Capitolo 4

Spazi vettoriali a coefficienti in un campo

4.1 Introduzione

Nel capitolo 2 abbiamo visto come i risultati su sistemi lineari e matrici valgano anche se i coefficienti considerati, anziché appartenere a $\mathbb{R}$ appartengono a un campo qualsiasi $\mathbb{K}$. Per far ciò avevamo notato come le proprietà che abbiamo utilizzato per studiare i sistemi lineari a coefficienti reali fossero unicamente le proprietà di campo di $\mathbb{R}$.

In questo capitolo in maniera analoga estendiamo la definizione e i risultati sugli spazi vettoriali al caso in cui gli scalari siano elementi di un campo qualsiasi $\mathbb{K}$.

4.2 Spazi vettoriali su un campo qualsiasi

Definizione 4.1 Sia $\mathbb{K}$ un campo fissato. Sia dato un insieme non vuoto V, i cui elementi vengono chiamati **vettori**. Chiameremo invece **scalari** gli elementi di $\mathbb{K}$. In V sia definita un'**operazione binaria interna**, cioè una legge che ad ogni coppia $(\mathbf{v}, \mathbf{w})$ di vettori di V associ un vettore di V che indichiamo con il simbolo $\mathbf{v} + \mathbf{w}$. Tale operazione viene chiamata **addizione** in V e il vettore $\mathbf{v}+\mathbf{w}$ viene detto **somma** dei vettori $\mathbf{v}$ e $\mathbf{w}$. Sia inoltre definita un'**operazione binaria esterna**, cioè una legge che ad ogni coppia $(k, \mathbf{v})$ formata da uno scalare k e da un vettori $\mathbf{v}$ di V associ un vettore di V che indichiamo con il simbolo $k\mathbf{v}$. Tale operazione viene chiamata **moltiplicazione per uno scalare** e il vettore $k\mathbf{v}$ viene detto **prodotto** dello scalare k per il vettore $\mathbf{v}$.
L'insieme V dotato delle operazioni di addizione e di moltiplicazione di un vettore per uno scalare viene detto **spazio vettoriale** su $\mathbb{K}$ se sono verificate le proprietà:

1. $(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$ per ogni $\mathbf{u}\in V$, $\mathbf{v}\in V$, $\mathbf{w}\in V$.
2. $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$ per ogni $\mathbf{u}\in V$, $\mathbf{v}\in V$.
3. Esiste un vettore $\mathbf{e}$ tale che $\mathbf{u}+\mathbf{e}=\mathbf{u}$ per ogni $\mathbf{u}\in V$.

   Si può dimostrare (vedi oltre) che un tale vettore $\mathbf{e}$ è unico. Indichiamo questo vettore con il simbolo $\mathbf{0}$ e lo chiamiamo **vettore nullo**.

   Scriveremo allora $\mathbf{u}+\mathbf{0}=\mathbf{u}$ per ogni $\mathbf{u}\in V$.
4. Per ogni vettore $\mathbf{u}$ esiste un vettore $\mathbf{v}$ tale che $\mathbf{u}+\mathbf{v}=\mathbf{0}$.

   Si può dimostrare (vedi oltre) che un tale vettore $\mathbf{v}$ è unico. Indichiamo questo vettore con il simbolo $-\mathbf{u}$ e lo chiamiamo **vettore opposto** del vettore $\mathbf{v}$.

   Scriveremo allora $\mathbf{u}+(-\mathbf{u})=\mathbf{0}$.
5. $1\mathbf{u}=\mathbf{u}$ per ogni $\mathbf{u}\in V$.
6. $h\,(k\,(\mathbf{u}))=(hk)\,\mathbf{u}$ per ogni $\mathbf{u}\in V$, $h\in\mathbb{K}$, $k\in\mathbb{K}$.
7. $(h+k)\,\mathbf{u}=h\mathbf{u}+k\mathbf{u}$ per ogni $\mathbf{u}\in V$, $h\in\mathbb{K}$, $k\in\mathbb{K}$.
8. $h\,(\mathbf{u}+\mathbf{v})=h\mathbf{u}+h\mathbf{v}$ per ogni $\mathbf{u}\in V$, $\mathbf{v}\in V$, $h\in\mathbb{K}$. $\triangle$

Esercizio di base EB.4.1 Dimostrare l'unicità del vettore nullo. $\triangle$

Esercizio di base EB.4.2 Dimostrare l'unicità del vettore opposto. $\triangle$

Estendiamo al caso di spazi vettoriali su un campo qualsiasi alcune definizioni e proprietà che abbiamo introdotto nel caso degli spazi vettoriali sul campo dei numeri reali.

Proposizione 4.2 *Dato uno spazio vettoriale V su un campo K si ha:*
1) $a\mathbf{0}=\mathbf{0}$ *per ogni* $a\in\mathbb{K}$
2) $0\mathbf{v}=\mathbf{0}$ *per ogni* $\mathbf{v}\in V$
3) $(-a)\mathbf{v}=-a\mathbf{v}$ *per ogni* $a\in\mathbb{K}$*, per ogni* $\mathbf{v}\in V$
4) Se $\mathbf{v}\neq\mathbf{0}$ *e se* $a\mathbf{v}=\mathbf{0}$*, allora* $a=0$

DIMOSTRAZIONE Lasciata per esercizio. ∎

Esercizio di base EB.4.3 Dimostrare la proposizione precedente $\triangle$

Definizione 4.3 Siano $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ dei vettori di uno spazio vettoriale V e siano k_1, k_2, ..., k_r degli scalari, cioè elementi del campo $\mathbb{K}$. Chiamiamo **combinazione lineare** dei vettori $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ a coefficienti k_1, k_2, ..., k_r il vettore

$$k_1\mathbf{v}_1+k_2\mathbf{v}_2+\cdots+k_r\mathbf{v}_r.$$ $\triangle$

Definizione 4.4 Diciamo che i vettori $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ sono **linearmente dipendenti** se esistono k_1, k_2, ..., k_r elementi del campo $\mathbb{K}$ non tutti nulli tali che:

$$k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \cdots + k_r\mathbf{v}_r = \mathbf{0}.$$

Detto in altri termini, i vettori $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ sono linearmente dipendenti se il vettore nullo può essere espresso come combinazione lineare di $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ oltre che nel modo banale (cioè quello in cui tutti i coefficienti sono nulli) anche in qualche altro modo. △

Definizione 4.5 Indichiamo con il simbolo $\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r \rangle$ l'insieme delle combinazioni lineari dei vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r$. Cioè:

$$\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r \rangle := \{k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \cdots + k_r\mathbf{v}_r \mid k_1 \in \mathbb{R},\, k_2 \in \mathbb{R}, \dots, k_r \in \mathbb{R}\}.$$

Se $V = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r \rangle$ diciamo che V è **uno spazio vettoriale generato** dai vettori $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$. Questi ultimi vettori vengono detti **generatori** di V. △

Definizione 4.6 Diciamo che i vettori $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ di uno spazio V costituiscono una **base** di V se sono verificate entrambe le proprietà

- $V = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r \rangle$;
- $\mathbf{v}_1$, $\mathbf{v}_2$,..., $\mathbf{v}_r$ sono linearmente indipendenti. △

Teorema 4.7 *Un insieme finito di vettori di uno spazio vettoriale V è una base se e solo se ogni vettore $\mathbf{v}$ di V si può esprimere in uno ed in un sol modo come combinazione lineare di tali vettori.*

DIMOSTRAZIONE Lasciata per esercizio. ■

Esercizio di base EB.4.4 Dimostrare il teorema precedente. △

Definizione 4.8 Data una base $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ di uno spazio vettoriale V su un campo K, abbiamo visto che ogni vettore $\mathbf{v}$ di V si scrive in un sol modo come combinazione lineare di $\mathbf{v}_1, \dots, \mathbf{v}_n$. I coefficienti di tale combinazione lineare si dicono **coordinate** del vettore $\mathbf{v}$ relative alla base data. △

4.3 Esempi di spazi vettoriali

Diamo ora alcuni esempi di spazi vettoriali su un campo $\mathbb{K}$.

1. Si consideri un piano π ed un suo punto O. Chiamiamo **vettore** di π applicato in O la coppia (O, P) dove P è un punto di π. Indichiamo con $V^2(\pi, O)$ l'insieme dei vettori di π applicati in O. Introducendo l'usuale definizione di addizione tra due vettori per mezzo della regola del parallelogramma e l'usuale moltiplicazione di un vettore per uno scalare, otteniamo uno spazio vettoriale sul campo $\mathbb{R}$ dei numeri reali.
   Due qualsiasi vettori di π non nulli applicati in O che non siano allineati formano una base di $V^2(\pi, O)$.

2. Analogamente l'insieme $V^3(O)$ dei vettori dello spazio applicati in un suo punto O, con le usuali operazioni di addizione tra vettori e di moltiplicazione di un vettore per uno scalare, è uno spazio vettoriale su $\mathbb{R}$. Una sua base è data da tre vettori applicati in O che non siano complanari.

3. L'insieme $\mathbb{R}$, con le usuali operazioni di addizione e di moltiplicazione, è uno spazio vettoriale su $\mathbb{R}$ stesso. Una sua base è data dal numero 1. Tale base viene detta **base canonica** di $\mathbb{R}$ su $\mathbb{R}$.
Un qualsiasi numero reale non nullo forma una base di $\mathbb{R}$.

4. L'insieme $\mathbb{R}^2$ delle coppie di numeri reali, con le usuali operazioni di addizione di coppie e di moltiplicazione di una coppia per un numero reale, è uno spazio vettoriale su $\mathbb{R}$. La coppia di vettori $\mathbf{e}_1 = (1,0),\ \mathbf{e}_2 = (0,1)$ forma una base di $\mathbb{R}^2$ sul campo $\mathbb{R}$, detta **base canonica** di $\mathbb{R}^2$.

5. L'insieme $\mathbb{R}^n$ delle n-ple di numeri reali, con le usuali operazioni di addizione di n-ple e di moltiplicazione di una n-pla per un numero reale, è uno spazio vettoriale su $\mathbb{R}$. Gli n vettori
$$\mathbf{e}_1 = (1,0,\ldots,0),\ \mathbf{e}_2 = (0,1,\ldots,0),\ \ldots,\ \mathbf{e}_n = (0,0,\ldots,1)$$
formano una base di $\mathbb{R}^n$ su $\mathbb{R}$, detta **base canonica** di $\mathbb{R}^n$.

6. Notiamo che, nel dimostrare che $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^n$ sono spazi vettoriali su $\mathbb{R}$, sfruttiamo solamente il fatto che $\mathbb{R}$ è un campo. Quindi, dato un campo $\mathbb{K}$, possiamo dimostrare in modo analogo che $\mathbb{K}, \mathbb{K}^2, \mathbb{K}^n$ sono spazi vettoriali su $\mathbb{K}$.
Anche in questo caso si hanno le basi canoniche. Il vettore 1, elemento neutro rispetto alla moltiplicazione di $\mathbb{K}$, è la **base canonica** dello spazio vettoriale $\mathbb{K}$ sul campo $\mathbb{K}$ stesso. I vettori $(1,0),(0,1)$ formano la **base canonica** di $\mathbb{K}^2$ su $\mathbb{K}$. Analogamente si ha la **base canonica** di $\mathbb{K}^n$ su $\mathbb{K}$.

7. Dato l'insieme $M(\mathbb{R},p,q)$ delle matrici ad elementi reali a p righe e q colonne, si consideri in esso l'operazione di addizione tra matrici e l'operazione di moltiplicazione di una matrice per un numero reale. Si ha uno spazio vettoriale sui reali. Sia $A(i,j)$ la matrice avente tutti gli elementi uguali a 0, fuorchè l'elemento della i-sima riga e j-sima colonna che è uguale a 1. L'insieme delle $p \cdot q$ matrici $A(i,j)$ è una base di $M(\mathbb{R},p,q)$. Essa viene detta **base canonica**.

8. Tutto ciò si generalizza al caso di matrici ad elementi in un campo $\mathbb{K}$ qualsiasi. Si ha che $M(\mathbb{K},p,q)$ è uno spazio vettoriale su $\mathbb{K}$. La base data dalle matrici $A(i,j)$ viene detta anche in questo caso **base canonica**.

9. Consideriamo l'insieme $\mathbb{C}$ dei numeri complessi. Esso è, con le usuali operazioni, uno spazio vettoriale su $\mathbb{C}$ stesso (esempio 6). La sua **base canonica** è data dal numero 1. Vogliamo considerare ora $\mathbb{C}$ come spazio vettoriale su R. A tale scopo consideriamo l'usuale addizione tra numeri complessi e la moltiplicazione di un numero complesso per un numero

reale. Si ottiene uno spazio vettoriale. Una sua base è data da $\{1, i\}$. Essa è detta **base canonica** dello spazio vettoriale $\mathbb{C}$ sul campo $\mathbb{R}$ dei reali. Notiamo che, se consideriamo $\mathbb{C}$ come spazio vettoriale su C, i vettori 1 e i non sono linearmente indipendenti. Si ha infatti $i \cdot 1 + (-1) \cdot i = 0$. Abbiamo quindi una loro combinazione lineare a coefficienti non nulli che è uguale al vettore nullo.

10. Sia dato l'insieme $\mathbb{C}^2$ delle coppie di numeri complessi. Abbiamo visto che, se in esso si considerano le usuali operazioni di addizione tra coppie e di moltiplicazione di una coppia per un numero complesso, otteniamo uno spazio vettoriale su $\mathbb{C}$ (esempio 6). La sua **base canonica** è data da $\{(1,0)\ ,\ (0,1)\}$.

11. Consideriamo ora, in analogia al caso precedente, le operazioni di addizione tra coppie di numeri complessi e di moltiplicazione di una coppia di numeri complessi per un numero reale. Abbiamo così uno spazio vettoriale su $\mathbb{R}$.
    I vettori $\{(1,0)\ ,\ (i,0)\ ,\ (0,1)\ ,\ (0,i)\}$ formano una base, detta **base canonica** dello spazio vettoriale $\mathbb{C}^2$ sul campo dei reali.

12. In modo analogo, per ogni intero $n > 0$, possiamo definire lo spazio vettoriale $\mathbb{C}^n$ sul campo dei reali. Esso è dotato della **base canonica** formata da $2n$ vettori. Essi sono dati dalle n-ple di numeri complessi, aventi tutti gli elementi nulli fuorchè uno che è uguale a 1 o a i. Lo spazio vettoriale $\mathbb{C}^n$ sul campo R ha quindi una base formata da $2n$ vettori.

13. Si consideri l'insieme $\mathbb{R}^n[x]$ dei polinomi di grado minore di n a coefficienti in $\mathbb{R}$ in una variabile x. Consideriamo in esso l'usuale addizione tra polinomi e l'usuale moltiplicazione di un polinomio per un numero reale. Dati cioè i polinomi:

    $$p(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

    $$q(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$$

    e un numero reale k, si pone:

    $$p(x) + q(x) = a_0 + b_0 + (a_1 + b_1)x + \cdots + (a_{n-1} + b_{n-1})x^{n-1}$$

    $$kp(x) = ka_0 + ka_1 x + \cdots + ka_{n-1} x^{n-1}.$$

    Si verifica facilmente che $\mathbb{R}^n[x]$ è uno spazio vettoriale su $\mathbb{R}$. Una sua base è data dai vettori:

    $$\mathbf{e}_0 = 1\ ,\ \mathbf{e}_1 = x\ ,\ \ldots\ ,\ \mathbf{e}_{n-1} = x^{n-1}$$

    Questa base viene detta **base canonica** di $\mathbb{R}^n[x]$ su $\mathbb{R}$.

14. Anche in questo caso notiamo che, per dimostrare che $\mathbb{R}^n[x]$ è uno spazio vettoriale su $\mathbb{R}$, abbiamo sfruttato solamente le proprietà di campo di R. Possiamo quindi generalizzare l'esempio precedente. Dato un campo $\mathbb{K}$, sia $\mathbb{K}^n[x]$ l'insieme dei polinomi di grado minore di n a coefficienti nel campo $\mathbb{K}$ nella variabile x. Esso è uno spazio vettoriale sul campo $\mathbb{K}$. La sua **base canonica** è uguale a quella dell'esempio precedente.

Esercizio di base EB.4.5 Consideriamo l'insieme $\mathbb{C}^n[x]$ dei polinomi di grado minore di n a coefficienti in C. Consideriamo in esso l'usuale operazione di somma tra polinomi e l'operazione di moltiplicazione di un polinomio per un numero reale. Ovviamente abbiamo uno spazio vettoriale su $\mathbb{R}$. Determinarne una base. △

4.4 Basi di Lagrange

Consideriamo lo spazio vettoriale $\mathbb{R}^3[x]$ dei polinomi in una variabile x, di grado minore di 3 a coefficienti nel campo $\mathbb{R}$ dei reali. Supponiamo di avere tre numeri reali x_1, x_2, x_3 distinti e supponiamo di avere tre numeri reali b_1, b_2, b_3 qualsiasi. Ci chiediamo se esistono polinomi $p(x) \in \mathbb{R}^3[x]$ per cui si abbia

$$p(x_1) = b_1 \qquad p(x_2) = b_2 \qquad p(x_3) = b_3.$$

Per rispondere a questa domanda, prendiamo un polinomio generico

$$p(x) = a_0 + a_1 x + a_2 x^2$$

e imponiamo le condizioni richieste. Otteniamo un sistema di tre equazioni nelle tre incognite a_0, a_1, a_2. La matrice dei coefficienti del sistema ha determinante non nullo (è una matrice di Vandermonde). Il sistema ammette quindi una ed una sola soluzione (teorema di Cramer). Abbiamo quindi il seguente risultato.

Teorema 4.9 *Dati tre numeri reali x_1, x_2, x_3 distinti e tre numeri reali b_1, b_2, b_3 qualsiasi, esiste uno ed un solo polinomio $p(x) \in R^3[x]$ per cui si abbia*

$$p(x_1) = b_1 \qquad p(x_2) = b_2 \qquad p(x_3) = b_3.$$

DIMOSTRAZIONE. Appena fatta. □

Nota 4.10 Si può dare un significato geometrico al teorema appena dimostrato. Fissato un sistema di riferimento cartesiano nel piano, dati tre punti distinti di esso non appartenenti a due a due ad una stessa retta parallela all'asse delle ordinate, per i tre punti passa o una retta o una parabola avente l'asse parallelo all'asse delle ordinate. △

Vogliamo ora determinare effettivamente il polinomio del teorema 4.9. Potremmo determinarlo risolvendo il sistema, per esempio utilizzando la regola di Cramer. Ma noi vogliamo fare il minimo di calcoli. Proviamo allora a risolvere un problema più semplice. Vogliamo determinare un polinomio $p_1(x) \in \mathbb{R}^3[x]$ per cui si abbia:

$$p_1(x_1) = 1 \qquad p_1(x_2) = 0 \qquad p_1(x_3) = 0.$$

Sappiamo dal teorema precedente che un polinomio siffatto esiste ed è unico. Notiamo che il polinomio cercato deve avere x_2 e x_3 come radici. Esso deve allora avere come fattori $(x - x_2)$ e $(x - x_3)$. Ma allora si deve avere
$p_1(x) = a(x-x_2)(x-x_3)$, con a numero reale che dobbiamo ancora determinare. Determiniamo a ricordandoci che il polinomio cercato deve valere 1 in x_1. In definitiva otteniamo:

$$p_1(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}$$

Notiamo che il polinomio $b_1p_1(x)$ verifica le condizioni:

$$b_1p_1(x_1) = b_1 \qquad b_1p_1(x_2) = 0 \qquad b_1p_1(x_3) = 0.$$

Torniamo al nostro problema iniziale: vogliamo determinare il polinomio che assuma in x_1, x_2, x_3 rispettivamente i valori b_1, b_2, b_3. Ricordiamo che il polinomio $b_1p_1(x)$ assume in x_1 il valore desiderato e che negli altri due punti si annulla. Dovrebbe ora essere chiaro il procedimento da seguire. Consideriamo il polinomio:

$$p_2(x) = \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}$$

esso verifica le condizioni:

$$p_2(x_1) = 0 \qquad p_2(x_2) = 1 \qquad p_2(x_3) = 0.$$

Consideriamo poi il polinomio:

$$p_3(x) = \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

esso verifica le condizioni:

$$p_3(x_1) = 0 \qquad p_3(x_2) = 0 \qquad p_3(x_3) = 1.$$

E quindi il polinomio:

$$p(x) = b_1p_1(x) + b_2p_2(x) + b_3p_3(x)$$

verifica le condizioni richieste:

$$p(x_1) = b_1 \qquad p(x_2) = b_2 \qquad p(x_3) = b_3.$$

Ecco che abbiamo determinato il nostro polinomio non facendo praticamente alcun calcolo.

Teorema 4.11 *I polinomi:*

$$p_1(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}$$

$$p_2(x) = \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}$$

$$p_3(x) = \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

formano una base, detta **base di Lagrange relativa a** x_1, x_2, x_3*, dello spazio vettoriale* $\mathbb{R}^3[x]$.

DIMOSTRAZIONE Dobbiamo dimostrare innanzitutto che i tre vettori generano lo spazio vettoriale. Sia $q(x)$ un polinomio di $R^3[x]$. Dobbiamo dimostrare che esso è esprimibile come combinazione lineare dei tre vettori. Consideriamo i valori $q(x_1), q(x_2), q(x_3)$ assunti da $q(x)$ in x_1, x_2, x_3.
Notiamo che il polinomio $p(x) = q(x_1)p_1(x) + q(x_2)p_2(x) + q(x_3)p_3(x)$ assume sui tre punti gli stessi valori assunti dal polinomio $q(x)$. Dal teorema 4.9 segue allora $q(x) = p(x)$, proprio ciò che volevamo dimostrare.
Dobbiamo ora dimostrare che i tre polinomi sono linearmente indipendenti. Sia $p(x) = b_1p_1(x) + b_2p_2(x) + b_3p_3(x) = 0$. Dobbiamo dimostrare che i tre coefficienti della combinazione lineare sono tutti nulli. Il polinomio $p(x)$, poiché è, per ipotesi, identicamente nullo, assume sui tre punti il valore 0. Ma il valore assunto da $p(x)$ sui punti x_1, x_2, x_3 è uguale rispettivamente a b_1, b_2, b_3. Da ciò otteniamo $b_1 = b_2 = b_3 = 0$; cioè la tesi. ■

Nota 4.12 In precedenza avevamo considerato la base canonica di $\mathbb{R}^3[x]$. Abbiamo ora determinato un'altra base, quella di Lagrange. Ognuna delle due basi ha i suoi pregi e difetti. Quella canonica ha il vantaggio che le coordinate di un polinomio relative ad essa sono proprio i coefficienti del polinomio; quella di Lagrange permette di evitare molti calcoli quando si voglia determinare un polinomio che assuma determinati valori in determinati punti. Vi sono altre basi di $\mathbb{R}^3[x]$ che, in particolari situazioni, potrebbero essere più convenienti della base canonica o della base di Lagrange. La scelta della base più conveniente dipende ovviamente dall'intuito. △

Esempio 4.13 Il polinomio $p(x) \in R^3[x]$ tale che

$$p(0) = 7 \qquad p(3) = 2 \qquad p(9) = 9$$

è dato da:

$$p(x) = 7\frac{(x-3)(x-9)}{(0-3)(0-9)} + 2\frac{(x-0)(x-9)}{(3-0)(3-9)} + 9\frac{(x-0)(x-3)}{(9-0)(9-3)}$$

Esempio 4.14 Notiamo che, nel costruire la base di Lagrange, abbiamo sfruttato solamente le proprietà di campo di $\mathbb{R}$. Possiamo quindi generalizzare tutto ciò al caso di polinomi in $K^3[x]$ con K campo qualsiasi. Cerchiamo, ad esempio, il polinomio $p(x)$ di grado minore di 3 a coefficienti in Z_5 verificante le seguenti condizioni:

$$p([3]_5) = [2]_5 \ , \quad p([4]_5) = [3]_5 \ , \quad p([0]_5) = [1]_5$$

Per rispondere a questa domanda consideriamo la base di Lagrange $\{p_1(x), p_2(x), p_3(x)\}$ di $\mathbb{Z}_5^3[x]$ relativa a $[3]_5$, $[4]_5$, $[0]_5$. Abbiamo allora

$$p(x) = [2]_5 p_1(x) + [3]_5 p_2(x) + [1]_5 p_3(x)$$

La base di Lagrange cercata è:

$$p_1(x) = ([3]_5 - [4]_5)^{-1}([3]_5 - [0]_5)^{-1}(x - [4]_5)(x - [0]_5)$$

$$p_2(x) = ([4]_5 - [3]_5)^{-1}([4]_5 - [0]_5)^{-1}(x - [3]_5)(x - [0]_5)$$

$$p_3(x) = ([0]_5 - [3]_5)^{-1}([0]_5 - [4]_5)^{-1}(x - [3]_5)(x - [4]_5)$$

Si lascia come esercizio lo sviluppo dei calcoli. △

Esercizio di base EB.4.6 Determinare un polinomio $p(x)$ di grado minore di 3, a coefficienti interi, tale che:

$$p(4) \equiv 19 \pmod 7 \quad , \quad p(23) \equiv 100 \pmod 7 \quad , \quad p(12) \equiv -5 \pmod 7$$

Nota 4.15 (Generalizzazione) Vogliamo ora determinare un polinomio $p(x)$ a coefficienti reali che assuma in n punti $x_1, x_2, \ldots, x_n$ distinti i valori reali $b_1, b_2, \ldots, b_n$. Con un procedimento analogo a quello dato nel teorema 4.9 si dimostra che di polinomi siffatti di grado minore di n ne esiste uno ed uno solo. Per determinarlo effettivamente conviene definire una **base di Lagrange** di $\mathbb{R}^n[x]$. Essa è analoga alla base di Lagrange di $R^3[x]$. La sua costruzione viene lasciata per esercizio. △

Esercizio di base EB.4.7 Determinare un polinomio di grado minore di 4 a coefficienti reali che assuma nei punti 0, 7, 8, 9 i valori 2, 5, 12, 31 rispettivamente. △

Nota 4.16 (Ulteriore generalizzazione) Tutto ciò può essere generalizzato al caso di polinomi a coefficienti in un campo K qualsiasi. △

Esercizio di base EB.4.8 Determinare un polinomio di grado minimo a coefficienti interi che assuma su 1, 3, 5 e 7 valori interi congrui modulo 11 rispettivamente ai numeri 3, 21, 121 e 12. △

4.5 Soluzioni degli esercizi di base

Soluzione dell'esercizio di base EB.4.1 La dimostrazione è analoga alla dimostrazione di 2.2.

Soluzione dell'esercizio di base EB.4.2 La dimostrazione è analoga alla dimostrazione di 2.3.

Soluzione dell'esercizio di base EB.4.3 Se proprio non si riesce a dare da soli le dimostrazioni, andare a vedere le dimostrazioni fatte nel caso degli spazi vettoriali sui reali: ci si accorgerà che non vi è quasi niente da cambiare.

Soluzione dell'esercizio di base EB.4.4 Se proprio non si riesce a dare da soli la dimostrazione, andare a vedere la dimostrazione fatta nel caso degli spazi vettoriali sui reali: ci si accorgerà che non vi è quasi niente da cambiare.

Soluzione dell'esercizio di base EB.4.5 Una base dello spazio vettoriale $\mathbb{C}^n[x]$ sul campo $\mathbb{R}$ è data da:

$$\mathbf{v}_1 = 1, \mathbf{v}_2 = i, \mathbf{v}_3 = x, \mathbf{v}_4 = ix, \ldots, \mathbf{v}_{2n-1} = x^{n-1}, \mathbf{v}_{2n} = ix^{n-1}$$

Chiamiamo **base canonica** tale base.

Soluzione dell'esercizio di base EB.4.6 Stiamo cercando un polinomio a coefficienti interi

$$p(x) = ax^2 + bx + c$$

verificante tre condizioni. Consideriamo per ora solo la prima condizione

$$p(4) \equiv 19 \pmod 7$$

Si ha $p(4) = a \cdot 4^2 + b \cdot 4 + c$ e quindi dobbiamo imporre: $[a \cdot 4^2 + b \cdot 4 + [c]_7 = [19]_7$. Ma

$$[a \cdot 4^2 + b \cdot 4 + c]_7 = [a]_7 \cdot [4]_7^2 + [b]_7 \cdot [4]_7 + [c]_7$$

e quindi stiamo essenzialmente cercando un polinomio $p(x)$ di $\mathbb{Z}_7^3[x]$, verificante la condizione $p([4]_7) = [19]_7 = [4]_7$. In modo analogo per le altre due condizioni. Da tutto ciò segue che dobbiamo risolvere un esercizio analogo all'esempio 4.14. Lasciamo lo sviluppo dei calcoli al lettore.

Soluzione dell'esercizio di base EB.4.7 Seguire il procedimento descritto nell'esercizio precedente.

4.6 Esercizi

Esercizio E.4.1 Se Z_p è il campo delle classi di resto modulo un primo p, da quanti elementi è formato lo spazio vettoriale Z_p^n?

Esercizio E.4.2 Determinare il polinomio $p(x) \in R^3[x]$ tale che

$$p(\pi) = 0.1 \qquad p(1.5) = 0 \qquad p(\sqrt{2}) = 12$$

Esercizio E.4.3 Determinare il polinomio di grado minimo a coefficienti reali che assuma in $3, 2, 4, 5$ e 9 i valori $0, 3, 1, 0$ e π.

Esercizio E.4.4 Siano x_1, x_2 e $x-3$ tre numeri reali distinti e siano b_1, b_2 e b_3 tre numeri reali qualsiasi.
Sappiamo che esiste uno ed un solo polinomio $p(x) \in R^3[x]$ tale che

$$p(x_1) = b_1, p(x_2) = b_2, p(x_3) = b_3$$

Quanti polinomi appartenenti a $R^4[x]$ esistono verificanti le tre condizioni precedenti?

Esercizio E.4.5 Determinare il polinomio $p(x)$ di grado minimo a coefficienti complessi tale che:

$$p(1) = p(2) = i \quad p(i) = p(2i) = 1$$

Esercizio E.4.6 Quanti sono i polinomi $p(x) \in \mathbf{Z}_{19}^3[x]$ tali che $p([2]_{19}) = [2]_{19}$, $p([3]_{19}) = [3]_{19}$?

4.7 Soluzioni degli esercizi

Soluzione dell'esercizio E.4.1 Gli elementi di Z_p^n sono le n-uple del tipo

$$\left([a_1]_p, [a_2]_p, \ldots, [a_n]_p\right)$$

Ciascun elemento $[a_i]_p$ può essere scelto in p modi diversi: dunque abbiamo p^n elementi.

Soluzione dell'esercizio E.4.2 Per rispondere alla domanda si potrebbe ovviamente scrivere un generico polinomio e imporre le condizioni richieste. Ma così facendo si perde troppo tempo.
Conviene invece fissare la base di Lagrange relativa ai valori π, 1.5 e $\sqrt{2}$. Essa è data $\{p_1(x), p_2(x), p_3(x)\}$ con:

$$p_1(x) = \frac{(x-1.5)(x-\sqrt{2})}{(\pi-1.5)(\pi-\sqrt{2})}$$
$$p_2(x) = \frac{(x-\pi)(x-\sqrt{2})}{(1.5-\pi)(1.5-\sqrt{2})}$$
$$p_3(x) = \frac{(x-\pi)(x-1.5)}{(\sqrt{2}-\pi)(\sqrt{2}-1.5)}$$

Il polinomio cercato è dato da:

$$p(x) = 0.1p_1(x) + 12p_3(x)$$

Soluzione dell'esercizio E.4.3 Sappiamo che il polinomio cercato appartiene a $R^5[x]$. Consideriamo quindi la base di Lagrange relativa a $3, 2, 4, 5$ e 9. Il polinomio cercato è il polinomio avente coordinate $0, 3, 1, 0$ e π relative a tale base.

Soluzione dell'esercizio E.4.4 Sappiamo che il polinomio di $R^3[x]$ verificante le condizioni date è il polinomio

$$p(x) = b_1p_1(x) + b_2p_2(x) + b_3p_3(x)$$

dove

$$\{p_1(x), p_2(x), p_3(x)\}$$

è la base di Lagrange di $R^3[x]$ relativa a x_1, x_2 e x_3.
Ma ora noi cerchiamo tutti i polinomi di $R^4[x]$ verificanti le condizioni date. La base di Lagrange di $R^3[x]$ non è una base di $R^4[x]$. Infatti ogni combinazione lineare dei vettori di tale base è un polinomio di grado minore di 3.
Per ottenere una base di Lagrange di $R^4[x]$ abbiamo bisogno di un altro valore x_4 distinto dai primi 3.
Consideriamo ora una base di Lagrange $\{q_1(x), q_2(x), q_3(x), q_4(x)\}$ relativa a x_1, x_2, x_3, x_4.
ATTENZIONE: i primi tre vettori di questa nuova base si guardano bene dall'essere uguali ai vettori della base di Lagrange di $R^3[x]$ considerata in precedenza!
Bene, i vettori di $R^4[x]$ verificanti le tre condizioni assegnate sono:

$$p(x) = b_1q_1(x) + b_2q_2(x) + b_3q_3(x) + cq_4(x)$$

dove b_1, b_2, b_3 sono i valori fissati ma dove c_4 è un numero reale qualsiasi.
Quindi ad ogni numero reale c_4 corrisponde un vettore. A valori diversi di c_4 corrispondono vettori diver si (perché?). Poiché i numeri reali sono infiniti, abbiamo infiniti polinomi verificanti le tre condizioni richieste.

Soluzione dell'esercizio E.4.5 Sappiamo che in $C^4[x]$ esiste uno ed un solo polinomio verificante le condizioni richieste.
Consideriamo la base di Lagrange

$$\{p_1(x), p_2(x), p_3(x), p_4(x)\}$$

di $C^4[x]$ relativa a $1, 2, i, 2i$.
Il polinomio cercato è

$$p(x) = i \cdot p_1(x) + i \cdot p_2(x) + p_3(x) + p_4(x)$$

Per determinare esplicitamente il polinomio $p(x)$ è ovviamente necessario determinare esplicitamente i quattro vettori della base di Lagrange. Lasciamo ciò al lettore.

Soluzione dell'esercizio E.4.6 Sono 19. Perché?