

0.1 Spazi Euclidei in generale

Sia V uno spazio vettoriale definito su $\mathbb{R}$. Diremo, estendendo una definizione data in precedenza, che V è uno spazio vettoriale *euclideo* se è definita una applicazione

$$V \times V \rightarrow \mathbb{R}$$

che ad ogni coppia di vettori $(\mathbf{u}, \mathbf{v})$ di V associa uno scalare, indicato con $(\mathbf{u}|\mathbf{v})$, che soddisfi le seguenti proprietà:

- (1) $(\alpha\mathbf{u}|\mathbf{v}) = (\mathbf{u}|\alpha\mathbf{v}) = \alpha(\mathbf{u}|\mathbf{v})$ per ogni $\mathbf{u}, \mathbf{v} \in V, \alpha \in \mathbb{R}$;
- (2) $(\mathbf{w}|\mathbf{u} + \mathbf{v}) = (\mathbf{w}|\mathbf{u}) + (\mathbf{w}|\mathbf{v})$ per ogni $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$;
- (3) $(\mathbf{u}|\mathbf{v}) = (\mathbf{v}|\mathbf{u})$ per ogni $\mathbf{u}, \mathbf{v} \in V$;
- (4) $(\mathbf{u}|\mathbf{v}) = 0$ per ogni $\mathbf{v} \in V$ implica $\mathbf{u} = \mathbf{0}$.

Una applicazione che soddisfi:

le proprietà (1) e (2), si dice *forma bilineare*,

le proprietà (1), (2) e (3), si dice *forma bilineare simmetrica*,

le proprietà (1), (2), (3) e (4), si dice *forma bilineare simmetrica non degenera*.

Se invece della (4) si richiede la proprietà:

$$(4') \quad (\mathbf{u}|\mathbf{u}) \geq 0 \quad \forall \mathbf{u} \in V \text{ e } (\mathbf{u}|\mathbf{u}) = 0 \implies \mathbf{u} = \mathbf{0},$$

allora si dice che la forma bilineare simmetrica è *definita positiva*.

Esercizio 0.1.1. Verificare che (4') implica (4) ma non viceversa.

Una forma bilineare simmetrica definita positiva si dice *prodotto scalare* e lo spazio euclideo si dice allora *proprio*.

Esempi 0.1.2. Abbiamo:

- I) $\mathbb{R}^n$ con il prodotto scalare canonico è uno spazio euclideo. In tal caso il prodotto scalare $(\mathbf{u}|\mathbf{v})$ è anche indicato con $\mathbf{u} \cdot \mathbf{v}$.
- II) Lo spazio vettoriale $C^0([a, b])$ delle funzioni continue sull'intervallo reale $[a, b]$ è uno spazio euclideo rispetto al prodotto scalare $(f|g) = \int_a^b f(t)g(t) dt$.
- III) Lo spazio vettoriale $M_n(\mathbb{R})$ con il prodotto scalare definito da $(A|B) = \text{Tr}(AB^T)$ è uno spazio euclideo.

Se V ha dimensione finita n e se $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ è una base di V , siano $\mathbf{u} = \sum_i a_i \mathbf{v}_i$ e $\mathbf{v} = \sum_j b_j \mathbf{v}_j$. Per le proprietà (1) e (2), avremo

$$(\mathbf{u}|\mathbf{v}) = \sum_{i,j} a_i b_j (\mathbf{v}_i, \mathbf{v}_j).$$

che mostra come il prodotto scalare di due vettori sia determinato una volta che siano assegnati i prodotti scalari dei vettori di una base. Se allora poniamo $g_{ij} = (\mathbf{v}_i, \mathbf{v}_j)$ potremo scrivere

$$(\mathbf{u}|\mathbf{v}) = \sum_{i,j} a_i b_j g_{ij}.$$

La (4) nella definizione di prodotto scalare si traduce allora come segue: il sussistere dell'eguaglianza $\sum_{i,j} a_i b_j g_{ij} = 0$ per ogni scelta delle b_j , $j = 1, \dots, n$, implica che

$$a_i = 0, \quad i = 1, \dots, n.$$

In particolare, ciò significa che per ogni $j = 1, \dots, n$:

$$(\mathbf{u}|\mathbf{v}_j) = \sum_i a_i g_{ij} = 0.$$

Questo equivale a dire che il sistema lineare omogeneo

$$\sum_i a_i g_{ij} = 0 \quad (j = 1, \dots, n)$$

ammette solo la soluzione banale e sappiamo che ciò equivale alla condizione $\det(g_{ij}) \neq 0$. La matrice g_{ij} è detta *matrice della forma* rispetto alla base $\mathcal{B}$.

Diremo che due vettori sono *ortogonali* se il loro prodotto scalare è zero.

Il prodotto scalare usuale su $\mathbb{R}^n$ è effettivamente una forma bilineare simmetrica definita positiva. Nel caso di uno spazio euclideo proprio, diremo *norma* del vettore $\mathbf{v}$ lo scalare $\|\mathbf{v}\| = \sqrt{(\mathbf{v}|\mathbf{v})}$. Questa norma induce su $\mathbb{R}^n$ una nozione di distanza o lunghezza. Chiameremo *unitario* (oppure *versore*) un vettore di norma 1.

Un insieme di vettori di V di norma 1 e a due a due ortogonali si chiama *sistema ortonormale di vettori*. Un tale sistema $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ è caratterizzato dalle condizioni

$$(\mathbf{v}_i|\mathbf{v}_j) = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

In modo del tutto analogo al caso di $\mathbb{R}^n$ si dimostra la seguente:

Proposizione 0.1.3. *I vettori di un sistema ortonormale sono linearmente indipendenti.*

Se dunque la dimensione di V è n ed il sistema ortonormale ha n vettori parleremo di *base ortonormale*. Richiamiamo il procedimento di Gram-Schmidt, che riannunciamo nel nuovo contesto più generale.

Teorema 0.1.4. (Procedimento di Gram-Schmidt) *Dato un qualunque insieme di r vettori linearmente indipendenti $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ è possibile costruire un sistema ortonormale di r vettori che generano lo stesso sottospazio U generato da $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$.*

Precisamente:

$$\begin{aligned}\mathbf{u}_1 &= \mathbf{v}_1, \\ \mathbf{u}_2 &= \mathbf{v}_2 - \frac{(\mathbf{v}_2|\mathbf{u}_1)}{(\mathbf{u}_1|\mathbf{u}_1)}\mathbf{u}_1, \\ \mathbf{u}_3 &= \mathbf{v}_3 - \frac{(\mathbf{v}_3|\mathbf{u}_2)}{(\mathbf{u}_2|\mathbf{u}_2)}\mathbf{u}_2 - \frac{(\mathbf{v}_3|\mathbf{u}_1)}{(\mathbf{u}_1|\mathbf{u}_1)}\mathbf{u}_1,\end{aligned}$$

in generale,

$$\mathbf{u}_r = \mathbf{v}_r - \frac{(\mathbf{v}_r|\mathbf{u}_{r-1})}{(\mathbf{u}_{r-1}|\mathbf{u}_{r-1})}\mathbf{u}_{r-1} - \cdots - \frac{(\mathbf{v}_r|\mathbf{u}_1)}{(\mathbf{u}_1|\mathbf{u}_1)}\mathbf{u}_1.$$

Dividendo ciascuno dei vettori $\mathbf{u}_i$ per il suo modulo otteniamo un sistema ortonormale di vettori.

Esempio 0.1.5. Sia $\mathbb{P}_2$ l'insieme dei polinomi nell'indeterminata t di grado minore o uguale a 2, con prodotto scalare

$$(p(t)|q(t)) = \int_{-1}^1 p(t)q(t) dt.$$

Determinare una base ortonormale a partire da $\{1, t, t^2\}$.

$$\begin{aligned}u_1(t) &= 1, & u_2(t) &= t - \frac{t \cdot 1}{1 \cdot 1}1 = t - \frac{\int_{-1}^1 t dt}{\int_{-1}^1 dt} = t, \\ u_3(t) &= t^2 - \frac{\int_{-1}^1 t^3 dt}{\int_{-1}^1 t^2 dt} - \frac{\int_{-1}^1 t^2 dt}{\int_{-1}^1 dt} = t^2 - \frac{1}{3}.\end{aligned}$$

Questi, a meno di un fattore moltiplicativo costante, sono i primi tre dei cosiddetti *polinomi di Legendre*. Si possono ottenere in maniera analoga polinomi di Legendre di grado arbitrariamente alto. Essi sono un esempio di successione di polinomi ortogonali, una classe importantissima di polinomi che comprende, ad esempio, la fondamentale successione dei polinomi di Chebyshev.

Esercizio 0.1.6. Consideriamo l'insieme T di tutte le funzioni del tipo

$$\frac{a_0}{2} + a_1 \cos t + b_1 \sin t + a_2 \cos 2t + b_2 \sin 2t + \cdots + a_n \cos nt + b_n \sin nt$$

con n intero fissato, $a_i, b_i \in \mathbb{R}$ e $-\pi \leq t \leq \pi$. T è un sottospazio vettoriale di dimensione $2n+1$ dello spazio vettoriale $C(-\pi, \pi)$ di tutte le funzioni continue definite nell'intervallo $-\pi \leq t \leq \pi$. Su T si può definire il prodotto scalare:

$$(a_1(t)|a_2(t)) = \int_{-\pi}^{\pi} a_1(t)a_2(t) dt.$$

Verificare che l'insieme

$$\{1, \cos t, \sin t, \cos 2t, \sin 2t, \dots, \cos nt, \sin nt\}$$

è una base ortogonale di T . (Suggerimento: occorre ricordarsi delle formule del tipo

$$\int \sin kt \sin ht dt = \frac{\sin(k-h)t}{2(h-k)} - \frac{\sin(k+h)t}{2(h+k)} + c). \text{ Trovare una base ortonormale.}$$

Data una funzione $f \in C(-\pi, \pi)$ con il prodotto scalare appena descritto, supponiamo che $\{\phi_1, \dots, \phi_{2n+1}\}$ sia la base ortonormale trovata sopra. Se $f \notin T$, possiamo comunque cercare di determinare l'elemento $g \in T$ che abbia distanza minima da f . La soluzione del nostro problema è data dallo sviluppo di Fourier :

$$g = \sum_{h=1}^{2n+1} (f, \phi_h) \phi_h.$$

Questa è l'approssimazione di una funzione continua mediante polinomi trigonometrici ortonormali. La funzione g coincide con la proiezione ortogonale di f sul sottospazio T . La parte di matematica che tratta questo tipo di questioni si chiama Analisi Armonica.

Esempio 0.1.7. Un altro esempio nello spazio $\mathbb{P}_n$, molto importante, si ottiene scegliendo $n + 1$ numeri reali distinti $\{x_0, x_1, \dots, x_n\}$ e definendo

$$(p(x)|q(x)) = p(x_0)q(x_0) + \dots + p(x_n)q(x_n) \quad (1)$$

È facile verificare le proprietà della definizione di prodotto scalare. L'unico punto delicato della verifica riguarda la proprietà della positività. In quella verifica, infatti, occorre verificare che $(p(x)|p(x)) = p(x_0)^2 + \dots + p(x_n)^2 \geq 0$, il che è evidente, ma occorre specificare che se si suppone che $(p(x)|p(x)) = 0$ ne deve seguire che $p(x)$ è il polinomio nullo. È in questa verifica che si vede l'importanza di scegliere proprio $n + 1$ numeri reali distinti. Abbiamo infatti che se $(p(x)|p(x)) = 0$ si ha

$$p(x_0)^2 + \dots + p(x_n)^2 = 0$$

da cui certamente segue che $p(x_0) = \dots = p(x_n) = 0$. Il polinomio $p(x)$ si annulla quindi in questi punti, ma perché deve essere proprio il polinomio nullo? La risposta è che essendo $p(x)$ un polinomio di grado $\leq n$ esso non può avere $n + 1$ radici, a meno che esso non sia proprio il polinomio nullo. Per maggior concretezza, prendiamo $n = 4$ e definiamo dei particolari polinomi, detti *polinomi di Lagrange*,

$$\begin{aligned} \delta_0(x) &= \frac{(x - x_1)(x - x_2)(x - x_3)(x - x_4)}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)(x_0 - x_4)} \\ \delta_1(x) &= \frac{(x - x_0)(x - x_2)(x - x_3)(x - x_4)}{(x_1 - x_0)(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)} \\ \delta_2(x) &= \frac{(x - x_0)(x - x_1)(x - x_3)(x - x_4)}{(x_2 - x_0)(x_2 - x_1)(x_2 - x_3)(x_2 - x_4)} \\ \delta_3(x) &= \frac{(x - x_0)(x - x_1)(x - x_2)(x - x_4)}{(x_3 - x_0)(x_3 - x_1)(x_3 - x_2)(x_3 - x_4)} \\ \delta_4(x) &= \frac{(x - x_0)(x - x_1)(x - x_2)(x - x_3)}{(x_4 - x_0)(x_4 - x_1)(x_4 - x_2)(x_4 - x_3)} \end{aligned}$$

Come si può osservare facilmente, in ciascuna delle espressioni abbiamo al numeratore un polinomio di grado 4 e al denominatore un numero reale non nullo, in quanto i

valori scelti sono tutti distinti. Inoltre, $\delta_0(x_0) = 1$, $\delta_1(x_1) = 1$, $\delta_2(x_2) = 1$, $\delta_3(x_3) = 1$, $\delta_4(x_4) = 1$ mentre $\delta_i(x_j) = 0$ se $i \neq j$. Dalla definizione 1 di prodotto scalare si verifica facilmente che i cinque polinomi di Lagrange costituiscono una base ortonormale di P_4 . Lo sviluppo di Fourier di un polinomio in $f(x) \in \mathbb{P}_n$ rispetto a questa base ortonormale è allora

$$\begin{aligned} f(x) &= (f(x)|\delta_0(x))\delta_0(x) + (f(x)|\delta_1(x))\delta_1(x) + (f(x)|\delta_2(x))\delta_2(x) \\ &\quad + (f(x)|\delta_3(x))\delta_3(x) + (f(x)|\delta_4(x))\delta_4(x) \\ &= f(x_0)\delta_0(x) + f(x_1)\delta_1(x) + f(x_2)\delta_2(x) \\ &\quad + f(x_3)\delta_3(x) + f(x_4)\delta_4(x) \end{aligned}$$

Ovviamente scelte analoghe sono possibili per un qualunque intero $n > 0$

Esempio 0.1.8. Possiamo sfruttare i polinomi di Lagrange per ottenere un metodo per condividere segreti in maniera sicura. Supponiamo che un numeroso gruppo di scienziati sia al lavoro su un progetto segretissimo. I documenti del progetto vengono tenuti al sicuro in una cassaforte dove la combinazione segreta è sconosciuta a ciascun membro del gruppo. Vogliamo però che la cassaforte possa essere aperta se almeno sei membri del gruppo di ricerca sono presenti ma che la combinazione rimanga segreta se ci sono meno di 6 membri presenti.

Supponiamo che la combinazione sia un numero che chiamiamo a_0 . Costruiamo un polinomio $p(x)$ di grado 5 che abbia termine noto uguale ad a_0 , e dei numeri arbitrari (fissati) per i restanti coefficienti

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

Distribuiamo a ciascuno dei membri del gruppo di ricerca un valore $p(x_i)$ (con $x_i \neq 0$). Non appena 6 membri si riuniscono essi possono calcolare i polinomi di Lagrange relativi ai punti $\{x_{i_0}, x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}, x_{i_5}\}$ e ottenere

$$\begin{aligned} p(x) &= p(x_{i_0})\delta_0(x) + p(x_{i_1})\delta_1(x) + p(x_{i_2})\delta_2(x) \\ &\quad + p(x_{i_3})\delta_3(x) + p(x_{i_4})\delta_4(x) + p(x_{i_5})\delta_5(x) \end{aligned} \quad (2)$$

Dopodiché non devono far altro che leggere il termine noto del polinomio così determinato. Osserviamo che se si cambiano i 6 valori fissati, occorre ricalcolare anche i polinomi di Lagrange, perché anch'essi dipendono dalla scelta fatta dei valori.

Esempio 0.1.9. Determinare il polinomio di quinto grado sapendo che i punti $(-8, -53635)$, $(-5, 794)$, $(-1, 7678)$, $(3, 8130)$, $(4, 8453)$, $(7, 13670)$ sono sul grafico del polinomio. Occorre per prima cosa definire i polinomi di Lagrange relativi ai valori $(x_0, x_1, x_2, x_3, x_4, x_5) = (-8, -5, -1, 3, 4, 7)$ e calcolare

$$\begin{aligned} &-53635\delta_0(x) + 794\delta_1(x) + 7678\delta_2(x) \\ &+ 8130\delta_3(x) + 8453\delta_4(x) + 13670\delta_5(x) \end{aligned} \quad (3)$$

si ottiene $7629 + 2x + 67x^2 + 8x^3 - 7x^4 + x^5$.

Osservazione 0.1.10. Col procedimento appena descritto è possibile ottenere un polinomio che passi per dei punti assegnati qualsiasi. Questi punti potrebbero essere ad esempio dei punti sul grafico di una funzione $f(x)$ che non sia necessariamente una funzione polinomiale. Il polinomio così ottenuto si dice *polinomio interpolatore di Lagrange* per la funzione f .

Esempio 0.1.11. Scrivere il polinomio $p(x) = 1 + x + x^2 \in \mathbb{P}_2$ in termini dei polinomi di Lagrange relativi alla scelta $x_0 = 1, x_1 = 2, x_2 = 0$ e poi di nuovo rispetto alla scelta $x_0 = -1, x_1 = 3, x_2 = 1$. In ambo i casi devo scrivere

$$p(x) = p(x_0)\delta_0(x) + p(x_1)\delta_1(x) + p(x_2)\delta_2(x)$$

Cambiando le scelte cambiano anche i polinomi δ_i .

Con la prima scelta abbiamo:

$$\delta_0(x) = \frac{(x-2)(x-0)}{(1-2)(1-0)} = 2x - x^2$$

$$\delta_1(x) = \frac{(x-1)(x-0)}{(2-1)(2-0)} = \frac{x^2 - x}{2}$$

$$\delta_2(x) = \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{x^2 - 3x + 2}{2}$$

e $p(1) = 3, p(2) = 7, p(0) = 1$ e quindi

$$1 + x + x^2 = 3(2x - x^2) + 7\left(\frac{x^2 - x}{2}\right) + \frac{x^2 - 3x + 2}{2}$$

Con la seconda scelta abbiamo:

$$\delta_0(x) = \frac{(x-3)(x-1)}{(-1-3)(-1-1)} = \frac{x^2 - 4x + 3}{8}$$

$$\delta_1(x) = \frac{(x+1)(x-1)}{(3+1)(3-1)} = \frac{x^2 - 1}{8}$$

$$\delta_2(x) = \frac{(x+1)(x-3)}{(1+1)(1-3)} = \frac{-x^2 + 2x + 3}{4}$$

e $p(-1) = 1, p(3) = 13, p(1) = 3$ e quindi

$$1 + x + x^2 = \frac{x^2 - 4x + 3}{8} + 13\left(\frac{x^2 - 1}{8}\right) + 3\left(\frac{-x^2 + 2x + 3}{4}\right)$$

Infine, all'interno dello stesso spazio vettoriale $V = \mathbb{R}^n$, possiamo ottenere numerosi esempi di prodotti scalari non standard considerando una qualunque matrice reale simmetrica definita positiva A di ordine n e definendo

$$(\mathbf{x}|\mathbf{y}) = \mathbf{x}^T A \mathbf{y}$$

per $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

Osserviamo che il prodotto scalare canonico su $\mathbb{R}^n$, cioè

$$(\mathbf{x}|\mathbf{y}) = x_1 y_1 + \cdots + x_n y_n$$

corrisponde alla matrice identità.

Con una dimostrazione del tutto analoga a quella data nel caso del prodotto scalare canonico si può vedere che vale:

Teorema 0.1.12. (Disuguaglianza di Schwarz) *Assegnati due vettori $\mathbf{u}, \mathbf{v}$ nello spazio euclideo V , sussiste la seguente disuguaglianza:*

$$|(\mathbf{u}|\mathbf{v})| \leq \|\mathbf{u}\| \|\mathbf{v}\|$$

ove il segno di uguaglianza vale se e solo se i due vettori sono proporzionali.