Víctor Ballester
NIU:1570866
Novembre 2019

---

1. Siguin

$$F_1 = \langle(1,-1,1,-1),(2,-2,1,1),(-3,3,0,1),(0,0,5,6)\rangle$$
$$F_2 = \langle(1,2,3,4),(-1,4,2,3)\rangle$$

subespais vectorials de $\mathbb{Q}^4$.

(a) Calculeu la dimensió i una base dels subespais vectorials F_1, F_2, $F_1 \cap F_2$ i $F_1 + F_2$.

Posem els vectors de F_1 en una matriu i calculem el rang d'aquesta matriu:

$$\begin{pmatrix} 1 & -1 & 1 & -1 \\ 2 & -2 & 1 & 1 \\ -3 & 3 & 0 & 1 \\ 0 & 0 & 5 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 5 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 21 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Procedim de manera anàloga per F_2:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ -1 & 4 & 2 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 6 & 5 & 7 \end{pmatrix}$$

Observant les files del les dues matrius esglaonades podem concloure que $\dim(F_1) = 3$ i $\dim(F_2) = 2$. Una base de F_1 és $B_{F_1} = ((1,-1,1,-1),(0,0,-1,3),(0,0,0,7))$ i una base de F_2 és $B_{F_2} = ((1,2,3,4),(0,6,5,7))$.

Pel que fa a la intersecció i la suma dels dos subespais, comencem posant a una matriu els vectors de les bases B_{F_1} i B_{F_2} amb la matriu identitat al costat.

$$\left(\begin{array}{cccc|ccccc} 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 & 0 & 0 & 0 & 1 & 0 \\ 0 & 6 & 5 & 7 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cccc|ccccc} 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 2 & 5 & -1 & 0 & 0 & 1 & 0 \\ 0 & 6 & 5 & 7 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \to$$

$$\to \left(\begin{array}{cccc|ccccc} 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 2 & 5 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -3 & 2 & 0 & 0 & -2 & 1 \end{array}\right) \to \left(\begin{array}{cccc|ccccc} 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 2 & 5 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & -2 & 1 \end{array}\right)$$

Per tant, una base de $F_1 + F_2$ és $B_{F_1+F_2} = ((1,-1,1,-1),(0,3,2,5),(0,0,-1,3),(0,0,0,7))$ i, per tant, $\dim(F_1 + F_2) = 4$. Pel que fa a la intersecció ens fixem en la fila de 0's de la matriu principal i mirem els coeficients de la matriu invertible en aquesta fila. Per la intersecció, sigui $\mathbf{v} \in F_1 \cap F_2$. Aleshores, $\mathbf{v} \in F_1$ i $\mathbf{v} \in F_2$. Per tant podem escriure el vector $\mathbf{v}$ com a combinació lineal dels vectors de B_{F_1} i B_{F_2}:

$$\mathbf{v} = a(1,-1,1,-1) + b(0,0,-1,3) + c(0,0,0,7)$$
$$\mathbf{v} = d(1,2,3,4) + e(0,6,5,7)$$

Igualant les dues expressions tenim que:

$$a(1,-1,1,-1) + b(0,0,-1,3) + c(0,0,0,7) + (-d)(1,2,3,4) + (-e)(0,6,5,7) = 0$$

Si ens fixem bé, els termes $a, b, c, -d, -e$ són exactament els coeficients de la matriu invertible en la fila de 0's de la matriu principal. Per tant, substituint tenim que $a = 2, b = 1, c = 0, d = 2, e = 1$.

Substituint aquests valors a una de les expressions anteriors de $\mathbf{v}$ tenim que: $\mathbf{v} = (2, -2, 1, 1)$ i, per tant, aquest vector forma una base de $F_1 \cap F_2$: $B_{F_1 \cap F_2} = ((2, -2, 1, 1))$. Per la fórmula de Graßmann tenim que $\dim(F_1 \cap F_2) = \dim(F_1) + \dim(F_2) - \dim(F_1 + F_2) = 3 + 2 - 4 = 1$ i ens quadre amb el nombre de vectors de $B_{F_1 \cap F_2}$.

(b) Amplieu la base de $F_1 \cap F_2$ que heu trobat a una base de F_1 i a una base de F_2.

Com que el vector de la base de $F_1 \cap F_2$ és un vector contingut en la base de F_1, l'ampliació de la base de $F_1 \cap F_2$ a una nova base de F_1 és exactament la base B_{F_1} que hem trobat anteriorment. Per ampliar la base de $F_1 \cap F_2$ a una base de F_2 cal crear una matriu amb els vectors de B_{F_2} i $B_{F_1 \cap F_2}$ i estudiar la dependència lineal d'aquests.

$$\begin{pmatrix} 2 & -2 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 0 & 6 & 5 & 7 \end{pmatrix} \to \begin{pmatrix} 2 & -2 & 1 & 1 \\ -2 & -4 & -6 & -8 \\ 0 & 6 & 5 & 7 \end{pmatrix} \to \begin{pmatrix} 2 & -2 & 1 & 1 \\ 0 & -6 & -5 & -7 \\ 0 & 6 & 5 & 7 \end{pmatrix} \to \begin{pmatrix} 2 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 6 & 5 & 7 \end{pmatrix}$$

Per tant, una base de F_2 ampliada a partir de la base de $F_1 \cap F_2$ és: $B'_{F_2} = ((2, -2, 1, 1), (0, 6, 5, 7))$.

(c) Trobeu un sistema d'equacions lineal homogeni tal que F_1 sigui el conjunt de les solucions d'aquest sistema.

Per tal de crear aquest sistema lineal homogeni, creem el sistema d'equacions que consisteix en posar els vectors de F_1 com a columnes d'una matriu i afegir el vector (x, y, z, t) com una columna de la matriu ampliada. Esglaonant la matriu fins obtenir una fila de zeros (l'obtindrem sigui com sigui ja que $\dim(F_1) = 3$) tenim que:

$$\left(\begin{array}{cccc|c} 1 & 2 & -3 & 0 & x \\ -1 & -2 & 3 & 0 & y \\ 1 & 1 & 0 & 5 & z \\ -1 & 1 & 1 & 6 & t \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & 2 & -3 & 0 & x \\ 0 & 0 & 0 & 0 & x+y \\ 0 & -1 & 3 & 5 & z-x \\ 0 & 3 & -2 & 6 & x+t \end{array}\right)$$

Per tant, observant l'element de la matriu ampliada de la fila de zeros de la matriu principal, veiem que $x + y = 0$ és el sistema lineal homogeni que té com a solucions el subespai F_1.

2. En aquest exercici estudiem $\mathbb{R}$ com a $\mathbb{Q}$-espai vectorial.

(a) Siguin $m_1, \ldots, m_k$ enters lliures de quadrats (si un primer p divideix a m_i aleshores p^2 no el divideix) i coprimers dos a dos (els primers que divideixen m_i no divideixen m_j, $\forall\, i, j$). Demostreu per inducció que el conjunt $\{\sqrt{m_1}, \ldots, \sqrt{m_k}\}$ és un conjunts d'elements $\mathbb{Q}$-linealment independents.

Demostrarem una cosa més forta que el que ens demanen. Demostrarem que el conjunt $L_{k+1} = \{1, \sqrt{m_1}, \ldots, \sqrt{m_{k+1}}, \ldots, \sqrt{m_1 m_2}, \ldots, \sqrt{m_1 \cdots m_{n+1}}\}$ és $\mathbb{Q}$-linealment independent. En concret el conjunt L_{k+1} és el conjunt generat per 1, per les arrels dels primers k nombres donats lliures de quadrats i coprimers dos a dos i també per tots els possibles productes d'aquestes arrels entre elles combinades entre si (en total, L_k té exactament 2^k elements). Per veure-ho demostrem primer que L_k és un extensió del cos sobre el cos dels racionals, és a dir, que podem expressar qualsevol element $x \in L_k$ com $x = \alpha_1 + \alpha_2\sqrt{m_1} + \cdots + \alpha_{2^k}\sqrt{m_1 \cdots m_k}$. Per demostrar-ho, hem de veure que L_k és tancat per producte i per inversos. Agafem dos elements $a, b \in L_k$. Hem de veure que $ab \in L_k$. Sabem que a serà de la forma $a = \sqrt{p_1 \cdots p_r}$ i b serà de la forma $b = \sqrt{q_1 \cdots q_s}$. El seu producte serà de la forma $ab = \sqrt{p_1 \cdots p_r}\sqrt{q_1 \cdots q_s}$. Ara, sigui M el producte de tots els p_i tals que $p_i = q_j$ per alguns i, j. Aleshores, $ab = M\sqrt{p_1 \cdots p_{i-1}p_{i+1} \cdots p_r}\sqrt{q_1 \cdots q_{j-1}q_{j+1} \cdots q_s}$ que clarament pertany a L_k. Ara hem de veure que donat un $c \in L_k$ $\exists\, d \mid cd = 1$ i $d = c^{-1}$. Sabem que c és de la forma $c = \sqrt{n_1 \cdots n_t}$ i d ha de ser de la forma $d = \frac{1}{\sqrt{n_1 \cdots n_t}} = \frac{\sqrt{n_1 \cdots n_t}}{n_1 \cdots n_t} = \frac{1}{n_1 \cdots n_t}\sqrt{n_1 \cdots n_t} \in L_k$. Per tant, hem demostrat que L_k és un cos. De la mateixa manera es demostra que tots els L_i amb $1 \le i \le k$ són cossos extensions del del cos $\mathbb{Q}$. De la definició de cos podem expressar qualsevol $x \in L_i$ com $x = a + b\sqrt{m_i}$ amb $a, b \in L_{i-1}$, és a dir, una base B_{L_i} sobre L_{i-1} és $B_{L_i} = (1, \sqrt{m_i})$, que té dimensió 2. De forma similar una base una base B_{L_i} sobre

L_{i-2} és $B_{L_i} = (1, \sqrt{m_i}, \sqrt{m_{i-1}}, \sqrt{m_{i-1}m_i})$. En particular podrem expressar una base de L_k sobre $\mathbb{Q}$ com $B_{L_k} = (1, \sqrt{m_1}, \ldots, \sqrt{m_{n+1}}, \ldots, \sqrt{m_1 m_2}, \ldots, \sqrt{m_1 \cdots m_{n+1}})$ que tindrà 2^k elements.
Amb aquesta informació introductòria, demostrarem per inducció sobre k que el conjunt $L_{k+1} = \{1, \sqrt{m_1}, \ldots, \sqrt{m_{k+1}}, \ldots, \sqrt{m_1 m_2}, \ldots, \sqrt{m_1 \cdots m_{n+1}}\}$ és linealment independent.
Demostrem primer el cas k=1:
Sigui $B_{L_1} = (1, \sqrt{m_1})$ una base de L_1 sobre $\mathbb{Q}$. Hem de demostrar que la base és $\mathbb{Q}$-linealment independent. Suposem que no. Per tant aquesta base tindrà dimensió 1, és a dir, generarà el mateix espai que $\mathbb{Q}$, per tant, $\sqrt{m_1} \in \mathbb{Q}$. És a dir, podem expressar $\sqrt{m1}$ com $\sqrt{m_1} = \frac{x}{y}$ sent $x, y \in \mathbb{Z}^*$ i coprimers entre si. Això és impossible ja que sabem que m_1 és lliure de quadrats. Vegem-ho. Expressant m_1 com a producte de primers tenim que $m_1 = r_1 \cdots r_l$ i retocant l'expressió anterior, tenim que:

$$\frac{x}{y} = \sqrt{m_1}$$
$$\frac{x^2}{y^2} = m_1$$
$$x^2 = (r_1 \cdots r_l)y^2$$

Si $x = (r_1 \cdots r_l)z$, tenim que:

$$\begin{aligned} x^2 &= (r_1 \cdots r_l)y^2 \\ z^2(r_1 \cdots r_l)^2 &= (r_1 \cdots r_l)y^2 \\ z^2(r_1 \cdots r_l) &= y^2 \end{aligned}$$

Llavors $(r_1 \cdots r_l)$ divideix y^2, i en particular divideix y. Però havíem dit que x i y eren coprimers, per tant, contradicció i L_1 és $\mathbb{Q}$-linealment independent.
Ara suposem cert que L_k és $\mathbb{Q}$-linealment independent i provem que L_{k+1} també ho és. Per veure-ho, raonarem per reducció a l'absurd. En particular, si L_{k+1} és linealment dependent la base $B_{L_{k+1}}$ sobre el cos L_k no té dimensió 2, sinó que $\dim(B_{L_{k+1}}) = 1$, de manera que els subespais L_k i L_{k+1} tenen la mateixa dimensió i, en conseqüència, $\sqrt{m_{k+1}} \in L_k$. Aleshores podrem expressar $\sqrt{m_{k+1}}$ de las següent manera:

$$\sqrt{m_{k+1}} = \alpha + \beta\sqrt{m_k}$$

amb $\alpha, \beta \in L_{k-1}$. Retocant l'expressió, tenim que:

$$\begin{aligned} (\sqrt{m_{k+1}})^2 &= (\alpha + \beta\sqrt{m_k})^2 \\ m_{k+1} &= \alpha^2 + \beta^2 m_k + 2\alpha\beta\sqrt{m_k} \end{aligned}$$

Si $\alpha\beta \neq 0$ tindrem una expressió de $\sqrt{m_k}$ en termes de nombres racionals, és a dir, $\dim(L_k) = 1 \neq 2$ sobre el cos L_{k-1}, cosa que contradiu que és impossible per la H.I.. Per tant, $\alpha\beta = 0$. Si $\alpha = 0$, aleshores obtenim la següent expressió:

$$\begin{aligned} m_{k+1} &= \beta^2 m_k \\ m_{k+1}m_k &= \beta^2 m_k^2 \\ \sqrt{m_{k+1}m_k} &= \beta m_k \\ \beta &= \frac{1}{m_k}\sqrt{m_{k+1}m_k} \end{aligned}$$

i llavors $\beta \notin L_{k-1}$ per ser $m_{k+1}m_k$ coprimers entre si i, per tant, no ser quadrat de cap racional. Si, d'altra banda, $\beta = 0$, tenim la següent expressió:

$$\begin{aligned} m_{k+1} &= \alpha^2 \\ \alpha &= \sqrt{m_{k+1}} \end{aligned}$$

i llavors $\alpha \notin L_{k-1}$ per H.I.. Observem que el cas $\alpha = \beta = 0$ no es pot donar ja que sinó $\sqrt{m_{k+1}} = 0$, que és absurd. Per tant, hem demostrat que el conjunt L_{k+1} és $\mathbb{Q}$-linealment independent.

□

(b) Demostreu que, per a tot $k \geq 0$, el conjunt $\{2, \sqrt{2}, \sqrt[4]{2}, \ldots, \sqrt[2^k]{2}\}$ és un conjunt $\mathbb{Q}$-linealment independent. Per fer-ho, podeu seguir els següents passos:

i. Demostreu que $\forall m \geq 1$ el polinomi $x^m - 2$ és irreductible a $\mathbb{Q}[x]$, és a dir, que no es pot escriure com a producte de dos polinomis a $\mathbb{Q}[x]$ de grau $\leq k$. En particular, per a qualsevol $k \geq 0$ el polinomi $x^{2^k} - 2$ és irreductible. (Indicació: trobeu primer les arrels complexes de $x^m - 2$, després escriviu $x^m - 2 = g(x)h(x)$ i raoneu per què els termes constant de $g(x)$ i $h(x)$ no poden ser enters).

Sigui $S = \{x_1, \ldots, x_m\}$ el conjunt de solucions del $P(x) = x^m - 2$. Aquest polinomi el podem expressar també de la forma $x^m = z = 2 + 0i = 2$. Sabem que el mòdul de z és $|z| = 2$ i l'argument és igual a $\theta = \arg(z) = 2\pi(n-1)$ $\forall n \in \mathbb{N}^*$. Els nombres complexos els podem expressar de la forma $z = |z|e^{\theta i}$, de manera que tindrem que $z = 2e^{2\pi(n-1)i}$. Substituint z a l'equació per x^m, tenim que: $x^m = 2e^{2\pi(n-1)i}$ i, per tant, $x = \sqrt[m]{2}e^{\frac{2\pi(n-1)i}{m}}$. Donant els primers m valors naturals a n (és a dir, $n = 1, \ldots, m$), tenim que el conjunt de solucions de l'equació principal són:

$$\begin{aligned} x_1 &= \sqrt[m]{2} \\ x_2 &= \sqrt[m]{2}e^{\frac{2\pi i}{m}} \\ &\vdots \\ x_m &= \sqrt[m]{2}e^{\frac{2\pi(m-1)i}{m}} \end{aligned}$$

De manera que podem factoritzar el polinomi $P(x)$ i expressar-lo en funció de les seves arrels:

$$P(x) = (x - \sqrt[m]{2}\lambda_1)(x - \sqrt[m]{2}\lambda_2)\cdots(x - \sqrt[m]{2}\lambda_m)$$

on $\lambda_j = e^{\frac{2\pi(j-1)i}{m}}$ per a $1 \leq j \leq m$. D'altra banda també podem factoritzar el polinomi com a producte de dos polinomis de grau més petit que m. Així tenim que:

$$\begin{aligned} P(x) &= g(x)h(x) \\ x^m - 2 &= (x-a)(b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0) \end{aligned}$$

Hem de veure que $a, b_0 \notin \mathbb{Q}$ i, en particular, $a, b_0 \notin \mathbb{Z}$. Per demostrar-ho, ho raonarem per reducció a l'absurd. Suposem que són $a, b_0 \in \mathbb{Q}$. Aleshores compararem els termes constants de les dos factoritzacions del polinomi $P(x)$ que hem fet anteriorment, que han de ser necessàriament iguals. Tenim llavors que:

$$P(x) = (x-a)(b_{m-1}x^{m-1} + \cdots + b_0) = (x - \sqrt[m]{2}\lambda_1)(x - \sqrt[m]{2}\lambda_2)\cdots(x - \sqrt[m]{2}\lambda_m)$$

i en particular:

$$\begin{aligned} -ab_0 &= (-\sqrt[m]{2})^m\lambda_1\cdots\lambda_m \\ -ab_0 &= (-\sqrt[m]{2})^m e^0 e^{\frac{2\pi i}{m}}\cdots e^{\frac{2\pi(m-2)i}{m}}e^{\frac{2\pi(m-1)i}{m}} \\ -ab_0 &= (-1)^m 2e^0e^{2\pi i}\cdots e^{2\pi(m-2)i}e^{2\pi(m-1)i} \\ (-1)^{m-1}\frac{ab_0}{2} &= e^{0+2\pi i+2\pi\cdot 2i+\cdots+2\pi(m-2)i+2\pi(m-1)i} \\ (-1)^{m-1}\frac{ab_0}{2} &= e^{2\pi i(1+\cdots+m-1)} \\ (-1)^{m-1}\frac{ab_0}{2} &= e^{2\pi i(\frac{m(m-1)}{2})} \\ (-1)^{m-1}\frac{ab_0}{2} &= e^{\pi m(m-1)i} \end{aligned}$$

Clarament la part de l'esquerra és racional, mentre que la de la dreta és irracional, igualtat que és absurda, per tant, la afirmació inicial era falsa i $a, b_0 \notin \mathbb{Q}$. En particular $a, b_0 \notin \mathbb{Z}$. Hem demostrat que el polinomi $P(x) = x^m - 2$ és irreductible a $\mathbb{Q}[x]$. En particular, fent $m = 2^k$ per a qualsevol $k \geq 0$ tenim que el polinomi $P'(x) = x^{2^k} - 2$ és irreductible.

ii. Demostreu que una combinació lineal no trivial dels elements fins a $\sqrt[2^k]{2}$ dona lloc a un polinomi de grau dividint 2^{k-1} que té $\sqrt[2^k]{2}$ com a arrel.
Sabem que podem expressar els elements del conjunt $\{2, \sqrt{2}, \sqrt[4]{2}, \ldots, \sqrt[2^k]{2}\}$ com una combinació lineal no trivial d'aquests:

$$2\mu_0 + \sqrt{2}\mu_1 + \cdots + \sqrt[2^j]{2}\mu_j + \cdots + \sqrt[2^k]{2}\mu_k = 0$$

amb $\mu_0, \ldots, \mu_k$ no tots 0. Ara bé, fent $x = \sqrt[2^k]{2}$ i substituint tots els termes irracionals dels sumands anteriors per l'expressió de x, podem escriure el següent polinomi:

$$Q(x) = \mu_1 x^{2^{k-1}} + \cdots + \mu_j x^{2^{k-j}} + \cdots + \mu_k x + 2\mu_0 = 0$$

que s'anul·la en $x = \sqrt[2^k]{2}$ i, per tant, $\sqrt[2^k]{2}$ és una arrel de $Q(x)$.

iii. Deduïu una contradicció fent servir els dos apartats anteriors (recordeu la divisió de polinomis: donats polinomis $a(x)$ i $b(x)$, existeixen polinomis $q(x)$ i $r(x)$ amb $\text{grau}(r(x)) \leq \text{grau}(b(x))$ tals que $a(x) = b(x)q(x) + r(x)$.)