



Corpi numerici.

Definizione. Un corpo C è un insieme dotato di due operazioni binarie, indicate come somma ($+ : C \times C \rightarrow C$) e prodotto (\cdot o più spesso nulla: $C \times C \rightarrow C$), verificanti le seguenti proprietà:

C con la somma è un *gruppo commutativo*, cioè:

$(a+b)+c=a+(b+c)$ per ogni $a,b,c \in C$;

esiste $0 \in C$ (zero) tale che $a+0=a=0+a$ per ogni $a \in C$;

per ogni $a \in C$ esiste $a' \in C$ (detto opposto di a , scritto $-a$) tale che $a+a'=0=a'+a$;

$a+b=b+a$ per ogni $a,b \in C$;

$C \setminus \{0\}$ con il prodotto è un *gruppo*, cioè:

$(ab)c=a(bc)$ per ogni $a,b,c \in C$;

esiste $1 \in C$ (uno) tale che $1 \cdot a = a = a \cdot 1$ per ogni $a \in C$;

per ogni $a \in C$ diverso da 0 esiste $a'' \in C$ (detto inverso di a , scritto a^{-1}) tale che $a a'' = 1 = a'' a$;

il prodotto è *distributivo* rispetto alla somma: $a(b+c)=ab+ac$ per ogni $a,b,c \in C$.

Il corpo si dice commutativo se il prodotto è commutativo; spesso un corpo commutativo si dice un campo. In un campo vale la formula del binomio di Newton: $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$ ove $n \in \mathbb{N}$ e $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.

Una funzione tra due corpi si dice un morfismo di corpi se rispetta le operazioni di somma e prodotto dei due corpi.

Un corpo si dice ordinato se in esso è definita una relazione d'ordine \geq soddisfacente alle seguenti proprietà: se $a \geq b$ allora $a+c \geq b+c$ per ogni $c \in C$; se $a \geq b$ e $c \geq 0$ allora $ac \geq bc$. Dato un corpo ordinato possiamo definire l'insieme degli elementi positivi $P \subseteq C$ come $P = \{a \in C : a > 0\}$; allora P gode delle seguenti proprietà: per ogni $c \in C$ non nullo si ha che $0 < c \in P$ oppure $-c \in P$ (e non entrambe); P è chiuso rispetto alla somma e al prodotto dei suoi elementi. Viceversa, dato un insieme P con le proprietà elencate, esiste un unico ordine su C per cui quello sia l'insieme dei positivi: $a \geq b$ se e solo se $a - b \in P$. In ogni corpo ordinato i quadrati sono positivi e in particolare $1 > 0$. Di conseguenza un corpo ordinato è in insieme infinito.

Campo razionale. L'insieme dei numeri razionali \mathbb{Q} è il più piccolo corpo contenente l'anello \mathbb{Z} dei numeri interi (in modo che le operazioni in \mathbb{Q} estendano quelle di \mathbb{Z}). È il quoziente di $\mathbb{Z} \times (\mathbb{Z} \setminus 0)$ per la relazione \sim di equivalenza definita da $(a,b) \sim (x,y)$ se e solo se $ay = bx$ (in \mathbb{Z}). La classe di (a,b) si scrive $\frac{a}{b}$, e le operazioni sono definite come d'usuale: $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$ e $\frac{a}{b} \frac{a'}{b'} = \frac{aa'}{bb'}$.

Campi finiti fondamentali. L'insieme quoziente $\mathbb{Z}/p\mathbb{Z}$ ($a \sim b$ se e solo se $a - b$ è divisibile per p), con le due operazioni ereditate da \mathbb{Z} , è un corpo se e solo se p è un numero primo. Si indica con \mathbb{F}_p ed è l'unico corpo finito con p elementi a meno di isomorfismo di corpi. Per ogni $x \in \mathbb{F}_p$ si ha $x^p = 1$ e $x^{p-1} = x$.

Caratteristica dei corpi. Per ogni corpo C vi è un'unica mappa $\mathbb{Z} \rightarrow C$ definita mandando 1 di \mathbb{Z} nell'1 di C e rispettando la somma. L'antimmagine in \mathbb{Z} dello zero (di C) contiene solo lo zero; in tal caso la funzione è iniettiva, il corpo

C contiene una copia di \mathbb{Z} e dunque di \mathbb{Q} , e C si dice di caratteristica zero;

contiene tutti i multipli di un fissato primo p ; in tal caso la funzione si fattorizza attraverso una mappa iniettiva $\mathbb{Z}/p\mathbb{Z} \rightarrow C$, il corpo C contiene una copia di $\mathbb{Z}/p\mathbb{Z}$, e C si dice di caratteristica (positiva) p . In un corpo di caratteristica p si ha che $(a+b)^p = a^p + b^p$

I corpi di caratteristica 0 sono sempre insiemi infiniti; per ogni $n \geq 1$ esiste (ed unico a meno di isomorfismi) un corpo di caratteristica p con esattamente p^n elementi (ma non è $\mathbb{Z}/p^n\mathbb{Z}$).

Campo reale. L'insieme \mathbb{R} dei numeri reali è il completamento ordinale del corpo dei numeri razionali \mathbb{Q} ; l'unico automorfismo di corpo di \mathbb{R} è l'identità.

Campo complesso. I numeri complessi $z \in \mathbb{C}$ sono espressioni $z = a + ib$, ove $a = \Re(z) \in \mathbb{R}$ si dice la parte reale di z , mentre $b = \Im(z) \in \mathbb{R}$ si dice la parte immaginaria di z . Quindi $z = \Re(z) + i\Im(z)$ per ogni $z \in \mathbb{C}$. La somma è definita per componenti (i.e. $(a+ib) + (a'+ib') = (a+a') + i(b+b')$) e il prodotto è definito ponendo $i^2 = -1$ (i.e. $(a+ib)(a'+ib') = (aa' - bb') + i(ab' + a'b)$).

coniugazione. Se z è un numero complesso, definiamo il suo coniugato \bar{z} come $\Re(z) - i\Im(z)$ (cambiamo di segno la parte immaginaria). Abbiamo allora una funzione $\mathbb{C} \rightarrow \mathbb{C}$ che è l'unico automorfismo di corpo non identico di \mathbb{C} . Rispetta le operazioni di somma ($z + z' = \bar{z} + z'$) e di prodotto ($zz' = \bar{z}\bar{z}'$). Inoltre, $z = \bar{z}$ se e solo se $z \in \mathbb{R}$; e la coniugazione è una involuzione ($\bar{\bar{z}} = z$ per ogni z), e quindi è la sua propria inversa.

norma. La norma (talvolta detta anche modulo) è la funzione $\mathbb{C} \rightarrow \mathbb{R}$ definita per ogni $z \in \mathbb{C}$ dalla radice quadrata positiva del prodotto $z\bar{z} = \Re(z)^2 + \Im(z)^2$, che risulta un numero reale. Proprietà: positività: $|z| \geq 0$ per ogni $z \in \mathbb{C}$ e $|z|=0$ se e solo se $z=0$; moltiplicatività: $|zz'| = |z||z'|$; subadditività: $|z+z'| \leq |z| + |z'|$; disuguaglianze sul quadrilatero: $||z|-|z'|| \leq |z-z'|$; $|z+z'|^2 + |z-z'|^2 = 2(|z|^2 + |z'|^2)$.

inversi. Da $|z|^2 = z\bar{z}$ si ha $z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\Re(z) - i\Im(z)}{\Re(z)^2 + \Im(z)^2}$ per ogni $z \neq 0$. Se z ha norma 1, l'inverso coincide con il coniugato.

forme esponenziale e trigonometrica. Si indica con \mathbb{S}^1 (circolo unitario del piano) l'insieme dei numeri complessi di norma 1. Se $\zeta \in \mathbb{S}^1$ allora $\zeta = \cos \vartheta + i \sin \vartheta$ con $\vartheta \in \mathbb{R}$ e si indica con $e^{i\vartheta}$. Si ha $e^{i\vartheta} e^{i\vartheta'} = e^{i(\vartheta+\vartheta')}$ e $1/e^{i\vartheta} = e^{-i\vartheta}$. Ogni $z \in \mathbb{C}$ non nullo si scrive $z = \rho \zeta$ con $\rho = |z| \in \mathbb{R} > 0$ e $\zeta = z/|z| \in \mathbb{S}^1$; dunque $z = \rho e^{i\vartheta}$ e ϑ si dice argomento di z .

formule di De Moivre. Se $z = \rho e^{i\vartheta} = \rho(\cos \vartheta + i \sin \vartheta)$ con $\rho \in \mathbb{R} > 0$, allora $z^n = \rho^n e^{in\vartheta} = \rho^n (\cos(n\vartheta) + i \sin(n\vartheta))$; da questo si ottengono le formule per le radici n -esime di z :

$$\sqrt[n]{\rho} e^{i(\frac{\vartheta}{n} + \frac{2\pi k}{n})} = \sqrt[n]{\rho} \left(\cos \left(\frac{\vartheta}{n} + \frac{2\pi k}{n} \right) + i \sin \left(\frac{\vartheta}{n} + \frac{2\pi k}{n} \right) \right)$$

per i valori interi di k compresi tra 0 ed $n-1$. In particolare le radici n -esime dell'unità, ovvero le soluzioni dell'equazione $X^n = 1$ in \mathbb{C} , sono i numeri complessi $e^{i\frac{2k\pi}{n}}$ per $k = 0, 1, \dots, n-1$; essi sono i vertici del poligono regolare con n lati inscritto nel cerchio unitario e un cui vertice sia 1.

esponenziali e logaritmi complessi. La funzione esponenziale complessa è data da $e^z = e^{a+ib} = e^a e^{ib} = e^a (\cos(b) + i \sin(b))$ se $z = a+ib$. Logaritmi complessi di z sono i numeri complessi w tali che $e^w = z$ e sono dati da $\log(\rho) + i(\vartheta + 2k\pi)$ per $k \in \mathbb{Z}$ se $z = \rho e^{i\vartheta} \neq 0$.

teorema fondamentale dell'algebra. Versione complessa: ogni polinomio non costante a coefficienti complessi ammette almeno uno zero in \mathbb{C} ; e dunque si fattorizza in fattori di primo grado. Versione reale: ogni polinomio non costante a coefficienti reali si fattorizza come prodotto di polinomi reali irriducibili che possono essere di primo grado oppure di secondo grado (e privi di radici reali, dunque con due radici complesse

coniugate). In particolare ogni polinomio reale di grado dispari ha almeno una radice reale.

Radici di equazioni polinomiali. Le equazioni polinomiali (a coefficienti in un corpo commutativo) di grado fino a 4 sono risolubili per radicali.

Secondo grado. Il polinomio aX^2+bX+c ($a \neq 0$) ha radici $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ se il campo non ha caratteristica 2; il termine $\Delta=b^2-4ac$ si dice discriminante dell'equazione e le radici sono nel campo stesso solo se Δ è un quadrato; dunque nel caso reale vi sono soluzioni reali solo se esso è nullo (una radice doppia) o positivo (due radici distinte).

Terzo grado: formule di Cardano-Tartaglia. Supponiamo che il campo abbia caratteristica diversa da 2 e 3. Il generico polinomio di terzo grado è aX^3+bX^2+cX+d ($a \neq 0$). Usando la "sostituzione di variabile" $X=Y-\frac{b}{3a}$, che permette di eliminare il termine di secondo grado, siamo ridotti a cercare le radici di un polinomio del tipo Y^3+pY+q . Si usa la sostituzione di Viète $Y=W-\frac{p}{3W}$ che dà $W^3=\frac{p^3}{27W^3}+q$ che ponendo $T=W^3$ e moltiplicando per T ci riporta ad un polinomio di secondo grado $T^2+qT-\frac{p^3}{27}$. Dalle formule risolutive otteniamo che $t_{1,2}=-\frac{q}{2} \pm \sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$. Se w è una radice cubica di t_1 , allora $w'=-\frac{p}{3w}$ è radice cubica di t_2 ; possiamo scrivere le radici come $y_{1,2,3}=w_{1,2,3}+w'_{1,2,3}$ dove w_i sono le radici cubiche di t_1 , e w'_i è la corrispondente radice cubica di t_2 tale che $w_i w'_i=-\frac{p}{3}$.

Il termine $\Delta=\frac{q^2}{4}+\frac{p^3}{27}=(\frac{q}{2})^2+(\frac{p}{3})^3$ è detto discriminante della equazione di terzo grado (qualcuno chiama discriminante il termine $D=-108\Delta=-4p^3-27q^2$); nel caso che l'equazione abbia coefficienti reali esso permette di distinguere diverse configurazioni delle radici. Se Δ è negativo, allora vi sono tre radici reali distinte; se Δ è positivo allora vi è una radice reale e due radici complesse coniugate; se Δ è zero vi sono radici multiple (un'unica radice se $p=q=0$ oppure due altrimenti).

Quarto grado: metodo di Ferrari. Il generico polinomio di quarto grado è $aX^4+bX^3+cX^2+dX+e$ ($a \neq 0$). Usando la solita "sostituzione di variabile" $X=Y-\frac{b}{4a}$, che permette di eliminare il termine di terzo grado, siamo ridotti a cercare le radici di un polinomio del tipo Y^4+pY^2+qY+r . Il metodo di Ferrari consiste ora nell'introdurre un termine U in modo tale che il polinomio si scriva come differenza di due quadrati, e di conseguenza si fattorizzi in polinomi di grado minore; completando il quadrato contenente Y^4 e pY^2 l'espressione

$$\left(Y^2 + \frac{p}{2} - \frac{U}{2}\right)^2 - \left(UY^2 - qY + \frac{U^2}{4} + \frac{pU}{2} + \frac{p^2}{4} - r\right)$$

e l'espressione nella seconda parentesi è un quadrato perfetto se il discriminante (come polinomio di secondo grado in Y) si annulla; quindi basta che u sia una radice del polinomio

$$q^2 - 4U\left(\frac{U^2}{4} + \frac{pU}{4} + \frac{p^2}{4} - r\right) = -U^3 - pU^2 - (p^2 - 4r)U + q^2$$

che è di terzo grado in U e che perciò sappiamo trattare con il metodo di Cardano-Tartaglia. Se ora u è una radice, il polinomio nelle Y si scrive

$$(Y^2 + vY + \frac{p}{2} - \frac{u}{2} - \frac{q}{2v})(Y^2 - vY + \frac{p}{2} - \frac{u}{2} + \frac{q}{2v})$$

se v è una radice quadrata di u . Siamo quindi ridotti a due polinomi di secondo grado nella Y , e le quattro radici che otteniamo sono le radici volute del polinomio di quarto grado.

Corpo dei quaternioni di Hamilton. L'insieme \mathbb{H} dei quaternioni è formato da tutte le espressioni del tipo $a+ib+jc+kd$ ove $a,b,c,d \in \mathbb{R}$ dotato delle seguenti operazioni:

somma: se $z=a+ib+jc+kd$ e $z'=a'+ib'+jc'+kd'$ allora $z+z'=a+a'+i(b+b')+j(c+c')+k(d+d')$;

prodotto: distributivo rispetto alla somma, associativo, e sui

simboli i,j,k : $\begin{array}{lll} ii=-1 & ij=k & ik=-j \\ ji=-k & jj=-1 & jk=i \\ ki=j & kj=-i & kk=-1 \end{array}$

(se $z=x+v$ e $z'=x'+v'$ con $x,x' \in \mathbb{R}$ e $v,v' \in \mathbb{R}^3$, allora $zz'=(xx'-v \cdot v')+(xv'+x'v+v \wedge v')$: interpretazione geometrica del prodotto di quaternioni). Il corpo dei quaternioni non è commutativo. Se $z=a+ib+jc+kd$ allora a si dice la parte reale di z , e $ib+jc+kd$ la parte immaginaria; un quaternione si dice puramente reale (risp. immaginario) se coincide con la sua parte reale (risp. immaginaria).

coniugazione. Dato $z=a+ib+jc+kd \in \mathbb{H}$, definiamo il suo coniugato $\bar{z}=a-ib-jc-kd$. Otteniamo così una applicazione di \mathbb{H} in sé che soddisfa alle seguenti proprietà: rispetta la somma: $z+\bar{z}'=\bar{z}+z'$; $\bar{z}=z$ se e solo se z è (puramente) reale; (anti)rispetta il prodotto: $\bar{zz'}=\bar{z'}\bar{z}$; $\bar{z}\bar{z}=z\bar{z}=a^2+b^2+c^2+d^2$ è puramente reale per ogni $z=a+ib+jc+kd$, e si tratta di un numero positivo (se $z \neq 0$); $\bar{\bar{z}}=z$ per ogni z (dunque di tratta di un isomorfismo involutorio).

norma. La norma è la funzione di \mathbb{H} in $\mathbb{R}_{>0}$ definita per ogni quaternione z da $|z|^2=z\bar{z}$; essa verifica le seguenti proprietà: positività: $|z| \geq 0$ per ogni $z \in \mathbb{C}$ e $|z|=0$ se e solo se $z=0$; moltiplicatività: $|zz'|=|z||z'|$; subaddittività: $|z+z'| \leq |z|+|z'|$. I quaternioni di norma 1 si scrivono $\cos\vartheta + (ix+iy+iz)\sin\vartheta$ con $x^2+y^2+z^2=1$.

inversi. Se z è quaternione non nullo, allora l'inverso di z è $z^{-1}=\frac{\bar{z}}{|z|^2}$. Se z è di norma 1, l'inverso coincide con \bar{z} .

interpretazione geometrica. Ogni quaternione $\zeta=\cos\vartheta+v\sin\vartheta$, con $v=(ia+jb+kc)$, di norma 1 determina una funzione $\varphi_\zeta(w)=\zeta w \bar{\zeta}$ sui quaternioni puramente immaginari $w=ix+jy+kz$ che è una rotazione di angolo 2ϑ attorno all'asse v . Si ha $\varphi_\zeta=\varphi_{\zeta'}$ se e solo se $\zeta'=\pm\zeta$, e $\varphi_{\zeta\zeta'}=\varphi_\zeta\varphi_{\zeta'}$ (la composizione di rotazioni corrisponde al prodotto di quaternioni).

Matrici.

Una matrice $n \times m$ a valori in un corpo C è una funzione $\{1, \dots, n\} \times \{1, \dots, m\} \rightarrow C$,

i.e. una struttura:

$$A=\left(a_{i,j}\right)_{\substack{i=1, \dots, n \\ j=1, \dots, m}}=\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix};$$

l'insieme di queste matrici di indica con $M_{n,m}(C)$. Scrittura per colonne e per righe:

$$A=\left(A_{(1)} \cdots A_{(m)}\right)=\begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(n)} \end{pmatrix}, \quad A_{(i)} \in M_{n,1}(C), A^{(j)} \in M_{1,m}(C).$$

Operazioni tra matrici:

prodotto per scalari (elementi di C): $cA:=(ca_{i,j})$.

somma: $A, B \in M_{n,m}(C)$, $A+B:=(b_{i,j}+a_{i,j}) \in M_{n,m}(C)$.

prodotto: $A \in M_{n,m}(C)$ e $B \in M_{m,l}(C)$,

$$AB:=\left(\sum_{j=1}^m a_{i,j} b_{j,k}\right)_{\substack{i=1, \dots, n \\ k=1, \dots, l}}=\left(A^{(i)} B_{(k)}\right) \in M_{n,l}(C).$$

La somma di matrici è commutativa, associativa, ammette elemento neutro (matrice nulla) e opposto per ogni elemento dato; il prodotto tra matrici è associativo ma in generale non commutativo, ed è distributivo rispetto alla somma; il prodotto per gli scalari si può interpretare come prodotto tra matrici, ed è quindi associativo e compatibile con esso.

Trasposizione. Sia $A \in M_{n,m}(C)$; definiamo $A^t \in M_{m,n}(C)$ tramite: $A^t:=\left(a_{i,j}\right)_{\substack{j=1, \dots, m \\ i=1, \dots, n}}$.

Si ha che $(A^t)^t = A$, $(A+B)^t = A^t + B^t$, $\mathbb{I}^t = \mathbb{I}$, $(AB)^t = B^t A^t$.

Matrici quadrate. Le matrici quadrate di un fissato ordine formano un'algebra associativa, ma non commutativa, con le operazioni introdotte. In $M_n(C) = M_{n,n}(C)$ esiste la matrice identica $\mathbb{I} := (\delta_{i,j})$ ove $\delta_{i,j}=1$ se $i=j$ e 0 altrimenti (delta di Kronecker), che è elemento neutro per la moltiplicazione. Il determinante di $A \in M_n(C)$ è l'elemento di C definito da

$$\det A = |A| := \sum_{\sigma \in \mathcal{P}_n} \prod_{i=1}^n a_{i,\sigma(i)}$$

ove \mathcal{P}_n indica l'insieme delle permutazioni sull'insieme $\{1, \dots, n\}$, e si calcola mediante gli sviluppi di Laplace per riga o colonna:

$$|A| = \sum_{j=1}^n (-1)^{i+j} a_{i,j} |A_{i,j}| = \sum_{i=1}^n (-1)^{i+j} a_{i,j} |A_{i,j}|$$

ove $A_{i,j} \in M_{n-1}$ è la matrice che si ottiene da A eliminando la i -esima riga e la j -esima colonna. $\det: M_n(C) \rightarrow C$ è l'unica funzione che sia multilinear sulle colonne (e sulle righe) e valga 1 sulla matrice identica. Come polinomio nelle entrate $a_{i,j}$ della matrice, $\det(A)$ è omogeneo di grado n ed irriducibile.

Annnullamenti o sviluppi (con cofattori) alieni: si ha che

$$\sum_{j=1}^n (-1)^{i+j} a_{k,j} |A_{i,j}| = 0 = \sum_{i=1}^n (-1)^{i+j} a_{i,k} |A_{i,j}|$$

per ogni $k \neq i$ (risp. $k \neq j$), poiché si tratta di sviluppi di Laplace di matrici con due righe (risp. colonne) uguali.

sviluppi di Laplace generalizzati. Sia K sottinsieme (ordinato) di $\{1, 2, \dots, n\}$ e indichiamo con $K' = \{1, 2, \dots, n\} \setminus K$ il complementare (ordinato). Sia $\epsilon(K, K')$ il segno della permutazione che manda i nell' i -esimo elemento della lista (K, K') . Allora

$$\det A = \epsilon(K, K') \sum_H \epsilon(H, H') \det A_{H, K} \det A_{H', K'}$$

dove la sommatoria è estesa a tutti i sottinsiemi H di $\{1, 2, \dots, n\}$ aventi la stessa cardinalità di K , H' è l'insieme complementare, $A_{H, K}$ indica la sottomatrice quadrata che si ottiene selezionando le righe (risp. le colonne) di indici in H (risp. in K).

Inoltre (sviluppi alieni): $\sum_H \epsilon(H, H') \det A_{H, K} \det A_{H', L} = 0$ per ogni $L \subseteq \{1, 2, \dots, n\}$ della stessa cardinalità di K' ma diverso da K' .

Casi notevoli di determinanti:

se la matrice è *triangolare* (inferiore se $a_{i,j}=0$ per $i > j$; superiore se $a_{i,j}=0$ per $i < j$) allora il determinante è il prodotto degli elementi in diagonale;

se la matrice è *a blocchi*: $\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A) \det(D) = \det \begin{pmatrix} A_0 \\ C & D \end{pmatrix}$, con A e D matrici quadrate;

det. di *Vandermonde*: $\det \begin{pmatrix} (x_i^k)_{i=0, \dots, n} \\ k=0, \dots, n \end{pmatrix} = \prod_{0 \leq i < j \leq n} (x_j - x_i)$;

det. di *Vandermonde generalizzati*:

$$\begin{aligned} \det \begin{pmatrix} (x_i^{\alpha_k})_{i=0, \dots, n} \\ k=0, \dots, n \end{pmatrix} &= \prod_{0 \leq i < j \leq n} (x_j - x_i) \det \begin{pmatrix} h_{\alpha_j-i}(x_0, \dots, x_n) \end{pmatrix}_{i, \alpha_j} \\ &= \prod_{0 \leq i < j \leq n} (x_j - x_i) \det \begin{pmatrix} p_{n-\beta_k+i}(x_0, \dots, x_n) \end{pmatrix}_{i, \beta_k} \end{aligned}$$

ove α_i è una successione crescente di interi positivi, β_k è la successione crescente complementare, i polinomi simmetrici elementari $p(x_1, \dots, x_n)$ sono definiti da

$$p(x_1, x_2, \dots, x_n, T) = \prod_{i=1}^n (1 - x_i T) = \sum_{j=0}^n (-1)^j p_j(x_1, x_2, \dots, x_n) T^j$$

(dunque $p_0=1$, $p_1=\sum_i x_i$, $p_2=\sum_{i < j} x_i x_j$, ed in generale p_j è la somma degli $\binom{n}{j}$ prodotti degli x_i presi a j a j senza ripetizioni) e i polinomi simmetrici elementari completi $h(x_0, \dots, x_n)$ sono definiti da

$$h(x_1, x_2, \dots, x_n, T) = \prod_{i=1}^n \frac{1}{1 - x_i T} = \sum_{j=0}^{\infty} h_j(x_1, x_2, \dots, x_n) T^j$$

(dunque $h_0=1$, $h_1=\sum_i x_i$, $h_2=\sum_i x_i^2 + \sum_{i < j} x_i x_j$, ed in generale h_j è la somma degli $\binom{n+j-1}{j}$ monomi di grado j negli x_i); dalla relazione $ph=1$ si ottiene per ogni $k \leq 1$ la formula $\sum_{i+j=k} (-1)^i p_i h_j = 0$.

det. di *Vandermonde derivati (confluenti)*: se $m \leq n$ e

$$D_{m,n}(x) = \left(\begin{pmatrix} x_j \\ i-1 \end{pmatrix}^{x_j-i} \right)_{i,j} \in M_{m,n}(C)$$

abbiamo che per ogni partizione n_1, n_2, \dots, n_s di n

$$\det(D_{n_i, n}(x_i)) = \prod_{i < j} (x_j - x_i)^{n_i n_j} .$$

alternanti doppi di *Cauchy*:

$$\det \left(\frac{1}{y_i - x_j} \right)_{i,j} = \frac{\prod_{i < j} (x_i - x_j) \prod_{i < j} (y_j - y_i)}{\prod_{i,j} (y_i - x_j)} .$$

una matrice quadrata si dice *antisimmetrica* se $A^t = -A$; se A è antisimmetrica di ordine dispari, allora $|A|=0$; inoltre

$$\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix} = (af + be - cd)^2 .$$

In generale, il determinante di una matrice antisimmetrica d'ordine dispari $2n+1$ è il quadrato d'un polinomio nei suoi coefficienti, che si chiama Pfaffiano d'ordine n ed è dato da

$$Pf^n(x_{i,j}) = \sum_{\substack{1 \leq i_s < j_s \leq n \\ (1 \leq s \leq n)}} \operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & 2n-1 & 2n \\ i_1 & j_1 & i_2 & j_2 & \cdots & i_n & j_n \end{pmatrix} \prod_s x_{i_s, j_s}$$

ove la sommatoria comprende $(2n-1)!!$ termini (e sono tutti i prodotti di n termini $x_{i,j}$ ove $i < j$ e gli indici sono tutti diversi).

det. *circolanti* sono quelli delle matrici (reali o complesse) in cui ogni riga si ottiene "circolando di una posizione a destra"

$$\text{la precedente: } \det((a_{j-i+1+[n]})_{i,j=1, \dots, n}) = \prod_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{i,j} \omega^{ij} ,$$

ove $[+n]$ indica di sommare n se il risultato non è positivo, ω è una radice complessa n -esima primitiva dell'unità.

La matrice circolante di termini $a, a+d, a+2d, \dots, a+(n-1)d$ ha determinante $(-nd)^{n-1} (a + \frac{n-1}{2}d)$. In particolare abbiamo che la matrice circolante di termini $1, 2, \dots, n$ ha determinante $\frac{n+1}{2}(-n)^{n-1}$.

La matrice d'ordine n avente entrate non diagonali tutte uguali ad 1 ed entrate diagonali uguali ad $1-x$ vale $(n-x)(-x)^{n-1} = (-1)^n x^{n-1} (x-n)$; si può vedere con le riduzioni elementari consistenti nel sottrarre alla prima riga tutte le altre, poi raccogliere il termine comune, e infine sottrarre la prima riga a tutte le altre.

Gruppo Generale Lineare. La matrice $A \in M_n(C)$ si dice *invertibile* se esiste $B \in M_n(C)$ tale che $AB = \mathbb{I} = BA$ (tale B è unica e si dice l'inversa di A). Basta per questo che $AB = \mathbb{I}$ o che $BA = \mathbb{I}$. Una matrice è invertibile se e solo se il suo determinante è diverso da zero.

Se $A \in M_n(C)$, la matrice dei complementi algebrici $A^c \in M_n(C)$ è la matrice che nella posizione i,j ha il termine $(-1)^{i+j} |A_{j,i}|$.

Formule notevoli: $\mathbb{I}^c = \mathbb{I}$, $\det(A^c) = \det(A)^{n-1}$, $(A^c)^c = \det(A)^{n-2} A$, $(AB)^c = B^c A^c$; per ogni matrice si ha $AA^c = A^c A = |A| \mathbb{I}$.

Se $A \in M_n(C)$ è invertibile la sua matrice inversa si indica con A^{-1} e si calcola tramite: $A^{-1} = \frac{A^c}{|A|} = \frac{1}{|A|} ((-1)^{i+j} |A_{j,i}|)_{i=1, \dots, n, j=1, \dots, n}$.

Formule notevoli: $\mathbb{I}^{-1} = \mathbb{I}$, $(A^{-1})^{-1} = A$, $(AB)^{-1} = B^{-1} A^{-1}$, $(A^t)^{-1} = (A^{-1})^t$ se le matrici A e B sono invertibili.

Il sottinsieme di $M_n(C)$ delle matrici invertibili si indica con $\operatorname{GL}(n, C)$ o $\operatorname{GL}_n(C)$, e si tratta di un gruppo (non commutativo) sotto il prodotto di matrici. Il determinante si restringe ad un morfismo di gruppi $\det: \operatorname{GL}_n(C) \rightarrow C^\times$ tra il gruppo delle

matrici invertibili con l'operazione di prodotto e il gruppo degli elementi non nulli di C con l'operazione di prodotto.

Gruppo Speciale Lineare. L'insieme delle matrici di determinante 1 è un sottogruppo di $\mathrm{GL}_n(C)$ che si dice il Gruppo Speciale Lineare e si indica con $\mathrm{SL}(n,C)$ o $\mathrm{SL}_n(C)$. Se $A \in \mathrm{SL}_n(C)$, allora $A^{-1} = A^c$.

Operazioni elementari. Sia $A \in M_{n,m}(C)$; le *operazioni elementari sulle righe* corrispondono a moltiplicare a sinistra (o pre-moltiplicare) la matrice A per opportune matrici invertibili $H \in M_n(C)$:

scambiare di posto le righe i -esima e j -esima; si tratta di moltiplicare per $S(i,j) := \mathbb{I} + e_{i,j} + e_{j,i} - e_{i,i} - e_{j,j}$;

moltiplicare la riga i -esima per $\alpha \in C$; si tratta di moltiplicare per $H(i,\alpha) := \mathbb{I} + (\alpha - 1)e_{i,i}$;

sostituire la i -esima riga con la somma di quella riga e il prodotto di $\alpha \in C$ per la j -esima riga; si tratta di moltiplicare per $H(i,j,\alpha) := \mathbb{I} + \alpha e_{i,j}$.

Tramite operazioni elementari sulle righe ogni matrice può essere ridotta in forma a scalini (per righe), i.e. tale che se $a_{i,j}$ è il primo elemento non nullo della i -esima riga, allora $i \leq j$; ogni matrice quadrata invertibile può essere ridotta per righe alla matrice identica, e questa riduzione permette il calcolo dell'inversa: $(A\mathbb{I})$ viene ridotta (per righe) a $(\mathbb{I}A^{-1})$.

Le *operazioni elementari sulle colonne* corrispondono a moltiplicare a destra (o post-moltiplicare) la matrice A per opportune matrici invertibili $H \in M_m(C)$:

scambiare di posto le colonne i -esima e j -esima; si tratta di moltiplicare per $S(i,j) := \mathbb{I} + e_{i,j} + e_{j,i} - e_{i,i} - e_{j,j}$;

moltiplicare la colonna i -esima per $\alpha \in C$; si tratta di moltiplicare per $H(i,\alpha) := \mathbb{I} + (\alpha - 1)e_{i,i}$;

sostituire la i -esima colonna con la somma di quella colonna e il prodotto di $\alpha \in C$ per la j -esima colonna; si tratta di moltiplicare per $H(i,j,\alpha) := \mathbb{I} + \alpha e_{j,i}$.

Tramite operazioni elementari sulle colonne ogni matrice può essere ridotta in forma a scalini (per colonne), i.e. tale che se $a_{i,j}$ è il primo elemento non nullo della j -esima colonna, allora $j \leq i$.

Rango. Il rango di una matrice $A \in M_{n,m}(C)$ è per definizione il massimo numero di colonne linearmente indipendenti. Ciò corrisponde al numero di colonne non nulle se la matrice è ridotta in forma a scalini per colonne. Equivalentemente è il massimo numero di righe linearmente indipendenti, che corrisponde al numero di righe non nulle se la matrice è ridotta in forma a scalini per righe. Il rango si indica con $\mathrm{rk}(A)$ e si caratterizza come il massimo ordine delle sottomatrici quadrate invertibili.

I minori di ordine k della matrice $A \in M_{n,m}(C)$ sono i determinanti delle sottomatrici quadrate di ordine k di A che si ottengono cancellando $n-k$ righe ed $m-k$ colonne di A . Il rango di una matrice coincide con il massimo ordine di un minore non nullo: la matrice A ha rango k se e solo se esiste un minore non nullo d'ordine k e tutti i minori d'ordine maggiore di k sono nulli.

Matrici di Minori e Complementi. Data $A \in M_n(C)$, per ogni $k \leq n$ definiamo $M^{(k)}(A)$ la k -esima matrice composta o matrice dei minori d'ordine k come

$$M^{(k)}(A) := \left(\begin{vmatrix} A_{(J)}^{(I)} \end{vmatrix} \right)_{\substack{|I|=k \\ |J|=k}}$$

con l'ordine lessicografico degli indici I e J ; e $C^{(k)}(A)$ la k -esima matrice complementare composta o matrice dei minori complementari segnati d'ordine $n-k$ come

$$C^{(k)}(A) := \left(\epsilon(I, I') \epsilon(J, J') \begin{vmatrix} A_{(J')}^{(I')} \end{vmatrix} \right)_{\substack{|I|=k \\ |J|=k}}^t$$

con l'ordine lessicografico degli indici I e J (si tratta della matrice trasposta della matrice $M^{(k)}(A)$ in cui ogni minore è stato sostituito con il suo complemento segnato).

Si ha subito che $M^{(1)}(A) = A$ e $C^{(1)}(A) = A^c$. Si osservi anche che $M^{(k)}(A)^t = M^{(k)}(A^t)$ e analogamente $C^{(k)}(A)^t = C^{(k)}(A^t)$.

Teorema del rango. Il rango di A è uguale ad r se e solo se $M^{(r)}(A) \neq \mathbb{O}$ e $M^{(r+1)}(A) = \mathbb{O}$; più in generale, il rango di $M^{(k)}(A)$ è uguale a $\binom{r}{k}$.

Teorema del prodotto di composte e loro complementari. Per ogni $k \leq n$ risulta $M^{(k)}(A)C^{(k)}(A) = C^{(k)}(A)M^{(k)}(A) = |A| \mathbb{I}_{\binom{n}{k}}$.

Teorema di Binet-Cauchy. Per ogni $k \leq n$ risulta:

$$M^{(k)}(\mathbb{I}_n) = \mathbb{I}_{\binom{n}{k}}; M^{(k)}(AB) = M^{(k)}(A)M^{(k)}(B);$$

$$C^{(k)}(\mathbb{I}_n) = \mathbb{I}_{\binom{n}{k}}; C^{(k)}(AB) = C^{(k)}(B)C^{(k)}(A);$$

per ogni $A, B \in M_n(C)$.

Teorema di Cauchy-Sylvester. Per ogni $k \leq n$ risulta

$$|M^{(k)}(A)C^{(k)}(A)| = |A|^{\binom{n}{k}}; \text{ inoltre}$$

$$|M^{(k)}(A)| = |A|^{\binom{n-1}{k-1}} \text{ e } |C^{(k)}(A)| = |A|^{\binom{n-1}{k}}.$$

Teorema (inverse di composte e loro complementari). Per ogni $k \leq n$ e per ogni matrice invertibile A , risulta

$$M^{(k)}(A)^{-1} = M^{(k)}(A^{-1}) = |A|^{-1} C^{(k)}(A);$$

$$C^{(k)}(A)^{-1} = C^{(k)}(A^{-1}) = |A|^{-1} M^{(k)}(A).$$

Teorema di Franke. Per ogni $h, k \leq n$ risulta

$$C^{(h)}(M^{(k)}(A)) = |A|^{\binom{n-1}{k-1} - h} M^{(h)}(C^{(k)}(A));$$

$$C^{(h)}(C^{(k)}(A)) = |A|^{\binom{n-1}{k} - h} M^{(h)}(M^{(k)}(A)).$$

Teorema di Jacobi. $M^{(h)}(A^c) = |A|^{h-1} C^{(h)}(A)$ per ogni $h \leq n$.

Spazi Vettoriali.

Definizioni. Uno spazio vettoriale su un corpo C è il dato di un insieme V dotato di due operazioni:

prodotto per gli scalari: $C \times V \rightarrow V: (\alpha, v) \mapsto \alpha v$;

somma di vettori: $V \times V \rightarrow V: (v, w) \mapsto v + w$;

soggetti ai seguenti assiomi:

V con l'operazione di somma è un *gruppo abeliano*; dunque esiste un elemento neutro 0 tale che $v + 0 = v = 0 + v$ ($\forall v$); l'operazione è associativa, $u + (v + w) = (u + v) + w$ ($\forall u, v, w$); l'operazione è commutativa, $v + w = w + v$ ($\forall v, w$); ogni elemento ha opposto, $(\forall v)(\exists w)v + w = 0 = w + v$;

l'operazione di moltiplicazione per gli scalari è: unitaria: $1v = v$ ($\forall v$); associativa: $\alpha(\beta v) = (\alpha\beta)v$ ($\forall \alpha, \beta, v$); distributiva a sinistra: $(\alpha + \beta)v = \alpha v + \beta v$ ($\forall \alpha, \beta, v$); distributiva a destra: $\alpha(v + w) = \alpha v + \alpha w$ ($\forall \alpha, v, w$).

Indipendenza lineare, basi. Sia $S \subseteq V$ un sottinsieme di uno spazio vettoriale; S si dice *linearmente indipendente (li)* se per ogni combinazione lineare $\sum_{s \in S} \alpha_s s$ (in cui quasi tutti gli α_s siano nulli) si ha che: $\sum_{s \in S} \alpha_s s = 0$ implica $\alpha_s = 0$ per ogni s . In caso contrario (esistono combinazioni non banali che danno il vettore nullo) S si dice un insieme linearmente dipendente (*ld*).

L'insieme S si dice un insieme di *generatori* per V se ogni elemento $v \in V$ si può scrivere come $v = \sum_{s \in S} \alpha_s s$ (con gli α_s quasi tutti nulli).

Un insieme S è un insieme massimale di vettori linearmente indipendenti se e solo se S è un insieme minimale di generatori per V ; inoltre ogni tale insieme si dice una base di V , è di

una fissata cardinalità, dipendente solo da V e da C , che si chiama la dimensione di V su C , e si indica $\dim_C V$ (teorema di esistenza delle basi).

Dato un insieme S e una base B di V , si può completare S a una base di V aggiungendovi opportuni elementi di B (teorema della base incompleta).

Sottospazi. Un sottinsieme W di uno spazio vettoriale V si dice un sottospazio vettoriale, e si indica $W \leq V$, se le operazioni di V inducono una struttura di spazio vettoriale su W . Ciò succede se e solo se valgono le seguenti condizioni:

$0 \in W$; se $u, v \in W$ allora $u+v \in W$; se $u \in W$ e $\alpha \in C$ allora $\alpha u \in W$; ovvero se e solo se valgono le:

$W \neq \emptyset$; se $u, v \in W$ e $\alpha, \beta \in C$ allora $\alpha u + \beta v \in W$.

Se $W \leq V$ allora $\dim_C W \leq \dim_C V$.

Spazi generati. Se S è un sottinsieme qualsiasi di V , indichiamo con $\langle S \rangle$ il più piccolo sottospazio vettoriale di V contenente S ; si tratta dell'intersezione di tutti i sottospazi vettoriali di V contenenti S ; o ancora dell'insieme di tutte le combinazioni lineari (finite) di elementi di S a coefficienti in C .

Formule delle dimensioni per i sottospazi. Siano W_1 e W_2 sottospazi vettoriali di V . L'intersezione insiemistica $W_1 \cap W_2$ è un sottospazio vettoriale; per contro l'unione $W_1 \cup W_2$ non è un sottospazio, e definiamo $W_1 + W_2 := \langle W_1 \cup W_2 \rangle$ i.e. il sottospazio vettoriale generato.

Vale la relazione (formula della dimensione per i sottospazi) $\dim_C W_1 + \dim_C W_2 = \dim_C(W_1 + W_2) + \dim_C(W_1 \cap W_2)$ (formula di Grassmann).

Se $W_1 + W_2 = V$ e $W_1 \cap W_2 = \{0\}$ si dice che W_1 e W_2 sono complementari e si scrive $V = W_1 \oplus W_2$; in tal caso si ha $\dim_C V = \dim_C(W_1) + \dim_C(W_2)$.

Quozienti. Sia W un sottospazio vettoriale di V ; allora la relazione " $u \sim v$ sse $u - v \in W$ " definisce una relazione di equivalenza in V che rispetta la struttura di spazio vettoriale, di modo che l'insieme quoziente $V/W := V/\sim$ ha una struttura canonica di spazio vettoriale indotta da quella di V . Si ha che $\dim_C V = \dim_C W + \dim_C(V/W)$.

Applicazioni Lineari.

Definizioni. Una applicazione $\varphi: V \rightarrow W$ si dice lineare se $\varphi(u+v) = \varphi(u) + \varphi(v)$ ($\forall u, v \in V$) e $\varphi(\alpha v) = \alpha \varphi(v)$ ($\forall v \in V, \forall \alpha \in C$); o equivalentemente

$\varphi(\alpha u + \beta v) = \alpha \varphi(u) + \beta \varphi(v)$ ($\forall u, v \in V, \forall \alpha, \beta \in C$).

Se φ è lineare si ha $\varphi(0) = 0$ e $\varphi(-v) = -\varphi(v)$.

Una applicazione lineare è determinata e unicamente definita dai valori assunti su una base del dominio (teorema di estensione).

I sottoinsiemi $\ker \varphi := \{v \in V \mid \varphi(v) = 0\}$ di V (nucleo o kernel di φ) e $\text{im } \varphi := \{w \in W \mid w = \varphi(v) \exists v \in V\}$ di W (immagine di φ) sono sottospazi vettoriali di V e W rispettivamente.

Se $\dim_C V$ è finita, allora $\dim_C V = \dim_C \ker \varphi + \dim_C \text{im } \varphi$ (formula delle dimensioni per un morfismo).

Il morfismo φ induce un isomorfismo (cioè una mappa invertibile) $\bar{\varphi}: V/\ker \varphi \rightarrow \text{im } \varphi$ (primo teorema di isomorfismo).

Se $\dim_C V = \dim_C W$ è finita, allora φ è un isomorfismo se e solo se $\ker \varphi = \{0\}$, ovvero se e solo se $\text{im } \varphi = W$.

L'insieme $\text{Hom}_C(V, W)$ formato dalle applicazioni lineari di V in W è uno spazio vettoriale su C tramite la struttura di W , ed ha dimensione $\dim_C(V) \dim_C(W)$ (prodotto delle due).

Somme e Prodotti. Data una famiglia \mathcal{I} di indici, e un insieme di spazi vettoriali V_i al variare di $i \in \mathcal{I}$, definiamo la

somma diretta $\bigoplus_{i \in \mathcal{I}} V_i$ e il prodotto diretto $\prod_{i \in \mathcal{I}} V_i$ come gli insiemi formati dalle \mathcal{I} -uple (v_i) di elementi con $v_i \in V_i$ per ogni i , e quasi tutti nulli (i.e. nulli tranne che per un numero finito di indici) nel caso della somma diretta. Si hanno strutture canoniche di spazio vettoriale su C con le operazioni "componente per componente".

In particolare la somma diretta è un sottospazio vettoriale del prodotto diretto, e se l'insieme di indici è finito, allora le due nozioni coincidono; abbiamo dei morfismi canonici di inclusione $\iota_j: V_j \rightarrow \bigoplus_{i \in \mathcal{I}} V_i$ e di proiezione $\pi_j: \prod_{i \in \mathcal{I}} V_i \rightarrow V_j$ per ogni j . Per ogni spazio vettoriale W su C , vi sono i seguenti isomorfismi $\text{Hom}_C(\bigoplus_{i \in \mathcal{I}} V_i, W) \cong \prod_{i \in \mathcal{I}} \text{Hom}_C(V_i, W)$ e $\text{Hom}_C(W, \prod_{i \in \mathcal{I}} V_i) \cong \prod_{i \in \mathcal{I}} \text{Hom}_C(W, V_i)$ dati dalle composizioni con le inclusioni e le proiezioni.

Il morfismo di inclusione $W_1 \rightarrow W_1 + W_2$ induce un isomorfismo $W_1/(W_1 \cap W_2) \rightarrow (W_1 + W_2)/W_2$ (secondo teorema di isomorfismo).

Se abbiamo $W_1 \supseteq W_2$ sottospazi di V , il morfismo canonico $V/W_2 \rightarrow V/W_1$ induce un isomorfismo $(V/W_2)/(W_1/W_2) \rightarrow V/W_1$ (terzo teorema di isomorfismo).

Coordinate. L'insieme C^n dotato delle operazioni "componente per componente" è uno spazio vettoriale su C di dimensione n e base canonica data dai vettori $e_i := (\delta_{ij})$. Si indica con $V_n(C)$ e si dice lo spazio vettoriale standard su C di dimensione n . Sia V uno spazio vettoriale su C di dimensione finita $n := \dim_C V$ e scegliamo una base $e = (e_1, \dots, e_n)$ di V . Questo determina un isomorfismo $V_n(C) \rightarrow V$ mandando la base canonica di $V_n(C)$ nella base scelta. In particolare $v \in V$ si scrive unicamente come $v = \sum_i x_i e_i$ con $x_i \in C$; le coordinate di v nella base data è la n -pla $(x_1, \dots, x_n)^t$.

Se W è un altro spazio vettoriale su C di dimensione finita $m := \dim_C W$, e $g = (g_1, \dots, g_m)$ è una base di W , e se $\varphi: V \rightarrow W$ è una applicazione lineare, allora possiamo associare a φ una matrice $\alpha_{e,g}(\varphi) \in M_{m,n}(C)$ tramite la definizione: $\varphi(e_1, \dots, e_n) = (g_1, \dots, g_m) \alpha_{e,g}(\varphi)$; cioè le colonne di $\alpha_{e,g}(\varphi)$ sono le coordinate nella base di W delle immagini tramite φ dei vettori della base di V .

Se v ha coordinate $x = (x_1, \dots, x_n)^t$, allora le coordinate di $\varphi(v)$ nella base di W sono date da $\varphi(x) = \alpha_{e,g}(\varphi)x$.

Effetto dei cambiamenti di base: se e' è un'altra base di V e g' un'altra base di W , allora la matrice $\alpha_{e',g'}(\varphi)$ è legata alla precedente tramite le matrici di cambiamento di base $\alpha_{e',e}(\text{id}_V)$ e $\alpha_{g,g'}(\text{id}_W)$ dalla formula $\alpha_{e',g'}(\varphi) = \alpha_{g,g'}(\text{id}_W) \alpha_{e,g}(\varphi) \alpha_{e',e}(\text{id}_V)$.

Si osservi che le matrici di cambiamento di base sono invertibili e si ha $\alpha_{e',e}(\text{id}_V) = \alpha_{e,e'}(\text{id}_V)^{-1}$.

In particolare nel caso $\dim_C V = \dim_C W$ allora φ è un isomorfismo se e solo se per qualunque scelta delle basi si ha che la matrice $\alpha_{e,g}(\varphi)$ è invertibile.

Nel caso che $V = W$ intendiamo sempre scegliere la stessa base su dominio e codominio, sicché la formula di cambiamento di base diventa $\alpha_{e',e}(\varphi) = \alpha_{e,e'}(\text{id}_W) \alpha_{e,e}(\varphi) \alpha_{e',e}(\text{id}_V)$.

Se $\psi: W \rightarrow U$ è un'altra applicazione lineare, e $h = (h_1, \dots, h_l)$ una base di U , allora $\alpha_{e,h}(\psi \circ \varphi) = \alpha_{g,h}(\psi) \alpha_{e,g}(\varphi)$ (la composizione di applicazioni lineari corrisponde alla moltiplicazione di matrici).

Descrizione di sottospazi. Se V è spazio vettoriale su C di dimensione finita n , ogni sottospazio W di V può essere descritto come immagine di una applicazione lineare iniettiva $i: V_m(C) \rightarrow V$ (descrizione parametrica o tramite generatori), oppure come nucleo di una applicazione lineare suriettiva $p: V \rightarrow V_c(C)$ ove $c = n - m$ si dice la codimensione di W in V (descrizione cartesiana). Scelta una base b di V (e la base canonica

e sugli spazi standard), le colonne di $\alpha_{e,b}(i)$ sono le coordinate dei generatori di W nella base b , e le righe di $\alpha_{b,e}(p)$ sono i coefficienti delle equazioni di un sistema di equazioni per W . Dunque il numero minimo m di generatori (dimensione di W) e il numero minimo c di equazioni cartesiane per W (codimensione di W in V) sono legati da $m+c=n$.

Principio dei minori orlati. Data una base di W si possono ottenere equazioni cartesiane di W annullando tutti i minori d'ordine $m+1$ che si ottengono orlando un fissato minore non nullo d'ordine m della matrice formata dai generatori dati cui si aggiunga la colonna delle variabili.

Forme canoniche per similitudine. Due matrici quadrate $A, B \in M_n(C)$ si dicono simili se esiste una matrice invertibile $P \in GL(n,C)$ tale che $B = PAP^{-1}$. Due matrici sono simili se e solo se rappresentano la stessa applicazione lineare di C^n in sè in due basi diverse (legate dal cambiamento di base dato da P). La relazione di similitudine è una relazione di equivalenza tra matrici.

Sia $A \in M_n(C)$ rappresentante l'applicazione φ di C^n in sè nella base canonica, $v \in C^n$ non nullo; allora v si dice autovettore di A (o di φ) di autovalore $\lambda \in C$ se $Av = \lambda v$ (o $\varphi(v) = \lambda v$), e $\lambda \in C$ si dice un autovalore di A (o di φ) se esiste un vettore $v \in C^n$ non nullo tale che $Av = \lambda v$.

Uno scalare $\lambda \in C$ è un autovalore di A (risp. di φ) se e solo se $\det(A - \lambda \mathbb{I}) = 0$ (risp. $\ker(\varphi - \lambda \text{id}) \neq \{0\}$).

Il polinomio caratteristico di A è

$$p_A(x) := \det(A - x\mathbb{I}) = x^n - \text{tr}(A)x^{n-1} + \dots + (-1)^n \det(A);$$

è invariante per similitudine, e dunque si può chiamare anche polinomio caratteristico $p_\varphi(x)$ di φ . Uno scalare $\lambda \in C$ è un autovalore di A (o di φ) se e solo se è zero del polinomio $p_A(x)$. Si dice che A (o φ) ha tutti i suoi autovalori in C se il polinomio caratteristico $p_A(x)$ si fattorizza in fattori lineari in $C[x]$.

Teorema di Hamilton-Cayley: $p_A(A) = 0$, ovvero $p_\varphi(\varphi) = 0$.

Il polinomio minimo $m_A(x)$ di A (o $m_\varphi(x)$ di φ) è il generatore monico dell'ideale di $C[x]$ formato dai polinomi che annullano A (o φ). Il polinomio minimo divide il polinomio caratteristico (seconda forma del teorema di Hamilton-Cayley).

Simmetrie e Proiezioni. Le matrici di polinomio minimo $x^2 - 1$ si dicono simmetriche di asse l'autospazio di 1 e di direzione l'autospazio di -1; le matrici di polinomio minimo $x^2 - x$ si dicono proiezioni sull'autospazio di 1 e di direzione l'autospazio di 0. Data una decomposizione $V = V' \oplus V''$, esistono uniche la simmetria di asse V' e direzione V'' , e la proiezione su V' e direzione V'' , definite dall'essere diagonalizzabili e dall'avere V' come auospazio di 1 e V'' come autospazio di -1 oppure 0 rispettivamente.

Teorema di decomposizione: se un polinomio $f(x)$ annulla φ e $f(x) = \prod_i f_i(x)$ è una fattorizzazione con i fattori $f_i(x)$ a due a due coprimi, allora $V = \bigoplus_i V_i$ ove $V_i = \ker(f_i(\varphi))$ e $\dim_C V_i = \deg_x f_i(x)$.

Forme canoniche triangolari. Una matrice A è simile (in C) a una matrice in forma triangolare se e solo se ha tutti i suoi autovalori in C .

Dato un autovalore $\lambda \in C$, definiamo la molteplicità $m(\lambda) :=$ molteplicità di λ come zero di $p_A(x)$ e la nullità $n(\lambda) := \dim_C \ker(\varphi - \lambda \text{id}) = n - \text{rk}(A - \lambda \mathbb{I})$. Si ha che $n(\lambda) \leq m(\lambda)$.

Forme diagonali. Una matrice A è simile (in C) a una matrice in forma diagonale se e solo se ha tutti i suoi autovalori in C e ogni autovalore ha molteplicità e nullità uguali (primo criterio di diagonalizzabilità). Secondo criterio: una matrice è diagonalizzabile se e solo se il polinomio minimo si fattorizza in fattori lineari distinti (ha tutti i suoi zeri e questi sono tutti semplici).

Due matrici A e B sono simultaneamente diagonalizzabili (i.e. esiste $P \in GL(n,C)$ tale che $P^{-1}AP$ e $P^{-1}BP$ sono entrambe diagonali) se e solo se sono (separatamente) diagonalizzabili e commutano tra loro (i.e. $AB = BA$, nel qual caso ciascuna delle due matrici è stabile sugli autospazi dell'altra).

Teoria di Jordan. Sia $p_\varphi(x) = \prod_i (x - \lambda_i)^{r_i}$ ($r_i = m(\lambda_i)$); poniamo $V_i := \ker((\varphi - \lambda_i \text{id})^{r_i})$, allora $V = \bigoplus_i V_i$, $\dim_C(V_i) = r_i$. Risulta $m_\varphi(x) = \prod_i (x - \lambda_i)^{s_i}$ ove s_i è il minimo intero tale che $\dim_C(\ker((\varphi - \lambda_i \text{id})^{s_i})) = r_i$.

L'applicazione φ è nilpotente se esiste $N \in \mathbb{N}$ tale che $\varphi^N = 0$; l'indice di nilpotenza è il minimo intero per cui ciò succede, si indica con $\text{nilp}(A)$. L'applicazione φ è nilpotente se e solo se una (e allora ogni) sua matrice associata è nilpotente (e gli ordini di nilpotenza sono uguali).

La matrice nilpotente standard di ordine m è la matrice $N_m := \sum_i e_{i,i+1} \in M_m(C)$. Una matrice A è nilpotente se e solo se è simile a una matrice a blocchi diagonali formati da matrici nilpotenti standard.

Il tipo di nilpotenza di una matrice nilpotente $A \in M_n(C)$ è la n -pla di naturali (i_1, \dots, i_n) ove i_l è il numero di blocchi nilpotenti standard di ordine l della forma ridotta di A . Due matrici nilpotenti sono simili se e solo se hanno lo stesso tipo di nilpotenza.

Esempi. Per $n=1$ l'unica matrice nilpotente è la matrice nulla.

Per $n=2$ le matrici nilpotenti sono di due tipi: la matrice nulla di tipo $(2,0)$ e la nilpotente standard $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ di tipo $(0,1)$.

Per $n=3$ abbiamo tre tipi di matrici nilpotenti:
la matrice nulla di tipo $(3,0,0)$;
la matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ di tipo $(1,1,0)$ (sse $\text{nilp}(A)=2$ e $\text{rk}(A)=1$);
la matrice $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ di tipo $(0,0,1)$ (sse $\text{nilp}(A)=3$ e $\text{rk}(A)=2$);

Per $n=4$ abbiamo cinque tipi di matrici nilpotenti:
la matrice nulla di tipo $(4,0,0,0)$;
 $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(2,1,0,0)$ (sse $\text{nilp}(A)=2$ e $\text{rk}(A)=1$);
 $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(1,0,1,0)$ (sse $\text{nilp}(A)=3$ e $\text{rk}(A)=2$);
 $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(0,2,0,0)$ (sse $\text{nilp}(A)=2$ e $\text{rk}(A)=2$);
 $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(0,0,0,1)$ (sse $\text{nilp}(A)=4$ e $\text{rk}(A)=3$).

Si dice matrice di Jordan di ordine m e autovalore λ la matrice $J_m(\lambda) := \lambda \mathbb{I} + N_m$.

Teorema di Jordan: una matrice ha tutti i suoi autovalori in C se e solo se è simile (in C) a una matrice a blocchi diagonali formati da matrici di Jordan.

La molteplicità di un autovalore λ_i di A come radice del polinomio minimo è la dimensione del più grande blocco di Jordan relativo a quell'autovalore.

Decomposizione astratta di Jordan. Sia A un endomorfismo di uno spazio vettoriale V di dimensione finita (rispettivamente: sia A una matrice quadrata) con tutti i suoi autovalori nel corpo di base C . Allora esistono unici due endomorfismi (risp. matrici) A_s, A_n tali che

- (i) A_s è semisemplice (=diagonalizzabile) e A_n è nilpotente;
- (ii) $A_s A_n = A_n A_s$ e $A = A_s + A_n$;
- (iii) esistono polinomi $p(X), q(X) \in C[X]$ privi di termine noto e tali che $A_s = p(A)$, $A_n = q(A)$; in particolare A_s ed A_n commutano con ogni endomorfismo (risp. ogni matrice) che commuti con A ;
- (iv) sottospazi stabili per A sono stabili sia per A_s che per A_n ;

(v) se $AB=BA$ con A e B soddisfacenti all'ipotesi detta, allora $(A+B)_s=A_s+B_s$ e $(A+B)_n=A_n+B_n$.

Decomposizione astratta moltiplicativa di Jordan. Sia A un automorfismo di uno spazio vettoriale V di dimensione finita (rispettivamente: sia A una matrice quadrata invertibile) con tutti i suoi autovalori nel corpo di base C . Allora i suoi autovalori sono tutti non nulli, ed esistono unici due endomorfismi (risp. matrici) A_s , A_u tali che

- (i) A_s è semisemplice (=diagonalizzabile) e A_n è unipotente (significa che ha 1 come unico autovalore);
- (ii) $A_s A_u = A_u A_s = A$;
- (iii) sottospazi stabili per A sono stabili sia per A_s che per A_n ;
- (iv) se $AB=BA$ con A e B soddisfacenti all'ipotesi detta, allora $(AB)_s=A_s B_s$ e $(AB)_u=A_u B_u$.

Dualità. Sia V uno spazio vettoriale su C di dimensione finita n . Definiamo il suo duale come $V^*:=\text{Hom}_C(V,C)$ (applicazioni lineari di V in C), che ha una struttura naturale di C -spazio vettoriale data da $(v^*+w^*)(v):=v^*(v)+w^*(v)$ e $(cv^*)(v):=cv^*(v)$ per $v^*, w^* \in V^*$.

Data una base $e=(e_1, \dots, e_n)$ di V , gli elementi e_i^* di V^* definiti da $e_i^*(e_j):=\delta_{i,j}$ formano una base di V^* ; $e^*=(e_1^*, \dots, e_n^*)$ si dice la base duale di e . In particolare $\dim_C V^*=\dim_C V$.

Esiste una applicazione canonica:

$$V \times V^* \longrightarrow C: (v, v^*) \mapsto v \circ v^* := v^*(v)$$

bilineare: $v \circ (v^*+w^*) = v \circ v^* + v \circ w^*$, $(v+w) \circ v^* = v \circ v^* + w \circ v^*$ e $(\lambda v) \circ v^* = \lambda(v \circ v^*) = v \circ (\lambda v^*)$;

non degenero: se $v \circ v^* = 0$ per ogni $v \in V$ (risp. $v^* \in V^*$) allora $v=0$ (risp. $v^*=0$).

Se $\varphi: V \rightarrow W$ è una applicazione lineare, allora definiamo $\varphi^*: W^* \rightarrow V^*$ tramite la regola $\varphi^*(w^*)(v):=w^*(\varphi(v))$ (i.e. $v \circ (\varphi^* w^*) = (\varphi v) \circ w^*$ ($\forall v \in V, \forall w^* \in W^*$)).

La matrice di φ^* nelle basi duali delle basi e di V e g di W è data dalla trasposta della matrice di φ in quelle basi: $\alpha_{g^*, e^*}(\varphi^*) = \alpha_{e, g}(\varphi)^t$. In particolare $\text{rk}(\varphi^*) = \text{rk}\varphi$ ($= \dim_C \text{im} \varphi$).

Abbiamo che $\text{id}_V^* = \text{id}_{V^*}$, $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Il morfismo canonico: $V \rightarrow V^{**}$, $v \mapsto \text{ev}(v)$ ove $\text{ev}(v)(v^*):=v^*(v)=v \circ v^*$ è un isomorfismo di spazi vettoriali (Notare che non c'è un isomorfismo canonico tra V e V^*). Sotto questa identificazione, per un morfismo φ , risulta $\varphi^{**} = \varphi$.

Nozione di ortogonalità: per S sottinsieme di V definiamo un sottospazio di V^* : $S^\perp := \{v^* \in V^* \mid s \circ v^* = 0 \ (\forall s \in S)\}$.

Proprietà dell'ortogonalità: se $S \subseteq T$ allora $T^\perp \subseteq S^\perp$; $S^{\perp\perp} = \langle S \rangle$; $W^{\perp\perp} = W$; $S^{\perp\perp\perp} = S^\perp$; $(W \cap W')^\perp = W^\perp + W'^\perp$ e $(W + W')^\perp = W^\perp \cap W'^\perp$ (ove W e W' sono sottospazi di V); in particolare il passaggio all'ortogonale induce un antiisomorfismo involutivo tra i reticolati di sottospazi di V e V^* ; inoltre $\dim_C(W^\perp) = n - \dim_C W$.

Se $\varphi: V \rightarrow W$, allora $\text{im}(\varphi^*) = \ker(\varphi)^\perp$ e $\ker(\varphi^*) = \text{im}(\varphi)^\perp$.

Dato un sottospazio W di V , la dualità canonica $V \times V^* \longrightarrow C$ induce una mappa con analoghe proprietà $(V/W) \times W^\perp \longrightarrow C$, da cui si deduce che $(V/W)^* \cong W^\perp$ e $(V^*/W^\perp)^* \cong W$. Inoltre $W^* \cong V^*/W^\perp$.

Spazi Vettoriali Euclidei.

Prodotto Scalare. Sia $V_n(\mathbb{R})$ lo spazio vettoriale standard su \mathbb{R} di dimensione n . Definiamo il prodotto scalare di due vettori v e w come $v \cdot w := v^t w = \sum_i v_i w_i$, ove si sono usate le coordinate nella base canonica.

Proprietà del prodotto scalare $V_n(\mathbb{R}) \times V_n(\mathbb{R}) \longrightarrow \mathbb{R}$:

commutatività: $v \cdot w = w \cdot v$ ($\forall v, w \in V$);

bilinearità: $v \cdot (\alpha_1 w_1 + \alpha_2 w_2) = \alpha_1(v \cdot w_1) + \alpha_2(v \cdot w_2)$ e $(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = \alpha_1(v_1 \cdot w) + \alpha_2(v_2 \cdot w)$ ($\forall v_i, w_i \in V, \forall \alpha_i \in C$);

positività: $v \cdot v \geq 0$; $v \cdot v = 0$ sse $v = 0$ ($\forall v \in V$);

$(v \cdot w)^2 \leq (v \cdot v)(w \cdot w)$ ($\forall v, w \in V$) (diseguaglianza di Cauchy-Schwarz; si dimostra a partire da $(v + \lambda w) \cdot (v + \lambda w) \geq 0$ per ogni $\lambda \in \mathbb{R}$).

Nozione di lunghezza dei vettori: $\|v\| := \sqrt{v \cdot v}$.

Valgono le seguenti regole: $\|v\|=0$ sse $v=0$; $\|\alpha v\|=|\alpha| \|v\|$;

$\|v+w\| \leq \|v\| + \|w\|$ (diseguaglianza triangolare);

$$\|v+w\|^2 = \|v\|^2 + 2(v \cdot w) + \|w\|^2;$$

$$\|v+w\|^2 + \|v-w\|^2 = 2(\|v\|^2 + \|w\|^2).$$

Nozione di misura dell'angolo tra due vettori:

$$\cos \theta(v, w) := \frac{v \cdot w}{\|v\| \|w\|}$$
 (ha senso per la diseguaglianza CS).

Nozione di ortogonalità tra due vettori: $v \perp w$ significa per definizione $v \cdot w = 0$.

Teorema di Pitagora: $v \perp w$ sse $\|v+w\|^2 = \|v\|^2 + \|w\|^2$.

Proiezione ortogonale di un vettore v nella direzione di w : $p_w(v) = \frac{v \cdot w}{\|w\|^2} w = \frac{v \cdot w}{w \cdot w} w$. Risulta che $p_w(v) \perp (v - p_w(v))$.

Si ha che $v+w = p_v+v + p_w+w$.

Teoremi di Euclide: $v \perp w$ sse $\|v\|^2 = \|v+w\| \|p_{v+w}(v)\|$;

$$v \perp w$$
 sse $\|v-p_{v+w}(v)\|^2 = \|p_{v+w}(v)\| \|p_{v+w}(w)\|$.

Per S sottinsieme di V definiamo $S^\perp := \{v \in V \mid v \perp s \ (\forall s \in S)\}$, che risulta un sottospazio vettoriale. Si ha: $\{0\}^\perp = V$, $V^\perp = 0$, $\langle S \rangle = (S^\perp)^\perp$. Dunque per W sottospazio: $(W^\perp)^\perp = W$. Se $S \subseteq T$ allora $T^\perp \subseteq S^\perp$; $S^{\perp\perp\perp} = S^\perp$.

Se W e W' sono sottospazi vettoriali di V : $(W+W')^\perp = W^\perp \cap W'^\perp$ e $(W \cap W')^\perp = W^\perp + W'^\perp$.

Teorema di decomposizione: se $W \leq V$ allora V è somma diretta di W e W^\perp e si scrive $V = W \boxplus W^\perp$. In particolare una base di W^\perp dà un sistema di equazioni cartesiane di W . Interpretazione euclidea delle equazioni cartesiane di un sottospazio: i coefficienti delle equazioni formano dei vettori ortogonali al sottospazio stesso.

Basi ortogonali e ortonormali. Una base di $V_n(\mathbb{R})$ si dice ortogonale se essa è formata di vettori a due a due ortogonali; si dice ortonormale se inoltre i vettori hanno tutti norma 1. Se (v_1, \dots, v_n) è una base ortonormale di $V_n(\mathbb{R})$, allora le coordinate di un vettore $v \in V_n(\mathbb{R})$ in quella base sono date da $(v \cdot v_1, \dots, v \cdot v_n)^t$; in altri termini, per ogni vettore v risulta $v = \sum_{i=1}^n (v \cdot v_i) v_i$.

Procedimento di ortogonalizzazione (Gram-Schmidt). Data una base qualsiasi v_1, \dots, v_n di $V_n(\mathbb{R})$ è sempre possibile ricavarne una base ortogonale u_1, \dots, u_n nel modo seguente: $u_1 = v_1$ e ad ogni passo si aggiunge il vettore u_i ottenuto togliendo a v_i tutte le sue proiezioni ortogonali sui precedenti vettori u_1, \dots, u_{i-1} . Per ottenere una base ortonormale, basta poi dividere ogni vettore u_i per la sua norma. Il procedimento funziona (cioè fornisce una base ortogonale) anche a partire da un qualsiasi insieme di generatori di $V_n(\mathbb{R})$, eliminando i vettori nulli generati dal procedimento stesso.

Soluzioni ai minimi quadrati per sistemi incompatibili. Dato un sistema lineare incompatibile $AX=b$ i vettori x tali che la norma di $Ax-b$ sia minima possibile (quelli dunque che meglio approssimano una soluzione nel senso della distanza euclidea) sono quelli per cui $Ax-b$ è ortogonale allo spazio generato dalle colonne di A , dunque se e solo se $A^t(Ax-b)=0$, e dunque se e solo se x risolve il sistema lineare $A^t AX = A^t b$ (la matrice $A^t A$ è simmetrica, e il suo rango è uguale al rango di A). Equivalentemente, se decomponiamo $b=a+a'$ con a appartenente al sottospazio generato dalle colonne di A , e a' ortogonale allo

stesso sottospazio, si tratta delle soluzioni del sistema lineare $AX=a$.

Gruppo Ortogonale e Ortogonale Speciale. Gli automorfismi di V che rispettano la struttura euclidea, i.e. $\varphi(v) \cdot \varphi(w) = v \cdot w$ per ogni $v, w \in V$, si dicono trasformazioni ortogonali. Ogni matrice A associata usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) risulta ortogonale, i.e. tale che $A^t A = \mathbb{I}$, ovvero $A^{-1} = A^t$. Le matrici ortogonali formano un sottogruppo di $GL(n, \mathbb{C})$ che si indica con $O(n, \mathbb{C})$ o con $O_n(\mathbb{C})$. Esso è formato da tutte e sole le matrici le cui colonne formano una base ortonormale di V . Se $A \in O(n, \mathbb{C})$, allora $\det A = \pm 1$.

Il gruppo $SO(n, \mathbb{C})$ o $SO_n(\mathbb{C})$ è definito dalla intersezione $O_n(\mathbb{C}) \cap SL_n(\mathbb{C})$ e si chiama Gruppo Ortogonale Speciale. Esso è un sottogruppo normale di $O_n(\mathbb{C})$ e il quoziente è ciclico d'ordine 2, cioè $\{\pm 1\}$ (orientamenti dello spazio). Per ogni matrice $R \in O(n, \mathbb{C}) \setminus SO_n(\mathbb{C})$, si ha che $O(n, \mathbb{C}) \setminus SO_n(\mathbb{C}) = R \cdot SO_n(\mathbb{C})$

Simmetrie e Proiezioni ortogonali. Per ogni vettore non nullo $v \in V_n(\mathbb{R})$; la matrice della simmetria di direzione v e asse l'iperpiano ortogonale v^\perp è $\mathbb{I} - 2 \frac{vv^t}{v^t v}$. Se supponiamo $v \cdot v = v^t v = 1$, allora la matrice di s è data da $\mathbb{I}_n - 2vv^t$. Si noti che vv^t è la matrice della proiezione su v con direzione v^\perp (quindi matrice di rango 1), mentre $\mathbb{I}_n - vv^t$ è matrice della proiezione su v^\perp con direzione v (quindi di rango $n-1$).

Se il sottospazio W è generato dalle colonne della matrice A (matrice $n \times m$ di rango m) abbiamo:

se $A^t A = \mathbb{I}_m$ allora AA^t è la matrice della proiezione ortogonale su W , $\mathbb{I}_n - AA^t$ è la matrice della proiezione ortogonale su W^\perp , e $\mathbb{I}_n - 2AA^t$ è la matrice della simmetria ortogonale di asse W ; in generale, la matrice della proiezione ortogonale su W è data da $A(A^t A)^{-1}A^t$, e dunque la simmetria ortogonale di asse W ha matrice data da $\mathbb{I}_n - 2A(A^t A)^{-1}A^t$.

Gruppi Ortogonali del Piano. Il gruppo $SO_2(\mathbb{R})$ (rotazioni del piano) è isomorfo al gruppo additivo \mathbb{R}/\mathbb{Z} (mandando $x \in \mathbb{R}/\mathbb{Z}$ nella matrice trigonometrica $\begin{pmatrix} \cos 2\pi x & -\sin 2\pi x \\ \sin 2\pi x & \cos 2\pi x \end{pmatrix}$) e al gruppo moltiplicativo \mathbb{S}^1 dei numeri complessi di modulo unitario (punti della circonferenza di centro origine e raggio 1 del piano, mandando $a+ib \in \mathbb{S}^1$ nella matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$). Unici elementi di $SO_2(\mathbb{R})$ diagonalizzabile su \mathbb{R} sono $\pm \mathbb{I}$. Ogni elemento di $O_2(\mathbb{R})$ si può scrivere come prodotto di al più due elementi di $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$ (due riflessioni formano una rotazione).

Gruppi Ortogonali dello Spazio. Tutte le matrici del gruppo $SO_3(\mathbb{R})$ (rotazioni dello spazio) ammettono l'autovalore 1 e rappresentano rotazioni dello spazio attorno all'asse definito da un autovettore associato all'autovalore 1. Ogni tale trasformazione è rappresentata da un quaternione unitario (e dal suo opposto).

Angoli di Eulero. Fissate due basi ortonormali e_1, e_2, e_3 ed E_1, E_2, E_3 esiste un unico elemento φ di $SO_3(\mathbb{R})$ tale che $\varphi e_i = E_i$ ($i=1, 2, 3$) e si può scrivere come composizione di al più tre rotazioni di angoli opportuni intorno a rette. Possiamo considerare i due piani $\langle e_1, e_2 \rangle$ e $\langle E_1, E_2 \rangle$. Se essi coincidono, allora φ è una rotazione attorno alla retta $\langle e_3 \rangle = \langle E_3 \rangle$, altrimenti la loro intersezione determina una retta, detta retta dei nodi, di versore diciamo n . Si considerino allora le seguenti rotazioni: rotazione di asse e_3 ed angolo $\psi = \vartheta(e_1, n)$ (precessione), rotazione di asse n ed angolo $\nu = \vartheta(e_3, E_3)$ (nutazione), rotazione di asse E_3 ed angolo $\rho = \vartheta(n, E_1)$ (rotazione propria). La composizione nell'ordine delle tre rotazioni dà φ . Si può quindi scrivere la matrice della trasformazione φ in termini dei tre angoli di precessione ψ , di nutazione ν e di rotazione propria ρ tramite la composizione:

$$\begin{pmatrix} \cos \rho & -\sin \rho & 0 \\ \sin \rho & \cos \rho & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \nu & -\sin \nu \\ 0 & \sin \nu & \cos \nu \end{pmatrix} \begin{pmatrix} \cos \psi & -\sin \psi & 0 \\ \sin \psi & \cos \psi & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} \cos \rho \cos \psi & -\sin \rho \cos \psi & \sin \rho \sin \psi \\ \sin \rho \cos \psi & -\cos \rho \cos \psi & \sin \rho \sin \psi \\ \sin \nu \cos \psi & \sin \nu \sin \psi & \cos \nu \end{pmatrix}.$$

Prodotto Hermitiano o Prodotto scalare complesso. Sia $V_n(\mathbb{C})$ lo spazio vettoriale standard su \mathbb{C} di dimensione n . Definiamo il prodotto scalare di due vettori $v=(z_j)^t$ e $w=(z'_j)^t$ come $v \cdot w := v^t \bar{w} = \sum_j z_j \bar{z}'_j$, ove si sono usate le coordinate nella base canonica.

Il prodotto scalare dà una funzione $V_n(\mathbb{C}) \times V_n(\mathbb{C}) \rightarrow \mathbb{C}$ che gode delle seguenti proprietà:

antisimmetria: $v \cdot w = \overline{w \cdot v}$ (per ogni $v, w \in V_n(\mathbb{C})$);

linearità sinistra: $(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = \alpha_1 (v_1 \cdot w) + \alpha_2 (v_2 \cdot w)$ e antilinearità destra: $v \cdot (\alpha_1 w_1 + \alpha_2 w_2) = \overline{\alpha_1} (v \cdot w_1) + \overline{\alpha_2} (v \cdot w_2)$ (per ogni $v, v_1, v_2, w, w_1, w_2 \in V_n(\mathbb{C})$, ed ogni $\alpha_1, \alpha_2 \in \mathbb{C}$);

positività: $v \cdot v \geq 0$ (per ogni $v \in V_n(\mathbb{C})$); $v \cdot v = 0$ se e solo se $v = 0$.

Lo spazio vettoriale $V_n(\mathbb{C})$ dotato del prodotto scalare si dice lo spazio euclideo (complesso) standard di dimensione n o spazio Hermitiano standard di dimensione n .

La norma o lunghezza di un vettore $v \in V_n(\mathbb{C})$ è definita come $\|v\| := \sqrt{v \cdot v}$ (si usa la positività). Un vettore di norma 1 si dice un versore.

disuguaglianza di Cauchy-Schwarz. Per ogni $v, w \in V_n(\mathbb{C})$ vale che $|v \cdot w|^2 \leq (v \cdot v)(w \cdot w)$ (si noti che $v \cdot w \in \mathbb{C}$, e usiamo la norma in senso complesso) e dunque $|v \cdot w| \leq \|v\| \|w\|$. Inoltre vale l'uguaglianza se e solo se v e w sono linearmente dipendenti. Si hanno le usuali proprietà $\|v\|=0$ se e solo se $v=0$; $\|\alpha v\|=|\alpha| \|v\|$; $\|v+w\| \leq \|v\| + \|w\|$ (disuguaglianza triangolare); $\|v \pm w\|^2 = \|v\|^2 \pm 2\Re(v \cdot w) + \|w\|^2$ (versione complessa del teorema di Carnot); $\|v+w\|^2 + \|v-w\|^2 = 2(\|v\|^2 + \|w\|^2)$.

Due vettori $v, w \in V_n(\mathbb{C})$ si dicono ortogonali e si scrive $v \perp w$ se vale $v \cdot w = 0$ (il loro prodotto scalare è zero).

Pitagora complesso. Abbiamo che $\Re(v \cdot w) = 0$ ($v \cdot w$ è puramente immaginario) se e solo se $\|v+w\|^2 = \|v\|^2 + \|w\|^2$.

Le nozioni di proiezione ortogonale, di basi ortogonali e ortonormali, di ortogonali di sottospazi sono simili a quelle reali, con alcune ovvie differenze:

Equazioni di sottospazi: l'interpretazione hermitiana (o euclidea complessa) delle equazioni di sottospazi diventa ora la seguente: i coefficienti di ogni equazione formano un vettore il cui coniugato è ortogonale al sottospazio stesso.

Relazioni con il caso reale. L'applicazione biiettiva $r: V_n(\mathbb{C}) \rightarrow V_{2n}(\mathbb{R})$ che manda un vettore complesso $v=(z_i)^t = (x_i+iy_i)^t$ nel vettore reale $r(v)=(x_1, \dots, x_n, y_1, \dots, y_n)^t$ possiede la proprietà che $\|r(v)\| = \|v\|$ per ogni $v \in V_n(\mathbb{C})$ (norme euclidean nel primo membro, ed hermitiana nel secondo), e più in generale $r(v) \cdot r(w) = \Re(v \cdot w)$ (prodotto scalare euclideo nel primo membro, ed hermitiano nel secondo) per $v, w \in V_n(\mathbb{C})$. In effetti possiamo esplicitare: $v \cdot v' = \sum_{j=1}^n (x_j x'_j + y_j y'_j) + i \sum_{j=1}^n (x_j y'_j - y_j x'_j)$ mentre $r(v) \cdot r(v') = \sum_{j=1}^n (x_j x'_j + y_j y'_j)$.

Gruppi Unitario e Speciale Unitario. Un automorfismo φ di $V_n(\mathbb{C})$ in sè φ rispetta la struttura hermitiana, i.e. $\varphi(v) \cdot \varphi(w) = v \cdot w$ per ogni $v, w \in V_n(\mathbb{C})$, se e solo se φ rispetta la norma dei vettori, i.e. $\|\varphi(v)\| = \|v\|$ per ogni $v \in V_n(\mathbb{C})$.

Tali automorfismi si dicono trasformazioni hermitiane o isometrie complesse di $V_n(\mathbb{C})$.

Se φ è una trasformazione hermitiana, ogni matrice A associata a φ usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) risulta una matrice hermitiana, i.e. tale che $A^t \bar{A} = \mathbb{I}$, ovvero $A^{-1} = \bar{A}^t$. Le matrici hermitiane formano un sottogruppo (non normale, se $n > 1$) di $GL(n, \mathbb{C})$ che si indica con $U(n, \mathbb{C})$ o $Un(\mathbb{C})$ e si dice il Gruppo Hermitiano. Se $A \in U(n, \mathbb{C})$, allora $|\det A| = 1$ ($\det A$ è numero complesso di modulo 1).

Gruppo Unitario Speciale. Il sottinsieme di $U_n(\mathbb{C})$ formato dalle matrici di determinante 1 si indica con $SU(n, \mathbb{C})$ o $SU_n(\mathbb{C})$ e si dice il gruppo unitario speciale. Si tratta di un sottogruppo normale di $U_n(\mathbb{C})$, e il quoziente $U_n(\mathbb{C})/SU_n(\mathbb{C})$ è isomorfo a \mathbb{S}^1 (gruppo moltiplicativo dei complessi di modulo 1).

Si osservi che l'intersezione di $U_n(\mathbb{C})$ e $SU_n(\mathbb{C})$ con $GL_n(\mathbb{R})$ danno rispettivamente $O_n(\mathbb{R})$ e $SO_n(\mathbb{R})$.

Descrizione esplicita di $U_2(\mathbb{C})$. Le matrici in $U_2(\mathbb{C})$ sono le matrici complesse del tipo $\begin{pmatrix} \alpha & \beta \\ -\rho\bar{\beta} & \rho\bar{\alpha} \end{pmatrix}$ con $|\alpha|^2 + |\beta|^2 = 1$, $|\rho| = 1$.

Struttura di $SU_2(\mathbb{C})$. Le matrici in $SU_2(\mathbb{C})$ sono tutte e sole le matrici complesse della forma $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ con $|\alpha|^2 + |\beta|^2 = 1$ e in effetti $SU_2(\mathbb{C})$ è isomorfo alla sfera tridimensionale in \mathbb{R}^4 con la struttura di gruppo dei quaternioni unitari (come $SO_2(\mathbb{R})$ è isomorfo alla sfera unidimensionale \mathbb{S}^1 in \mathbb{R}^2 con la struttura di gruppo dei complessi unitari). Usando le componenti reali: se $\alpha = x_0 + ix_1$ e $\beta = x_2 + ix_3$ otteniamo

$$\begin{aligned} \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} &= x_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_1 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= x_0 \mathbb{I}_2 + x_1 I + x_2 J + x_3 K. \end{aligned}$$

Lo spazio vettoriale reale di dimensione 4 generato da \mathbb{I}_2, I, J, K in $GL_2(\mathbb{C})$ ha (considerando il prodotto tra matrici) struttura di corpo isomorfo a quello dei quaternioni: $I^2 = J^2 = K^2 = -\mathbb{I}_2$, $IJ = JK = -KI$, $JK = I = -KJ$, $KI = J = -IK$; il quadrato della norma dei quaternioni corrisponde al determinante delle matrici, quindi i quaternioni unitari corrispondono alle matrici unitarie speciali.

Un elemento di $SU_2(\mathbb{C})$ determina quindi un quaternione e di conseguenza un elemento di $SO_3(\mathbb{R})$ (rotazione attorno ad un fissato asse): $A \in SU_2(\mathbb{C})$ determina una isometria φ_A dello spazio vettoriale euclideo reale $(I, J, K)_{\mathbb{R}}$, di cui I, J, K formano una base ortonormale (la norma essendo data dal determinante delle matrici), tramite la formula $\varphi_A(X) = AXA^t$.

Questo determina un omomorfismo di gruppi $SU_2(\mathbb{C}) \rightarrow SO_3(\mathbb{R}) = \text{Aut}(\langle I, J, K \rangle_{\mathbb{R}})$; si tratta di un morfismo suriettivo con nucleo $\{\pm \mathbb{I}_2\}$. Quindi dare un elemento di $SU_2(\mathbb{C})$ consiste nel dare un elemento di $SO_3(\mathbb{R})$ con un segno ± 1 ; per questo $SU_2(\mathbb{C})$ viene spesso chiamato il gruppo degli spin.

Cross Product. Sia $V_n(C)$ lo spazio vettoriale standard su C di dimensione n . Definiamo una applicazione $\text{cross}: V^{n-1} \rightarrow V$ tramite la formula:

$$\text{cross}(v_1, \dots, v_{n-1}) := \det \begin{pmatrix} e \\ v_1^t \\ \vdots \\ v_{n-1}^t \end{pmatrix} = \begin{vmatrix} e_1 & \cdots & e_n \\ v_{1,1} & \cdots & v_{1,n} \\ \vdots & \ddots & \vdots \\ v_{n-1,1} & \cdots & v_{n-1,n} \end{vmatrix}$$

In particolare: per $n=1$ si ha $\text{cross}(\emptyset) = e = 1$;

per $n=2$ si ha $\text{cross}(v) = \begin{pmatrix} y \\ -x \end{pmatrix}$ se $v = \begin{pmatrix} x \\ y \end{pmatrix}$.

per $n=3$ si ha $\text{cross}(v, w) = \begin{pmatrix} yz' - y'z \\ x'z - xz' \\ xy' - x'y \end{pmatrix}$ se $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ e $w = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$.

Proprietà del cross product:

$\text{cross}(v_1, \dots, v_{n-1}) = 0$ se e solo se v_1, \dots, v_{n-1} sono ld;

$\text{cross}(v_{\sigma(1)}, \dots, v_{\sigma(n-1)}) = \text{sgn}(\sigma) \text{cross}(v_1, \dots, v_{n-1})$ ($\forall \sigma \in \mathcal{P}_{n-1}$);

$v_i \cdot \text{cross}(v_1, \dots, v_{n-1}) = 0$ (cioè, se si tratta di spazi euclidei, $\text{cross}(v_1, \dots, v_{n-1})$ è ortogonale a v_i nel caso reale, al coniugato nel caso complesso hermitiano) per ogni i ;

multilinearità: $\text{cross}(v_1, \dots, \sum_j \alpha_j w_j, \dots, v_{n-1}) = \sum_j \alpha_j \text{cross}(v_1, \dots, w_j, \dots, v_{n-1})$;

identità di Lagrange:

$$\left\| \text{cross}(v_1, \dots, v_{n-1}) \right\|^2 = \begin{vmatrix} \|v_1\|^2 & v_1 \cdot v_2 & \cdots & v_1 \cdot v_{n-1} \\ v_2 \cdot v_1 & \|v_2\|^2 & \cdots & v_2 \cdot v_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n-1} \cdot v_1 & v_{n-1} \cdot v_2 & \cdots & \|v_{n-1}\|^2 \end{vmatrix}.$$

Si tratta di un caso speciale della seguente formula:

$$\text{cross}(v_1, \dots, v_{n-1}) \cdot \text{cross}(u_1, \dots, u_{n-1}) = \det(v_i \cdot u_j).$$

Se v_1, \dots, v_{n-1} sono li, allora $v_1, \dots, v_{n-1}, \text{cross}(v_1, \dots, v_{n-1})$ formano una base di V . Risulta:

$$\text{cross}(u_2, \dots, u_{n-1}, \text{cross}(v_1, \dots, v_{n-1})) = \sum_{i=1}^{n-1} (-1)^{i+1} |u_a \cdot v_b|_{\substack{a \neq 1 \\ b \neq i}} v_i.$$

Nel caso $n=2$ l'identità di Lagrange si riduce a $\|\text{cross}(v)\| = \|v\|$

Nel caso $n=3$, $\text{cross}(v, w) = v \wedge w$, l'identità di Lagrange è

$$\|v \wedge w\|^2 = \|v\|^2 \|w\|^2 - (v \cdot w)^2 \quad \text{e si generalizza in} \\ \sum_{i < j} (x_i y_j - x_j y_i)^2 = (\sum_{i=1}^n x_i^2) (\sum_{i=1}^n y_i^2) - (\sum_{i=1}^n x_i y_i)^2. \\ \text{Inoltre risulta } u \wedge (v \wedge w) = (u \cdot w)v - (u \cdot v)w.$$

Da un punto di vista geometrico, il cross product di $n-1$ vettori linearmente indipendenti si caratterizza come: il vettore di direzione ortogonale ai vettori dati, di verso tale che l'orientazione di $v_1, \dots, v_{n-1}, \text{cross}(v_1, \dots, v_{n-1})$ concordi con quella della base scelta, di lunghezza il volume $(n-1)$ -dimensionale del "parallelepipedo" formato dai vettori v_1, \dots, v_{n-1} .

Prodotto misto. $|w v_1 \dots v_{n-1}| := w \cdot \text{cross}(v_1, \dots, v_{n-1})$ si dice il prodotto misto dei vettori w e v_1, \dots, v_{n-1} ; è un elemento di C che si annulla se e solo se gli n vettori coinvolti sono ld. Si ha $|v_{\sigma(1)} \dots v_{\sigma(n)}| = \text{sgn}(\sigma) |v_1 \dots v_n|$ per ogni permutazione σ . Il modulo del prodotto misto si interpreta come volume n -dimensionale del poliparallelepipedo generato dagli n vettori.

Endomorfismi simmetrici ed Hermitiani. Sia V uno spazio vettoriale euclideo reale (risp. complesso hermitiano). Un endomorfismo f di V si dice simmetrico (risp. hermitiano) se $f(v) \cdot w = v \cdot f(w)$ per ogni $v, w \in V$; ciò succede sse $A^t = A$ (risp. $A^t = \bar{A}$) se A è la matrice di f in una (e allora per ogni) base ortonormale.

Ogni endomorfismo simmetrico (risp. hermitiano) ammette una base di autovettori ortogonali; in particolare una matrice reale A è simmetrica se e solo se è ortogonalmente diagonalizzabile (cioè esiste P con $P^t P = \mathbb{I}$ tale che $P^t A P$ sia diagonale); e una matrice complessa A è hermitiana ($A^t = \bar{A}$) se e solo se è unitariamente diagonalizzabile (cioè esiste U con $\bar{U}^t U = \mathbb{I}$ tale che $\bar{U}^t A U$ sia diagonale).

Una matrice reale è simultaneamente ortogonale e ortogonalmente diagonalizzabile se e solo se è la matrice di una simmetria ortogonale (cioè con asse e direzione ortogonali tra loro).

Sistemi di Equazioni Lineari.

Notazioni. Un sistema lineare di m equazioni ed n incognite

$$\begin{cases} a_{1,1} X_1 + \dots + a_{1,n} X_n = b_1 \\ \vdots \\ a_{m,1} X_1 + \dots + a_{m,n} X_n = b_m \end{cases}$$

si rappresenta in forma matriciale come

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

e in forma compatta con $AX = b$ ove $A \in M_{m,n}(C)$, $X = (X_1, \dots, X_n)^t$ e $b \in C^m$.

La matrice A si dice la matrice incompleta del sistema, la matrice $(Ab) \in M_{m,n+1}(C)$ si dice la matrice completa del sistema. Il sistema si dice quadrato se $m=n$. Omogeneo se b è il vettore nullo.

Soluzioni del sistema sono le n -ple $(x_1, \dots, x_n)^t \in C^n$ per cui valgono tutte le uguaglianze. Nel caso sia vuoto il sistema si dice impossibile. Geometricamente si tratta di trovare l'antimmagine di $b \in C^m$ per l'applicazione $C^n \rightarrow C^m$ che è rappresentata dalla matrice A nelle basi canoniche.

Se il sistema è omogeneo si tratta di un sottospazio vettoriale di C^n (il nucleo della suddetta applicazione lineare).

Sistemi equivalenti. Due sistemi $AX=b$ e $A'X=b'$ con $A, A' \in M_{m,n}(C)$ si dicono equivalenti se hanno lo stesso insieme di soluzioni.

Se $H \in M_m(C)$ è una matrice invertibile, allora $AX=b$ è equivalente a $(HA)X=Hb$.

Rouché-Capelli. Il sistema $AX=b$ con $A \in M_{m,n}(C)$ ammette soluzioni se e solo se il rango della matrice completa è uguale al rango della matrice incompleta, sia r , e in tal caso se x è una tale soluzione, l'insieme di tutte le soluzioni si scrive come $x+W$ dove W è il sottospazio vettoriale di C^n delle soluzioni del sistema lineare omogeneo associato, i.e. $AX=0$; si ha che $\dim_C W = n-r$.

Riduzione di Gauss. Tramite operazioni elementari sulle righe della matrice completa si può trasformare il sistema in un sistema equivalente in forma a scalini, da cui si leggono subito i ranghi delle matrici, e si scrivono le eventuali soluzioni.

Cramer. Il sistema $AX=b$ con $A \in M_n(C)$ (sistema quadrato) ha un'unica soluzione se e solo se $\det A \neq 0$, i.e. se la matrice A è invertibile, e in tal caso la soluzione è $x=A^{-1}b$. Se $A(i)$ è la matrice che si ottiene da A sostituendo la i -sima colonna con la colonna b dei termini noti, si ha che $x_i = |A(i)| / |A|$.

Geometria Affine.

Assiomi. Uno Spazio Affine con spazio delle traslazioni V (spazio vettoriale di dimensione n su un corpo C) è un insieme \mathbb{A} dotato di una azione di V : $\mathbb{A} \times V \rightarrow \mathbb{A}$: $(x, v) \mapsto x+v$ soggetti ai seguenti assiomi:

azione nulla: $x+0=x$ ($\forall x$);

associatività: $(x+v)+w=x+(v+w)$ ($\forall x, v, w$);

differenza di punti: $(\forall x, y)(\exists! v)x+v=y$. (l'unico vettore v si scrive $v=y-x$, sicché possiamo parlare di "differenza tra punti").

Coordinate. Lo spazio affine standard $\mathbb{A}^n(C)$ di dimensione n su C con spazio delle traslazioni $V_n(C)$ è l'insieme C^n . La scelta di un punto $O \in \mathbb{A}$ e di una base $e=(e_1, \dots, e_n)$ di V determinano un sistema di coordinate in \mathbb{A} : ogni punto $P \in \mathbb{A}$ si scrive unicamente come $P=O+\sum_i x_i e_i$, e (x_1, \dots, x_n) si dicono le coordinate di P nel riferimento dato da (O, e_1, \dots, e_n) .

Equivalentemente si possono scegliere $n+1$ punti O, P_1, \dots, P_n tali che i vettori $P_i - O$ siano li, dunque una base di V .

Sottospazi affini. Un sottinsieme del tipo $P+W$ con $P \in \mathbb{A}$ e W un sottospazio vettoriale di V di dimensione m si dice una varietà affine di dimensione m di \mathbb{A} ; W si chiama lo spazio direttore.

Una varietà affine di descrive tramite equazioni parametriche: se w_1, \dots, w_m sono una base di W , allora ogni punto X di $P+W$ si scrive come $X=P+\sum_i \alpha_i w_i$ ove gli $\alpha_i \in C$ sono i parametri e, se P ha coordinate (x_1, \dots, x_n) , si può esplicitare:

$$\begin{cases} X_1 = x_1 + \sum_i \alpha_i w_{i,1} \\ \dots \\ X_n = x_n + \sum_i \alpha_i w_{i,n} \end{cases}$$

Oppure tramite un sistema di $n-m$ equazioni lineari (rappresentazione cartesiana) che si ottengono dalla condizione

$$\text{rk}(X - x \quad w_1 \quad \dots \quad w_m) \leq m$$

(esiste una sottomatrice quadrata invertibile di ordine m : e allora basta annullare i determinanti di ordine $m+1$ contenenti quella sottomatrice). Equivalentemente si può chiedere che

$$\text{rk}\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ X & x & w_1 & \dots & w_m \end{pmatrix} \leq m+1.$$

Viceversa un sistema lineare di m equazioni nelle incognite $X=(X_1, \dots, X_n)$ (che abbia soluzioni) determina una varietà affine di dimensione $n-r$ ove r è il rango comune delle matrici completa e incompleta. Il sistema di equazioni si dice minima se è composto esattamente di r equazioni. Risolvere il sistema equivale a trovare una rappresentazione parametrica per la varietà lineare.

Posizioni reciproche di sottospazi affini: siano $L=P+W$ e $L'=P'+W'$, con $m:=\dim_C W$ e $m':=\dim_C W'$; i due sottospazi si dicono incidenti se $L \cap L' \neq \emptyset$ (e l'intersezione è un sottospazio affine); disgiunti in caso contrario. Si dicono parallele se $W \subseteq W'$ o $W' \subseteq W$; in tal caso possono appartenersi ($L \subseteq L'$ resp. $L' \subseteq L$) oppure essere disgiunte. Si dicono sghembe sono disgiunte e se $W \cap W' = \emptyset$.

Poniamo $L \wedge L' := L \cap L'$, e $L \vee L' :=$ minima sottovarietà contenente L e L' , detta la congiungente di L ed L' , che si descrive come $P + \langle P' - P, W, W' \rangle$ ovvero $P' + \langle P - P', W, W' \rangle$ se le varietà sono disgiunte, altrimenti possiamo supporre $P=P'$ e allora si tratta di $P' + \langle W, W' \rangle$.

Formule di Grassmann affini: $\dim_C(L \vee L') + \dim_C(L \wedge L') \leq \dim_C L + \dim_C L'$ e vale l'uguaglianza se L e L' sono incidenti oppure sghembe ($\dim_C \emptyset := -1$); se le varietà sono disgiunte (in particolare parallele) è $\dim_C(L \vee L') + \dim_C(W \cap W') = \dim_C L + \dim_C L' + 1$.

Due sottospazi affini si dicono complementari se sono sghembi e la loro congiungente è tutto lo spazio affine; in particolare la somma delle loro dimensioni è $n-1$ (e dunque gli spazi direttori non sono complementari).

Condizioni di indipendenza tra punti: una collezione di $m+1$ punti $P_0, P_1, \dots, P_m \in \mathbb{A}$ si dice indipendente se i vettori $P_1 - P_0, \dots, P_m - P_0 \in V$ sono li. Ciò si verifica sse la matrice $(P_1 - P_0 \quad \dots \quad P_m - P_0)$ ha rango m (dunque $m \leq n$), ovvero sse la matrice

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ P_0 & P_1 & \dots & P_m \end{pmatrix}$$

ha rango $m+1$.

Una collezione indipendente di $m+1$ punti $P_0, P_1, \dots, P_m \in \mathbb{A}$ determina una varietà affine di dimensione m : la più piccola varietà affine contenente quei punti. Ha equazioni parametriche $X = P_0 + \sum_i \alpha_i (P_i - P_0)$ ed equazioni cartesiane date dalla condizione:

$$\text{rk}(X - P_0 \quad P_1 - P_0 \quad \dots \quad P_m - P_0) \leq m$$

ovvero che

$$\text{rk}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ X & P_0 & P_1 & \dots & P_m \end{pmatrix} \leq m+1.$$

Calcolo baricentrico. Dati $m+1$ punti $P_0, P_1, \dots, P_m \in \mathbb{A}$ e m coefficienti $\alpha_1, \dots, \alpha_m \in C$ tali che $\sum_i \alpha_i = 1$, il punto definito da $P := P_0 + \sum_i \alpha_i (P_i - P_0)$ risulta indipendente dal punto di base P_0 e si può dunque scrivere come $P := \sum_i \alpha_i P_i$ ("somma pesata di punti": la somma dei punti è definita solo se i coefficienti hanno somma 1). Il punto P si dice il baricentro del sistema dei punti $P_1, \dots, P_m \in \mathbb{A}$ con i pesi rispettivi $\alpha_1, \dots, \alpha_m \in C$.

Un sottinsieme L di \mathbb{A} è un sottospazio affine se e solo se è stabile per somme pesate di punti, ovvero sse quando contiene

due punti contiene la retta generata (combinazioni pesate di due punti).

Le combinazioni pesate di m punti indipendenti descrivono lo spazio affine generato da quei punti. In particolare: le combinazioni pesate di due punti distinti descrivono la retta congiungente i due punti; le combinazioni pesate di tre punti non allineati descrivono il piano congiungente i tre punti.

Il punto medio del segmento tra P_1 e P_2 è $\frac{1}{2}P_1 + \frac{1}{2}P_2$.

Il baricentro del triangolo di vertici P_1 , P_2 e P_3 sta nelle rette congiungenti un vertice col punto medio del lato opposto ed è $\frac{1}{3}P_1 + \frac{1}{3}P_2 + \frac{1}{3}P_3$.

Nel caso $C=\mathbb{R}$, possiamo descrivere il segmento tra P_1 e P_2 come le combinazioni pesate dei due punti con i combinatori $\alpha_1, \alpha_2 \in [0, 1]$; il triangolo di vertici P_1 , P_2 e P_3 tramite le combinazioni pesate con $\alpha_1, \alpha_2, \alpha_3 \in [0, 1]$; in generale l'inviluppo convesso di m punti si rappresenta tramite le combinazioni $\sum_i \alpha_i P_i$ con $\sum_i \alpha_i = 1$ e $0 \leq \alpha_i \leq 1$ per ogni i .

Dati tre punti allineati $X, A, B \in \mathbb{A}$, se $X = \lambda A + \mu B$ con $\lambda + \mu = 1$, definiamo $(XAB) = DR(X; A, B) := -\frac{\mu}{\lambda}$. Se $\xi, \alpha, \beta \in C$ sono le coordinate di X, A, B , allora $(XAB) = \frac{\xi - \beta}{\xi - \alpha}$ (“rapporto tra le distanze”). X è il punto medio tra A e B sse $(XAB) = -1$.

Azione delle permutazioni: Se $(ABC) = \lambda$, allora: $(BAC) = \frac{\lambda}{\lambda-1}$; $(ACB) = \frac{1}{\lambda}$; $(CBA) = 1 - \lambda$; $(BCA) = \frac{\lambda-1}{\lambda}$; $(CAB) = \frac{1}{1-\lambda}$.

Abbiamo che $(ABC) = (ABD)(ADC)$.

Sia dato un triangolo di vertici i punti A, B, C (non allineati); siano A', B', C' tre punti rispettivamente sulle rette $B \vee C$, $A \vee C$, $A \vee B$; allora:

Teorema di Menelao: A', B', C' sono allineati sse

$$(A'BC)(B'CA)(C'AB) = 1;$$

Teorema di Ceva: $A \vee A'$, $B \vee B'$, $C \vee C'$ si incontrano in un punto sse $(A'BC)(B'CA)(C'AB) = -1$.

Affinità. Una affinità di \mathbb{A} è una biiezione $F: \mathbb{A} \rightarrow \mathbb{A}$ che rispetti la somma pesata dei punti, i.e. $F(\sum_i \alpha_i P_i) = \sum_i \alpha_i F(P_i)$ se $\sum_i \alpha_i = 1$. Ciò equivale all'esistenza di $\varphi \in \text{Aut}_C(V)$ tale che $F(P+v) = F(P) + \varphi(v)$ per ogni $P \in \mathbb{A}$ e $v \in V$; o ancora tale che $F(P) - F(Q) = \varphi(P-Q)$ per ogni $P, Q \in \mathbb{A}$. L'insieme delle affinità di \mathbb{A} è un gruppo sotto la composizione e si indica con $\text{Aff}(\mathbb{A})$.

Fissato $R \in \mathbb{A}$, ogni affinità è determinata da un vettore $v = F(R) - R$ e dalla applicazione lineare associata φ , tramite: $F(Q) = R + v + \varphi(P-Q)$. Questo dà un isomorfismo di gruppi $\text{Aff}(\mathbb{A}) \rightarrow V \times \text{Aut}_C(V)$ ove la legge di gruppo di $V \times \text{Aut}_C(V)$ è data da $(v, \varphi) \circ (w, \psi) = (v + \varphi w, \varphi \circ \psi)$.

Diciamo traslazioni di \mathbb{A} le affinità con $\varphi = \text{id}_V$; gli elementi di $\text{Trasl}(\mathbb{A})$ sono determinati da $v \in V$ e risulta $\text{Trasl}(\mathbb{A}) \cong V$.

Diciamo affinità centrali di centro R le affinità che tengono fisso R ; si indicano con $\text{Centr}_R(\mathbb{A})$ e sono determinate da $\varphi \in \text{Aut}_C(V)$ e risulta $\text{Centr}_R(\mathbb{A}) \cong \text{Aut}_C(V)$.

La scelta di un riferimento affine (O, e) ove e è una base di V identifica $\text{Aff}(\mathbb{A})$ al sottogruppo di $\text{GL}(n+1, C)$ delle matrici della forma $\begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}$ dove $v \in V$ e $A' \in \text{GL}(n, C)$.

Siano $\varphi \in \text{Aff}(\mathbb{A})$ e L un sottinsieme di \mathbb{A} ; allora L è sottovarietà affine se e solo se $\varphi(L)$ lo è, e in tal caso hanno la stessa dimensione. Se L è definita dalle equazioni $BX = b$ e φ è rappresentata dalla matrice $A = \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}$ allora $\varphi(L)$ è definita dalle equazioni $BA'^{-1}X = b + BA'^{-1}v$. In forma compatta: L è dato da $(-bB)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0$, $\varphi(L)$ da $(-bB)A^{-1}\begin{pmatrix} 1 \\ X \end{pmatrix} = 0$.

Simmetrie. Siano U e V sottospazi complementari di $V_n(C)$ (i.e. $V_n(C) = U \oplus V$). La simmetria di $\mathbb{A}^n(C)$ di asse la varietà affine $P+U$ e direzione il sottospazio V è l'affinità definita dall'avere P come punto unito e applicazione lineare associata

la simmetria di $V_n(C)$ di asse U e direzione V (i.e. l'applicazione che al vettore $u+v$ con $u \in U$ e $v \in V$ associa $u-v$). I punti uniti della simmetria sono tutti e soli i punti di $P+U$. Inoltre il quadrato di una simmetria è sempre l'identità.

Proiezioni (parallele, o dall'infinito). Siano U e V sottospazi complementari di $V_n(C)$ (i.e. $V_n(C) = U \oplus V$). La proiezione di $\mathbb{A}^n(C)$ sulla varietà affine $P+U$ nella direzione del sottospazio V è la trasformazione affine definita dall'avere P come punto unito e applicazione lineare associata la proiezione di $V_n(C)$ su U con direzione V (i.e. l'applicazione che al vettore $u+v$ con $u \in U$ e $v \in V$ associa u). I punti uniti della proiezione sono tutti e soli i punti di $P+U$. Inoltre il quadrato di una proiezione è sempre la proiezione stessa. Una proiezione è una affinità sse è la funzione identica.

Proiezioni di centro affine. Siano L e L' sottospazi affini complementari di $\mathbb{A}^n(C)$ (i.e. sgombri e $\mathbb{A}^n(C) = L \vee L'$). La proiezione $\pi: \mathbb{A}^n(C) \setminus L' \rightarrow \mathbb{A}^n(C)$ di $\mathbb{A}^n(C)$ su L e di centro L' è la funzione definita da $\pi(P) = (P \vee L') \wedge L$. Si tratta di una funzione $\pi: \mathbb{A}^n(C) \setminus L' \rightarrow L$ suriettiva i cui punti fissi sono esattamente gli elementi di L . Per ogni sottospazio affine M complementare con L' (dunque della stessa dimensione di L), π si restringe a una affinità $\pi: M \rightarrow L$ che si dice proiezione da M a L di centro L' .

Piano affine: \mathbb{A}^2 . Siano $P_i = (x_i, y_i)^t \in \mathbb{A}^2$ punti del piano e $v_i = (l_i, m_i)^t \in V$ vettori dello spazio direttore.

condizione di allineamento di tre punti:

$$\begin{vmatrix} x_1 - x_0 & x_2 - x_0 \\ y_1 - y_0 & y_2 - y_0 \end{vmatrix} = 0, \text{ ovvero } \begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{vmatrix} = 0.$$

retta per due punti: $P_0 + \langle P_1 - P_0 \rangle$;

$$\text{equazioni parametriche } \begin{cases} X = x_0 + \alpha(x_1 - x_0) \\ Y = y_0 + \alpha(y_1 - y_0) \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & x_1 - x_0 \\ Y - y_0 & y_1 - y_0 \end{vmatrix} = 0, \text{ ovvero } \begin{vmatrix} 1 & 1 & 1 \\ X & x_0 & x_1 \\ Y & y_0 & y_1 \end{vmatrix} = 0.$$

retta per un punto e direzione un vettore: $P_0 + \langle v_0 \rangle$;

$$\text{equazioni parametriche } \begin{cases} X = x_0 + \alpha l_0 \\ Y = y_0 + \alpha m_0 \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & l_0 \\ Y - y_0 & m_0 \end{vmatrix} = 0, \text{ ovvero } \begin{vmatrix} 1 & 1 & 0 \\ X & x_0 & l_0 \\ Y & y_0 & m_0 \end{vmatrix} = 0.$$

Posizione reciproche di due rette: date due rette $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ di equazioni cartesiane rispettivamente $a_0 X + b_0 Y + c_0 = 0$ e $a_1 X + b_1 Y + c_1 = 0$, esse risultano:

incidenti se v_0 e v_1 sono *li*; ovvero sse la matrice $\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}$ ha rango due. In tal caso il punto di incidenza ha coordinate date dalla regola di Cramer applicata al sistema delle due equazioni.

parallele e distinte se v_0 e v_1 sono *ld* e $P_0 \notin r_1$; ovvero sse la matrice incompleta $\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}$ ha rango uno e la matrice completa $\begin{pmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{pmatrix}$ ha rango due.

coincidenti se v_0 e v_1 sono *ld* e $P_0 \in r_1$; ovvero sse le matrici incomplete e completa hanno rango uno.

fasci di rette: le rette passanti per un fissato punto P_0 si scrivono come $P_0 + \langle \begin{pmatrix} l \\ m \end{pmatrix} \rangle$, ovvero $m(X-x_0) - l(Y-y_0) = 0$ con $(l, m) \neq (0, 0)$.

le rette parallele ad un fissato vettore direzione v_0 si scrivono come $P + \langle v_0 \rangle$ con P punto qualsiasi, ovvero $m_0 X - l_0 Y + c = 0$ con $c \in C$.

due rette distinte r_0 e r_1 determinano un fascio di rette che si descrive tramite $\lambda(a_0 X + b_0 Y + c_0) + \mu(a_1 X + b_1 Y + c_1) = 0$, ovvero $(\lambda a_0 + \mu a_1)X + (\lambda b_0 + \mu b_1)Y + (\lambda c_0 + \mu c_1) = 0$ per $(\lambda, \mu) \neq (0, 0)$.

Una retta r_2 appartiene al fascio determinato da r_0 e r_1 se e solo se la matrice completa del sistema delle tre rette ha determinante nullo.

Spazio affine: \mathbb{A}^3 . Siano $P_i = (x_i, y_i, z_i)^t \in \mathbb{A}^3$ punti dello spazio e $v_i = (l_i, m_i, n_i)^t \in V$ vettori dello spazio delle traslazioni.

condizione di complanarità di quattro punti:

$$\begin{vmatrix} x_1 - x_0 & x_2 - x_0 & x_3 - x_0 \\ y_1 - y_0 & y_2 - y_0 & y_3 - y_0 \\ z_1 - z_0 & z_2 - z_0 & z_3 - z_0 \end{vmatrix} = 0, \text{ ovvero } \begin{vmatrix} 1 & 1 & 1 & 1 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ z_0 & z_1 & z_2 & z_3 \end{vmatrix} = 0.$$

condizione di allineamento di tre punti:

$$\text{rk} \begin{pmatrix} x_1 - x_0 & x_2 - x_0 \\ y_1 - y_0 & y_2 - y_0 \\ z_1 - z_0 & z_2 - z_0 \end{pmatrix} = 1, \text{ ovvero } \text{rk} \begin{pmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{pmatrix} = 2.$$

piano per tre punti non allineati: $P_0 + \langle P_1 - P_0, P_2 - P_0 \rangle$;

$$\text{equazioni parametriche} \quad \begin{cases} X = x_0 + \alpha_1(x_1 - x_0) + \alpha_2(x_2 - x_0) \\ Y = y_0 + \alpha_1(y_1 - y_0) + \alpha_2(y_2 - y_0) \\ Z = z_0 + \alpha_1(z_1 - z_0) + \alpha_2(z_2 - z_0) \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & x_1 - x_0 & x_2 - x_0 \\ Y - y_0 & y_1 - y_0 & y_2 - y_0 \\ Z - z_0 & z_1 - z_0 & z_2 - z_0 \end{vmatrix} = 0, \text{ ovvero } \begin{vmatrix} 1 & 1 & 1 & 1 \\ X & x_0 & x_1 & x_2 \\ Y & y_0 & y_1 & y_2 \\ Z & z_0 & z_1 & z_2 \end{vmatrix} = 0.$$

piano per un punto e direzione due vettori li: $P_0 + \langle v_0, v_1 \rangle$;

$$\text{equazioni parametriche} \quad \begin{cases} X = x_0 + \alpha l_0 + \beta l_1 \\ Y = y_0 + \alpha m_0 + \beta m_1 \\ Z = z_0 + \alpha n_0 + \beta n_1 \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & l_0 & l_1 \\ Y - y_0 & m_0 & m_1 \\ Z - z_0 & n_0 & n_1 \end{vmatrix} = 0 \text{ ovvero } \begin{vmatrix} 1 & 1 & 0 & 0 \\ X & x_0 & l_0 & l_1 \\ Y & y_0 & m_0 & m_1 \\ Z & z_0 & n_0 & n_1 \end{vmatrix} = 0.$$

posizioni reciproche di due piani: dati due piani $\pi_0 = P_0 + \langle v_0, v'_0 \rangle$ e $\pi_1 = P_1 + \langle v_1, v'_1 \rangle$ di equazioni cartesiane rispettivamente $a_0 X + b_0 Y + c_0 Z + d_0 = 0$ e $a_1 X + b_1 Y + c_1 Z + d_1 = 0$, essi risultano:

incidenti se $\text{rk}(v_0 v'_0 v_1 v'_1) = 3$; ovvero sse la matrice $\begin{pmatrix} a_0 b_0 c_0 \\ a_1 b_1 c_1 \end{pmatrix}$ ha rango due. In tal caso la retta di incidenza ha equazioni cartesiane date dal sistema delle due equazioni.

paralleli e distinti se $\text{rk}(v_0 v'_0 v_1 v'_1) = 2$; (i.e. gli spazi direttori coincidono: $\langle v_0, v'_0 \rangle = \langle v_1, v'_1 \rangle$) e $P_0 \notin \pi_1$ (i.e. $\pi_0 \cap \pi_1 = \emptyset$); ovvero sse la matrice incompleta $\begin{pmatrix} a_0 b_0 c_0 \\ a_1 b_1 c_1 \end{pmatrix}$ ha rango uno e la matrice completa $\begin{pmatrix} a_0 b_0 c_0 d_0 \\ a_1 b_1 c_1 d_1 \end{pmatrix}$ ha rango due.

coincidenti se gli spazi direttori coincidono e $P_0 \in \pi_1$; ovvero sse le matrici incomplete e completa hanno rango uno.

fasci di piani: i piani contenenti una fissata retta $r_0 = P_0 + \langle v_0 \rangle$

(asse del fascio) di equazioni cartesiane $\begin{cases} a_0 X + b_0 Y + c_0 Z + d_0 = 0 \\ a'_0 X + b'_0 Y + c'_0 Z + d'_0 = 0 \end{cases}$

si scrivono come $P_0 + \langle v_0, (l, m, n)^t \rangle$ con (l, m, n) vettore li con v_0 , ovvero $\lambda(a_0 X + b_0 Y + c_0 Z + d_0) + \mu(a'_0 X + b'_0 Y + c'_0 Z + d'_0) = 0$ (i.e. $(\lambda a_0 + \mu a'_0)X + (\lambda b_0 + \mu b'_0)Y + (\lambda c_0 + \mu c'_0)Z + (\lambda d_0 + \mu d'_0) = 0$ con $(\lambda, \mu) \neq (0, 0)$).

i piani paralleli ad un fissato spazio direttore $\langle v_0, v_1 \rangle$ si scrivono come $P + \langle v_0, v_1 \rangle$ con P punto qualsiasi, ovvero $(m_0 n_1 - n_0 m_1)X + (-l_0 n_1 + n_0 l_1)Y + (l_0 m_1 - m_0 l_1)Z + c = 0$ con $c \in C$ (i coefficienti sono i minori d'ordine due di $(v_0 v_1)$).

due piani distinti π_0 e π_1 determinano un fascio di piani descritto da $\lambda(a_0 X + b_0 Y + c_0 Z + d_0) + \mu(a_1 X + b_1 Y + c_1 Z + d_1) = 0$, ovvero $(\lambda a_0 + \mu a_1)X + (\lambda b_0 + \mu b_1)Y + (\lambda c_0 + \mu c_1)Z + (\lambda d_0 + \mu d_1) = 0$ per $(\lambda, \mu) \neq (0, 0)$.

un piano π_2 appartiene al fascio di piani determinato da π_0 e π_1 se e solo se la matrice completa del sistema dei tre piani ha rango due.

stelle di piani: i piani passanti per un fissato punto P_0 si scrivono come $P_0 + \langle v, w \rangle$ con v e w vettori li, ovvero $m(X - x_0) + l(Y - y_0) + n(Z - z_0) = 0$ con $(l, m, n) \neq (0, 0, 0)$.

i piani paralleli ad un fissato vettore direzione v_0 (ovvero a una qualsiasi retta r_0 di direzione v_0) si scrivono come $P + \langle v_0, v \rangle$ con P punto qualsiasi e v vettore li con v_0 , ovvero $aX + bY + cZ + d = 0$ con $d \in C$, $(a, b, c) \neq (0, 0, 0)$ tale che $al_0 + bm_0 + cn_0 = 0$.

tre piani distinti π_0 , π_1 e π_2 che non appartengano ad un fascio determinano una stella di piani che si descrive tramite $\lambda(a_0 X + b_0 Y + c_0 Z + d_0) + \mu(a_1 X + b_1 Y + c_1 Z + d_1) + \nu(a_2 X + b_2 Y + c_2 Z + d_2) = 0$, ovvero $(\lambda a_0 + \mu a_1 + \nu a_2)X + (\lambda b_0 + \mu b_1 + \nu b_2)Y + (\lambda c_0 + \mu c_1 + \nu c_2)Z + (\lambda d_0 + \mu d_1 + \nu d_2) = 0$ per $(\lambda, \mu, \nu) \neq (0, 0, 0)$.

retta per due punti distinti: $P_0 + \langle P_1 - P_0 \rangle$;

$$\text{equazioni parametriche} \quad \begin{cases} X = x_0 + \alpha(x_1 - x_0) \\ Y = y_0 + \alpha(y_1 - y_0) \\ Z = z_0 + \alpha(z_1 - z_0) \end{cases}$$

ed equazioni cartesiane date dalla condizione:

$$\text{rk} \begin{pmatrix} X - x_0 & x_1 - x_0 \\ Y - y_0 & y_1 - y_0 \\ Z - z_0 & z_1 - z_0 \end{pmatrix} = 1, \text{ ovvero } \text{rk} \begin{pmatrix} 1 & 1 & 1 \\ X & x_0 & x_1 \\ Y & y_0 & y_1 \\ Z & z_0 & z_1 \end{pmatrix} = 2.$$

retta per un punto e di direzione un vettore: $P_0 + \langle v_0 \rangle$;

$$\text{equazioni parametriche} \quad \begin{cases} X = x_0 + \alpha l_0 \\ Y = y_0 + \alpha m_0 \\ Z = z_0 + \alpha n_0 \end{cases}$$

ed equazioni cartesiane date da:

$$\text{rk} \begin{pmatrix} X - x_0 & l_0 \\ Y - y_0 & m_0 \\ Z - z_0 & n_0 \end{pmatrix} = 1 \text{ ovvero } \text{rk} \begin{pmatrix} 1 & 1 & 0 \\ X & x_0 & l_0 \\ Y & y_0 & m_0 \\ Z & z_0 & n_0 \end{pmatrix} = 2.$$

posizione reciproche di due rette: date due rette $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ di equazioni cartesiane rispettivamente

$$\begin{cases} a_0 X + b_0 Y + c_0 Z + d_0 = 0 \\ a'_0 X + b'_0 Y + c'_0 Z + d'_0 = 0 \end{cases} \text{ e } \begin{cases} a_1 X + b_1 Y + c_1 Z + d_1 = 0 \\ a'_1 X + b'_1 Y + c'_1 Z + d'_1 = 0 \end{cases}$$

esse risultano:

sghembe se v_0 e v_1 sono li e $r_0 \cap r_1 = \emptyset$, ovvero sse la matrice incompleta del sistema delle due rette ha rango tre, e la matrice completa rango quattro;

incidenti e distinte se v_0 e v_1 sono li e $r_0 \cap r_1 \neq \emptyset$; ovvero sse le matrici incomplete e completa hanno rango tre. In tal caso il piano di appartenenza è dato da $P_0 + \langle v_0, v_1 \rangle$ ed è l'unico piano appartenente a entrambi i fasci di asse le due rette. Il punto di incidenza ha coordinate date dalla soluzione del sistema delle quattro equazioni.

parallele e distinte se v_0 e v_1 sono ld e $r_0 \cap r_1 = \emptyset$; ovvero sse la matrice incompleta ha rango due e la matrice completa ha rango tre. Il piano di appartenenza è $P_0 + \langle P_1 - P_0, v_0 \rangle$ ed è l'unico piano appartenente a entrambi i fasci di asse le due rette.

coincidenti se v_0 e v_1 sono ld e $r_0 \cap r_1 \neq \emptyset$; ovvero sse la matrice incompleta e la matrice completa hanno rango due.

fasci di rette in un piano: con equazioni cartesiane, si tratta di intersecare il piano dato con la stella dei piani che soddisfano alle condizioni poste (passaggio per un punto o contenente una fissata direzione).

Se $\pi_0 = P_0 + \langle v_0, v'_0 \rangle$ è il piano di giacenza, e si tratta del fascio per $P_1 \in \pi_0$, il fascio di rette si scrive come $P_1 + \langle \alpha v_0 + \beta v'_0 \rangle$ con $(\alpha, \beta) \neq (0, 0)$; se si tratta del fascio di rette di direzione $v_1 \in \langle v_0, v'_0 \rangle$ allora si scrive come $(P_0 + \alpha v_0 + \beta v'_0) + \langle v_1 \rangle$ con (α, β) qualsiasi.

stelle di rette: le rette passanti per un fissato punto P_0 si scrivono come $P_0 + \langle (l, m, n)^t \rangle$ con $(l, m, n) \neq (0, 0, 0)$, ovvero scegliendo due equazioni indipendenti tra $m(X - x_0) - l(Y - y_0) = 0$, $n(X - x_0) - l(Z - z_0) = 0$ e $n(Y - y_0) - m(Z - z_0) = 0$.

le rette parallele ad un fissato vettore direzione v_0 si scrivono come $P+\langle v_0 \rangle$ con $P=(x,y,z)^t$ punto qualsiasi, ovvero scegliendo due equazioni indipendenti tra $m_0(X-x)-l_0(Y-y)=0$, $n_0(X-x)-l_0(Z-z)=0$ e $n_0(Y-y)-m_0(Z-z)=0$.

posizioni reciproche di rette e piani: dati un piano $\pi_0=P_0+\langle v_0, v'_0 \rangle$ e una retta $r_1=P_1+\langle v_1 \rangle$, di equazioni cartesiane rispettivamente $a_0X+b_0Y+c_0Z+d_0=0$ e $\begin{cases} a_1X+b_1Y+c_1Z+d_1=0 \\ a'_1X+b'_1Y+c'_1Z+d'_1=0 \end{cases}$, essi risultano:

incidenti se v_0, v'_0 e v_1 sono l ; ciò accade sse le matrici completa e incompleta del sistema piano-rettina hanno rango comune tre; le coordinate del punto di intersezione si ottengono applicando la regola di Cramer a tale sistema;

paralleli e disgiunti se $v_1 \in \langle v_0, v'_0 \rangle$ (i.e. se v_0, v'_0 e v_1 sono ld) e $\pi_0 \cap r_1 = \emptyset$; ovvero sse la matrice incompleta ha rango due e la matrice completa ha rango tre.

appartenersi se $v_1 \in \langle v_0, v'_0 \rangle$ (i.e. se v_0, v'_0 e v_1 sono ld) e $\pi_0 \cap r_1 \neq \emptyset$; ovvero sse le matrici incompleta e completa hanno rango due. In tal caso $r_1 \subseteq \pi_0$.

Geometria Euclidea.

Uno Spazio Euclideo Reale è uno Spazio Affine \mathbb{E} il cui spazio delle traslazioni sia uno spazio vettoriale euclideo reale.

Interpretazione euclidea delle equazioni cartesiane: i coefficienti delle variabili formano dei vettori che sono ortogonali al sottospazio direttrice della varietà. Se L è il sottospazio $P_0+\langle v_1, \dots, v_m \rangle$ ed ha equazioni cartesiane date dal sistema $AX-b=0$ con $A \in M_{r,n}$, $b \in \mathbb{R}^m$ ed $r=n-m$, allora risulta che le righe A^1, \dots, A^r intese come (coordinate di) elementi di V sono indipendenti e ortogonali al sottospazio $\langle v_1, \dots, v_m \rangle$. Si ha $V=\langle v_1, \dots, v_m \rangle \boxplus \langle A^1, \dots, A^r \rangle$.

Distanza tra punti: Definiamo la funzione distanza $d: \mathbb{E} \times \mathbb{E} \rightarrow \mathbb{R}$ tramite: $d(P, Q) := \|Q - P\|$.

Proprietà della funzione distanza:

$d(P, Q) = 0$ se e solo se $P = Q$;

simmetria: $d(P, Q) = d(Q, P)$;

disuguaglianza triangolare: $d(P, Q) \leq d(P, R) + d(R, Q)$.

Distanza tra punti e sottospazi: la distanza tra un punto P_1 e il sottospazio L è definita come $d(P_1, L) := \inf_{Q \in L} d(P_1, Q)$. Si annulla se e solo se $P_1 \in L$. Se $P_1 \notin L$ allora esiste unico $P'_1 \in L$ tale che $d(P_1, L) + d(P'_1, Q)$, e si chiama il punto di minima distanza. Si trova imponendo al generico vettore $P_1 - P_0 + \sum \alpha_i v_i$ di essere ortogonale ad ogni v_i (si tratta di un sistema quadrato con incognite le α_i).

Distanza tra sottospazi: siano L ed L' sue sottospazi di dimensioni m ed m' ; la loro distanza è definita da $d(L, L') := \inf_{Q \in L, Q' \in L'} d(Q, Q')$. Si annulla se e solo se $L \cap L' \neq \emptyset$. Se $L \cap L' = \emptyset$, allora si possono trovare i punti di minima distanza $P \in L$ e $P' \in L'$, cioè tali che $d(L, L') = d(P, P')$, imponendo al generico vettore $P_0 - P'_0 + \sum \alpha_i v_i - \sum \beta_j v'_j$ di essere ortogonale a ogni v_i e ad ogni v'_j . I punti di minima distanza sono unici se e solo se le varietà L ed L' sono sghembe.

In generale: $d(P+W, P'+W') = d(P, P'+W'+W)$.

Se r è retta per P e direzione v , allora per ogni punto Q si ha $d(Q, r)^2 = \|Q - P\|^2 - \frac{((Q - P) \cdot v)^2}{\|v\|^2}$.

Se π è iperpiano di equazione $a_1X_1 + \dots + a_nX_n + a_0 = 0$ (in un riferimento ortonormale) allora per ogni punto Q di coordinate (q_i) (nello stesso riferimento) si ha $d(Q, \pi) = \frac{|a_1q_1 + \dots + a_nq_n + a_0|}{\sqrt{a_1^2 + \dots + a_n^2}}$.

Se invece π è iperpiano per P e di direzione v_1, \dots, v_{n-1} allora per ogni punto Q si ha $d(Q, \pi) = \frac{|\det(Q - P, v_1, \dots, v_{n-1})|}{\|\text{cross}(v_1, \dots, v_{n-1})\|}$.

Area di triangoli: dati tre punti non allineati P_0 , P_1 e P_2 , detti $P_1 - P_0 = (l_1, \dots, l_n)$ e $P_2 - P_0 = (m_1, \dots, m_n)$, l'area del triangolo da essi definito è $A(P_0, P_1, P_2) = \frac{1}{2} \sqrt{\sum_{i < j} (l_i m_j - l_j m_i)^2}$ (sotto radice vi sono i quadrati dei minori d'ordine due della matrice dei due vettori).

Volumi di m-edri: dati $m+1$ punti indipendenti P_0, \dots, P_m , detti $v_i = P_i - P_0$, risulta che l' $(m+1)$ -edro definito da quei punti ha misura m -dimensionale data da $\frac{1}{m!} \|(v_1 \dots v_m)\|$ ove definiamo la "norma" di una matrice $m \times n$ con $m \leq n$ come la radice quadrata della somma dei quadrati dei minori di ordine m della matrice stessa (si tratta di $\binom{n}{m}$ termini).

Per un insieme di indici $1 \leq i_1 < \dots < i_m \leq n$, abbreviato I , indichiamo con $P(I)$ la m -pla delle coordinate di P dei posti in I , e con $P(\bar{I})$ la $(n-m)$ -pla delle coordinate di P dei posti non in I . Allora l' m -volume in questione si scrive come

$$\frac{1}{m!} \sqrt{\sum_I \left| \begin{matrix} 1 & \dots & 1 \\ P_0(I) & \dots & P_m(I) \end{matrix} \right|^2}$$

ove la somma è sulle m -pla intere tali che $1 \leq i_1 < \dots < i_m \leq n$.

In particolare per $m=n-1$ risulta:

$$\frac{1}{(n-1)!} \sqrt{\sum_{i=1}^n \left| \begin{matrix} 1 & \dots & 1 \\ P_0(i) & \dots & P_{n-1}(i) \end{matrix} \right|^2}$$

E per $m=n$ risulta: $\frac{1}{n!} |\det \left(\begin{matrix} 1 & \dots & 1 \\ P_0 & \dots & P_n \end{matrix} \right)|$.

Trasformazioni Euclideanee, Rigidità, Conformità. Una applicazione $F \in \text{Aff}(\mathbb{E})$ si dice una congruenza (o rigidità, o isometria) se l'applicazione φ associata rispetta la struttura euclidea, i.e. il prodotto scalare. Si dice diretta o inversa a seconda che il determinante della isometria associata sia 1 o -1. Indichiamo con $\text{Rig}(\mathbb{E})$ questo gruppo (nota: $\text{Rig}(\mathbb{E}) \supseteq \text{Trasl}(\mathbb{E})$), e definiamo le rigidità centrali di centro R $\text{Rig}_R(\mathbb{E}) := \text{Rig}(\mathbb{E}) \cap \text{Centr}_R(\mathbb{E})$. Ogni elemento di $\text{Rig}(\mathbb{E})$ si può scrivere come composizione di una traslazione e di una rigidità di centro R preassegnato, e anche in ordine inverso.

Una applicazione $F \in \text{Aff}(\mathbb{E})$ si dice una similitudine (o omotetia) se esiste $\rho \in \mathbb{R}$ (positivo) tale che $d(F(P), F(Q)) = \rho d(P, Q)$. Ciò equivale a dire che F è una conformità, i.e. rispetta gli angoli tra i segmenti. Una dilatazione di centro R è un elemento di $\text{Centr}_R(\mathbb{E})$ la cui matrice associata sia $\alpha \mathbb{I}$ (α è il fattore di dilatazione); si tratta di una conformità. Ogni conformità si scrive come composizione di una rigidità seguita da una dilatazione di centro R preassegnato, o anche in ordine inverso.

Piano euclideo: \mathbb{E}^2 .

interpretazione euclidea delle equazioni cartesiane delle rette: la retta r di equazione $aX+bY+c=0$ ha direzione ortogonale al vettore $(a, b)^t$, dunque ha vettore direttrice $(b, -a)$. L'angolo $\vartheta(r, r')$ tra due rette r ed r' è l'angolo formato dai vettori normali alle due rette, e quindi $\cos \vartheta(r, r') = \frac{|aa' + bb'|}{\sqrt{a^2 + b^2} \sqrt{a'^2 + b'^2}}$.

distanza punto-rettta: $d(P_0, r) = \frac{|ax_0 + by_0 + c|}{\sqrt{a^2 + b^2}}$.

Se $r = P_1 + \langle v_1 \rangle$ e $u_1 = \text{cross}(v_1)$ (i.e. un vettore normale alla retta) allora $d(P_0, r) = \frac{|(P_1 - P_0) \cdot u_1|}{\|u_1\|}$.

asse di un segmento: si tratta della retta dei punti equidistanti dai due punti dati P_0 e P_1 ; si scrive $(\frac{1}{2}P_0 + \frac{1}{2}P_1) + \langle P_1 - P_0 \rangle^\perp$, oppure tramite l'equazione:

$$(x_1 - x_0) \left(X - \frac{x_0 + x_1}{2} \right) + (y_1 - y_0) \left(Y - \frac{y_0 + y_1}{2} \right) = 0.$$

bisettrici di due rette incidenti: se $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ e $\|v_0\| = \|v_1\|$, allora le bisettrici sono date da $P + \langle v_0 \pm v_1 \rangle$ ove $P = r_0 \cap r_1$.

se abbiamo equazioni cartesiane $a_0X+b_0Y+c_0=0$ e $a_1X+b_1Y+c_1=0$ con $a_0^2+b_0^2=a_1^2+b_1^2$ allora le bisettrici hanno equazioni $(a_0X+b_0Y+c_0)\pm(a_1X+b_1Y+c_1)=0$.

area di triangoli: $A(P_0, P_1, P_2) = \frac{1}{2} |\det \begin{pmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{pmatrix}|$.

distanza tra rette parallele: è la distanza tra un punto qualsiasi di una e l'altra retta.

Classificazione delle rigidità piane:

Rotazioni: sono le rigidità dirette che hanno un punto unito;

Traslazioni: Sono le rigidità dirette prive di punti uniti;

Riflessioni: sono le rigidità inverse che hanno punti uniti (una retta, in effetti, di punti uniti);

Glissoriflessioni: sono le rigidità inverse prive di punti uniti: si possono sempre scrivere come composizione di una riflessione e di una traslazione parallela all'asse di riflessione.

Spazio euclideo: \mathbb{E}^3 .

interpretazione euclidea delle equazioni dei piani e delle rette: il piano π di equazione cartesiana $aX+bY+cZ+d=0$ è ortogonale al vettore $(a,b,c)^t$; dunque il sottospazio direttrice del piano è dato da $((a,b,c)^t)^\perp$.

La retta $r=\pi\cap\pi'$ determinata dalle equazioni cartesiane di due piani non paralleli ha direzione ortogonale ai vettori $(a,b,c)^t$ e $(a',b',c')^t$, dunque un suo vettore direttrice è dato da $(a,b,c)^t \wedge (a',b',c')^t$.

L'angolo $\vartheta(\pi, \pi')$ tra due piani π e π' , corrisponde all'angolo tra i vettori normali, e dunque $\vartheta(\pi, \pi') = \frac{|aa'+bb'+cc'|}{\sqrt{a^2+b^2+c^2}\sqrt{a'^2+b'^2+c'^2}}$.

L'angolo tra due rette incidenti si misura come l'angolo tra i vettori direttori.

L'angolo tra un piano π e una retta $r=\pi\cap\pi''$ si scrive come $\sin\vartheta(\pi, r) = \frac{|(abc)v|}{\sqrt{a^2+b^2+c^2}\|v\|}$ se v è un vettore direttrice della retta, per esempio $v=(a'b'c')^t \wedge (a''b''c'')^t$.

distanza punto-piano: $d(P_0, \pi) = \frac{|ax_0+by_0+cz_0+d|}{\sqrt{a^2+b^2+c^2}}$.

Se $\pi=P_1+\langle v_1, v'_1 \rangle$ allora $d(P_0, \pi) = \frac{|(P_1-P_0) \cdot (v_1 \wedge v'_1)|}{\|v_1 \wedge v'_1\|}$

(interpretazione geometrica: il numeratore è il volume di un parallelepipedo di cui il denominatore è la base).

distanza tra piani paralleli: si tratta della distanza tra un punto qualsiasi di un piano e l'altro piano.

distanza retta-piano: è nulla se non sono paralleli, e in tal caso è la distanza di un punto qualsiasi della retta dal piano.

distanza retta-retta: siano $r=P+\langle v \rangle$ e $r'=P'+\langle v' \rangle$;

allora se r ed r' non sono parallele: $d(r, r') = \frac{|(P-P') \cdot (v \wedge v')|}{\|v \wedge v'\|}$

(interpretazione geometrica: il numeratore è il volume di un parallelepipedo di cui il denominatore è l'area di base); mentre se sono parallele: $d(r, r') = \frac{\|(P-P') \wedge v\|}{\|v\|}$

(interpretazione geometrica: il numeratore è area di un parallelogramma di cui il denominatore è la misura della base).

distanza punto-retta: sia $r=P+\langle v \rangle$, allora $d(P_0, r) = \frac{\|(P-P') \wedge v\|}{\|v\|}$;

se abbiamo $r=\pi\cap\pi'$, allora

$$d(P_0, r) = \left\| \frac{|ax_0+by_0+cz_0|}{a^2+b^2+c^2} (a, b, c)^t + \frac{|a'x_0+b'y_0+c'z_0|}{a'^2+b'^2+c'^2} (a', b', c')^t \right\|$$

e si scrive anche

$$d(P_0, r) = \sqrt{d(P_0, \pi)^2 + d(P_0, \pi')^2 + d(P_0, \pi)d(P_0, \pi') \cos\vartheta(\pi, \pi')}$$

asse di un segmento: si tratta del piano dei punti equidistanti dai due punti dati P_0 e P_1 ; si scrive $(\frac{1}{2}P_0 + \frac{1}{2}P_1) + (P_1 - P_0)^\perp$, oppure tramite l'equazione:

$$(x_1-x_0)\left(X-\frac{x_0+x_1}{2}\right) + (y_1-y_0)\left(Y-\frac{y_0+y_1}{2}\right) + (z_1-z_0)\left(Z-\frac{z_0+z_1}{2}\right) = 0.$$

bisettrici di due piani incidenti: se abbiamo equazioni cartesiane $a_0X+b_0Y+c_0Z+d_0=0$ e $a_1X+b_1Y+c_1Z+d_1=0$ con $a_0^2+b_0^2+c_0^2=a_1^2+b_1^2+c_1^2$ allora i piani bisettori hanno equazioni $(a_0X+b_0Y+c_0Z+d_0)\pm(a_1X+b_1Y+c_1Z+d_1)=0$.

area di triangoli: $A(P_0, P_1, P_2) = \frac{1}{2} \|(P_1-P_0) \wedge (P_2-P_0)\|$, e si esplicita come

$$\frac{1}{2} \sqrt{\left| \begin{array}{ccc} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{array} \right|^2 + \left| \begin{array}{ccc} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ z_0 & z_1 & z_2 \end{array} \right|^2 + \left| \begin{array}{ccc} 1 & 1 & 1 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{array} \right|^2}.$$

volume di tetraedri:

$$V(P_0, P_1, P_2, P_3) = \frac{1}{6} \left| \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ z_0 & z_1 & z_2 & z_3 \end{pmatrix} \right|.$$

Classificazione delle rigidità spaziali:

Rotazioni (di asse una retta): sono le rigidità dirette con (una retta di) punti uniti;

Traslazioni: sono rigidità dirette senza punti uniti;

Roto-traslazioni o Glissorotazioni: sono rigidità dirette senza punti uniti, composizioni di una rotazione di asse una retta e di una traslazione parallela all'asse;

Riflessioni: sono le rigidità inverse con (un piano di) punti uniti;

Roto-riflessioni: sono le rigidità inverse con un punto unito: composizione di una riflessione e di una rotazione di asse ortogonale al piano di riflessione;

Glissoriflessioni: sono le rigidità inverse prive di punti uniti: composizione di una riflessione e di una traslazione di direzione parallela al piano di riflessione.

Copyright © 2004 M. Cailotto, March 2004 v03.04

Dip. di Matematica Pura ed Applicata, Univ. Padova (Italy)

Thanks to TeX, a trademark of the American Mathematical Society, and DEK.

Stampa e distribuzione di questo Formulario sono consentiti per scopi didattici e scientifici, escluso qualsiasi scopo di lucro, e purché questa nota di copyright sia presente in ogni copia.