene allo spazio $\Lambda^k(V)$ (talvolta scritto come $\operatorname{Alt}^k(V)$) se:

$$f(x_1, \ldots, x_k) = 0 \impliedby \exists\, i, j \leq k \mid x_i = x_j.$$

Questo implica che:

$$f(x_1, \ldots, x_k) = \operatorname{sgn}(\sigma) f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \quad \forall\, \sigma \in S_k$$

Se $k > n$, un argomento della base di V si ripete sempre nel computo f negli elementi della base, e quindi ogni alternante è pari a $\underline{0}$, ossia $\dim \Lambda^k(V) = 0$.

Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V. Dato un insieme di indici crescente I, si definisce il prodotto esterno (o *prodotto wedge*) $\underline{v_{i_1}}^* \wedge \cdots \wedge \underline{v_{i_k}}^*$ tra elementi della base come la forma k-lineare alternante determinata dalla relazione:

$$\underline{v_{i_1}}^* \wedge \cdots \wedge \underline{v_{i_k}}^* = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\, \underline{v_{i_{\sigma(1)}}}^* \otimes \cdots \otimes \underline{v_{i_{\sigma(k)}}}^*.$$

Si definisce l'insieme:

$$\mathcal{B}_\Lambda = \left\{ \underline{v_{i_1}}^* \wedge \cdots \wedge \underline{v_{i_k}}^* \mid 1 \leq i_1 < \cdots < i_k \leq n \right\}.$$

L'insieme $\mathcal{B}_\Lambda$ è sia generatore che linearmente indipendente su $\Lambda^k(V)$, ed è dunque base. Allora $\dim \Lambda^k(V) = \binom{n}{k}$. Riassumendo si può scrivere:

$$\dim \Lambda^k(V) = \begin{cases} 0 & \text{se } k > n\,, \\ \binom{n}{k} & \text{altrimenti.} \end{cases}$$

Quindi è quasi sempre vero che:

$$\underbrace{\dim \operatorname{Sym}^k(V)}_{=\binom{n+k-1}{k}} + \underbrace{\dim \Lambda^k(V)}_{\leq \binom{n}{k}} < \underbrace{\dim \operatorname{Mult}(V^k, \mathbb{K})}_{=n^k},$$

e dunque che $\operatorname{Sym}^k(V) + \Lambda^k(V) \neq \operatorname{Mult}(V^k, \mathbb{K})$.

Determinante di una matrice

Si definisce il determinante det di una matrice di taglia $n \times n$ come l'unica forma n-lineare alternante di $(\mathbb{K}^n)^n$ tale che $\det(\underline{e_1}, \ldots, \underline{e_n}) = 1$ (infatti $\dim \Lambda^n(V) = \binom{n}{n} = 1$, e quindi ogni forma alternante è multipla delle altre, eccetto per lo zero).

Equivalentemente $\det = \underline{e_1}^* \wedge \cdots \wedge \underline{e_n}^*$.

Siano A, $B \in M(n, \mathbb{K})$. Si scrive $\det(A)$ per indicare $\det(A_1, \ldots, A_n)$. Vale pertanto la seguente relazione:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

- $\det(I_n) = 1$,
- $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$,
- $\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = a(ei - fh) - b(di - fg) + c(dh - eg)$,
- $\det(A) \neq 0 \iff A$ invertibile (ossia non singolare),
- $\det(\lambda A) = \lambda^n A$,
- $\det(A) = \det(A^\top)$ (è sufficiente applicare la definizione di det e manipolare algebricamente il risultato per evidenziare l'uguaglianza),
- se A è antisimmetrica, n è dispari e $\operatorname{char} \mathbb{K} \neq 2$, $\det(A) = \det(-A^\top) = (-1)^n \det(A^\top) = (-1)^n \det(A) = -\det(A) \implies \det(A) = 0$ (quindi ogni matrice antisimmetrica di taglia dispari non è invertibile),
- $\det(AB) = \det(A)\det(B)$ (*teorema di Binet* – è sufficiente considerare la forma $\frac{\det(AB)}{\det(B)}$ in funzione delle righe di A e determinare che tale forma è alternante e che vale 1 nell'identità, e che, per l'unicità del determinante, deve obbligatoriamente essere pari a $\det(A)$),
- se A è invertibile, $\det(A^{-1}) = \det(A)^{-1}$,
- $\det \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = \det(\lambda_1 \underline{e_1}, \ldots, \lambda_n \underline{e_n}) = \prod_{i=1}^n \lambda_i$,
- se A è triangolare superiore (o inferiore), allora $\det(A)$ è il prodotto degli elementi sulla sua diagonale principale,
- $\det(A_1, \ldots, A_n) = \operatorname{sgn}(\sigma) \det(A_{\sigma(1)}, \ldots, A_{\sigma(n)})$, $\forall\, \sigma \in S_n$ (infatti det è alternante),
- $\det \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = \det(AD - BC)$, se C e D commutano e D è invertibile,
- $\det \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right) = \det(A)\det(C)$,
- se A è nilpotente (ossia se $\exists\, k \mid A^k = 0$), $\det(A) = 0$,
- se A è idempotente (ossia se $A^2 = A$), allora $\det(A) = 1$ o $\det(A) = 0$,
- se A è ortogonale (ossia se $AA^\top = I_n$), allora $\det(A) = \pm 1$,
- se A è un'involuzione (ossia se $A^2 = I_n$), allora $\det(A) = \pm 1$,

Le operazioni del terzo tipo dell'algoritmo di eliminazione di Gauss (ossia l'aggiunta a una riga di un multiplo di un'altra riga – a patto che le due righe siano distinte) non alterano il determinante della matrice iniziale, mentre lo scambio di righe ne inverte il segno (corrisponde a una trasposizione di S_n). L'operazione del secondo tipo (la moltiplicazione di una riga per uno scalare) altera il determinante moltiplicandolo per tale scalare.

Inoltre, se D è invertibile, vale la seguente scomposizione:

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = \left(\begin{array}{c|c} I_k & BD^{-1} \\ \hline 0 & I_k \end{array}\right) \left(\begin{array}{c|c} A - BD^{-1}C & 0 \\ \hline 0 & D \end{array}\right) \left(\begin{array}{c|c} I_k & 0 \\ \hline D^{-1}C & I_k \end{array}\right),$$

dove $k \times k$ è la taglia di A. Pertanto vale la seguente relazione, sempre se D è invertibile:

$$\det \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = \det(A - BD^{-1}C)\det(D).$$

È possibile computare il determinante di A, scelta la riga i, mediante lo sviluppo di Laplace:

$$\det(A) = \sum_{j=1}^{n} a_{ij} \operatorname{Cof}_{i,j}(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{i,j}).$$

Si definisce matrice di Vandermonde una matrice $A \in M(n, \mathbb{K})$ della forma:

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1}. \end{pmatrix}$$

Vale allora che:

$$\det(A) = \prod_{1 \le i < j \le n} (x_j - x_i),$$

verificabile notando che $\det(A)$ è di grado $\frac{n(n-1)}{2}$ e che ponendo $x_i = x_j$ per una coppia (i, j), tale matrice ha due righe uguali, e quindi determinante nullo $\implies (x_j - x_i) \mid \det(A) \overset{\text{UFD}}{\implies} \det(A) = \prod_{1 \le i < j \le n} (x_j - x_i)$. Pertanto una matrice di Vandermonde è invertibile se e solo se la sua seconda colonna contiene tutti scalari distinti nelle coordinate. Tale matrice risulta utile nello studio dell'interpolazione di Lagrange (ossia nella dimostrazione dell'unicità del polinomio di $n-1$ grado tale che $p(\alpha_i) = \beta_i$ per i coppie (α_i, β_i) con α_i tutti distinti).

Autovalori e diagonalizzabilità

Sia $f \in \operatorname{End}(V)$. Si dice che $\lambda \in \mathbb{K}$ è un autovalore di f se e solo se $\exists\, \underline{v} \neq \underline{0}$, $\underline{v} \in V$ tale che $f(\underline{v}) = \lambda \underline{v}$, e in tal caso si dice che $\underline{v}$ è un autovettore relativo a λ. Un autovalore è tale se esiste una soluzione non nulla a $(f - \lambda Id_V)\underline{v} = \underline{0}$, ossia se e solo se:

$$\det(f - \lambda Id_V) = 0.$$

Questa relazione è ben definita dacché il determinante è invariante per qualsiasi cambio di base applicato ad una matrice associata di f. Si definisce allora $p_f(\lambda) = \det(f - \lambda Id_V)$, detto polinomio caratteristico di f, ancora invariante per matrici associate a f. Si denota inoltre con spettro di f l'insieme $sp(f)$ degli autovalori di f e con $V_\lambda = \operatorname{Ker}(f - \lambda Id_V)$ lo spazio degli autovettori relativo a λ, detto autospazio di λ.

Si definisce la molteplicità algebrica $\mu_{a,f}(\lambda)$ di un autovalore λ come la molteplicità che assume come radice del polinomio $p_f(\lambda)$. Si definisce la molteplicità geometrica $\mu_{g,f}(\lambda)$ di un autovalore λ come la dimensione del suo autospazio V_λ. Quando è noto l'endomorfismo che si sta considerando si omette la dicitura f nel pedice delle molteplicità.

- $p_f(\lambda)$ ha sempre grado $n = \dim V$,
- $p_f(\lambda)$ è sempre monico a meno del segno,
- il coefficiente di λ^n è sempre $(-1)^n$,
- il coefficiente di λ^{n-1} è $(-1)^{n+1} \operatorname{tr}(f)$,
- il termine noto di $p_f(\lambda)$ è $\det(f - 0 \cdot Id_V) = \det(f)$,
- poiché $p_f(\lambda)$ appartiene all'anello euclideo $\mathbb{K}[\lambda]$, che è dunque un UFD, esso ammette al più n radici,
- $sp(f)$ ha al più n elementi, ossia esistono al massimo n autovalori (dalla precedente considerazione),
- se $\mathbb{K} = \mathbb{C}$ e $p_f \in \mathbb{R}[\lambda]$, $\lambda \in sp(f) \iff \overline{\lambda} \in sp(f)$ (infatti λ è soluzione di p_f, e quindi anche $\overline{\lambda}$ deve esserne radice, dacché i coefficienti di p_f sono in $\mathbb{R}$),
- se $\mathbb{K}$ è un campo algebricamente chiuso, $p_f(\lambda)$ ammette sempre almeno un autovalore distinto (o esattamente n se contati con molteplicità),
- $0 \in sp(f) \iff \dim \operatorname{Ker} f > 0 \iff \operatorname{rg} f < 0 \iff \det(f) = 0$,
- autovettori relativi ad autovalori distinti sono sempre linearmente indipendenti,
- dati λ_1, ..., λ_k autovalori di f, gli spazi V_{λ_1}, ..., V_{λ_k} sono sempre in somma diretta,
- $\sum_{i=1}^k \mu_a(\lambda_i)$ corrisponde al numero di fattori lineari di $p_f(\lambda)$,
- $\sum_{i=1}^k \mu_a(\lambda_i) = n \iff p_f(\lambda)$ è completamente fattorizzabile in $\mathbb{K}[\lambda]$,
- vale sempre la disuguaglianza $n \ge \mu_a(\lambda) \ge \mu_g(\lambda) \ge 1$ (è sufficiente considerare una base di V_λ estesa a base di V e calcolarne il polinomio caratteristico sfruttando i blocchi della matrice associata, notando che $\mu_g(\lambda)$ deve forzatamente essere minore di $\mu_a(\lambda)$),
- vale sempre la disuguaglianza $n \ge \sum_{i=1}^k \mu_a(\lambda_i) \ge \sum_{i=1}^k \mu_g(\lambda_i)$,
- se $W \subseteq V$ è un sottospazio f-invariante, allora $p_{f|_W}(\lambda) \mid p_f(\lambda)$[1] (è sufficiente prendere una base di W ed estenderla a base di V, considerando poi la matrice associata in tale base, che è a blocchi),
- se $W \subseteq V$ è un sottospazio f-invariante, ed estesa una base $\mathcal{B}_W$ di W ad una $\mathcal{B}$ di V, detto $U = \operatorname{Span}(\mathcal{B} \setminus \mathcal{B}_W)$ il supplementare di W che si ottiene da tale base $\mathcal{B}$, vale che $p_f = p_{f|_W}(\lambda) \cdot p_{\hat{f}}$, dove $\hat{f} : V/W \to V/W$ è tale che $\hat{f}(\underline{u} + W) = f(\underline{u}) + W$ (come prima, è sufficiente considerare una matrice a blocchi),
- se $V = W \oplus U$, dove sia W che U sono f-invarianti, allora $p_f = p_{f|_W}(\lambda) \cdot p_{f|_U}(\lambda)$ (la matrice associata in un'unione di basi di W e U è infatti diagonale a blocchi).

[1] lavorando su endomorfismi, la notazione $f|_W$ è impiegata per considerare f ristretta a W sia sul dominio che sul codominio.

Si dice che f è diagonalizzabile se V ammette una base per cui la matrice associata di f è diagonale, o equivalentemente se, dati λ_1, ..., λ_k autovalori di f, si verifica che:

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_k}.$$

Ancora in modo equivalente si può dire che f è diagonalizzabile se e solo se:

$$\begin{cases} \sum_{i=1}^k \mu_a(\lambda_i) = n, \\ \mu_g(\lambda_i) = \mu_a(\lambda_i) \ \forall\, 1 \le i \le k, \end{cases}$$

ossia se il polinomio caratteristico è completamente fattorizzabile in $\mathbb{K}[\lambda]$ (se non lo fosse, la somma diretta $V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_k}$ avrebbe forzatamente dimensione minore di V, ed esisterebbero altri autovalori in un qualsiasi campo di spezzamento di $p_f(\lambda)$) e se $\sum_{i=1}^k \mu_g(\lambda_i) = n$. Tale condizione, in un campo algebricamente chiuso, si riduce a $\mu_g(\lambda_i) = \mu_a(\lambda_i)$, $\forall\, 1 \le i \le k$.

Considerando la forma canonica di Jordan di f, si osserva anche che f è diagonalizzabile se e solo se per ogni autovalore la massima taglia di un blocco di Jordan è esattamente 1, ossia se il polinomio minimo di f è un prodotto di fattori lineari distinti.

Data f diagonalizzabile, la matrice diagonale J a cui f è associata è, dati gli autovalori λ_1, ..., λ_k, una matrice diagonale dove λ_i compare sulla diagonale esattamente $\mu_g(\lambda_i)$ volte.

Data $A \in M(n, \mathbb{K})$, A è diagonalizzabile se e solo se f_A, l'applicazione indotta dalla matrice A, è diagonalizzabile, ossia se A è simile ad una matrice diagonale J, computabile come prima. Si scrive in particolare $p_A(\lambda)$ per indicare $p_{f_A}(\lambda)$.

Una matrice $P \in \operatorname{GL}(M(n, \mathbb{K}))$ tale che $A = PJP^{-1}$, è tale che $AP = PJ$: presa la i-esima colonna, allora, $AP^{(i)} = PJ^{(i)} = P^{(i)}$; ossia è sufficiente costruire una matrice P dove l'i-esima colonna è un autovettore relativo all'autovalore presente in J_{ii} linearmente indipendente con gli altri autovettori presenti in P relativi allo stesso autovalore (esattamente nello stesso modo in cui si costruisce in generale tale P con la forma canonica di Jordan).

Se A e B sono diagonalizzabili, allora $A \sim B \iff p_A(\lambda) = p_B(\lambda)$ (infatti due matrici diagonali hanno lo stesso polinomio caratteristico se e solo se compaiono gli stessi identici autovalori).

Se f è diagonalizzabile, allora ogni spazio W f-invariante di V è tale che:

$$W = (W \cap V_{\lambda_1}) \oplus \cdots \oplus (W \cap V_{\lambda_k}),$$

dove λ_1, ..., λ_k sono gli autovalori distinti di f.

Due endomorfismi f, $g \in \operatorname{End}(V)$ diagonalizzabili si dicono simultaneamente diagonalizzabili se esiste una base $\mathcal{B}$ di V tale per cui sia la matrice associata di f in $\mathcal{B}$ che quella di g sono diagonali. Vale in particolare che f e g sono simultaneamente diagonalizzabili se e solo se $f \circ g = g \circ f$. Per trovare tale base è sufficiente, dati λ_1, ..., λ_k autovalori di f, considerare $g|_{V_{\lambda_i}}$ $\forall\, 1 \leq i \leq k$ (V_{λ_i} è infatti g-invariante, dacché, per $\underline{v} \in V_{\lambda_i}$, $f(g(\underline{v})) = g(f(\underline{v})) = g(\lambda_i \underline{v}) = \lambda_i g(\underline{v}) \implies g(\underline{v}) \in V_{\lambda_i}$), che, essendo una restrizione di un endomorfismo diagonalizzabile su un sottospazio invariante, è diagonalizzabile: presa allora una base di autovettori di $g|_{V_{\lambda_i}}$, questi sono anche base di autovettori di V_{λ_i}; unendo tutti questi autovettori in un'unica base $\mathcal{B}$ di V, si otterrà dunque che una base in cui le matrici associate di f e g sono diagonali.

Gabriel Antonio Videtta,
https://poisson.phc.dm.unipi.it/~videtta/