Víctor Ballester
NIU:1570866
Gener 2020

---

1. Sigui E l'$\mathbb{R}$-espai vectorial dels polinomis amb coeficients reals de grau menor o igual que, és a dir, $E = \{p(x) \in \mathbb{R}[x] \mid \operatorname{gr}(p(x)) \leq 3\}$. Siguin

$$F = \{a_0 + a_1x + a_2x^2 + a_3x^3 \in E \mid -a_0 + a_1 + a_3 = 0\}$$
$$G = \langle 1 - x - x^2 + x^3, 2 + x - x^2\rangle$$

(a) Calculeu la dimensió i una base de F, G, $F \cap G$, $F + G$.
Per l'isomorfisme de coordenació tenim l'isomorfisme següent:

$$\begin{aligned} \mathbb{R}^4 &\longrightarrow F \\ (a_0, a_1, a_2, a_3) &\longmapsto a_0 + a_1x + a_2x^2 + a_3x^3 \end{aligned}$$

Sabent, a més, que tots els polinomis de F han de complir que $a_0 = a_1 + a_3$, llavors tenim que les coordenades de F a $\mathbb{R}^4$ seran $(a_1 + a_3, a_1, a_2, a_3) = a_1(1, 1, 0, 0) + a_2(0, 0, 1, 0) + a_3(1, 0, 0, 1)$ i, per tant, una base de F és $B_F = ((1, 1, 0, 0), (0, 0, 1, 0), (1, 0, 0, 1))$ i la dimensió de F és $\dim(F) = 3$.
D'altra banda i de la mateixa manera que anteriorment, agafem les coordenades dels dos polinomis que generen G i vegem que són linealment independents:

$$\begin{pmatrix} 1 & -1 & -1 & 1 \\ 2 & 1 & -1 & 0 \end{pmatrix}$$

Clarament ho són, per la última coordenada nul·la del segon polinomi. Així una base de G és $B_G = ((1, -1, -1, 1), (2, 1, -1, 0)$ i la dimensió de G és $\dim(G) = 2$.
Pel que fa a la intersecció i la suma dels dos subespais, comencem posant a una matriu els vectors de les bases B_F i B_G amb la matriu identitat al costat.

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

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

Per tant, una base de $F + G$ és $B_{F+G} = ((1, 1, 0, 0), (0, 0, 1, 0), (0, -1, 0, 1), (0, 0, -1, -1))$ i, per tant, $\dim(F + G) = 4$. Pel que fa a la intersecció, sigui $\mathbf{v} \in F \cap G$. Aleshores, $\mathbf{v} \in F$ i $\mathbf{v} \in G$. Per tant podem escriure el vector $\mathbf{v}$ com a combinació lineal dels vectors de B_F i B_G:

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

Igualant les dues expressions tenim que:

$$a(1, 1, 0, 0) + b(0, 0, 1, 0) + c(1, 0, 0, 1) + (-d)(1, -1, -1, 1) + (-e)(2, 1, -1, 0) = 0$$

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 $a = -2, b = 0, c = 1, d = 1, e = -1$. Substituint aquests valors a una de les expressions anteriors de $\mathbf{v}$ tenim que: $\mathbf{v} = (-1, -2, 0, 1)$ i, per tant, aquest vector forma una base de $F \cap G$: $B_{F\cap G} = ((-1, -2, 0, 1))$. Per la fórmula de Graßmann tenim que $\dim(F \cap G) = \dim(F) + \dim(G) - \dim(F + G) = 3 + 2 - 4 = 1$ i ens quadre amb el nombre de vectors de $B_{F\cap G}$.

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

Per ampliar la base de $F \cap G$ a una base de F cal crear una matriu amb els vectors de B_F i $B_{F\cap G}$ i estudiar la dependència lineal d'aquests.

$$\begin{pmatrix} -1 & -2 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} -1 & -2 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & -2 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Així, una base de F a partir de l'ampliació de la base de $F \cap G$ és $B_{F'} = ((-1,-2,0,1),(0,-1,0,1),(0,0,1,0))$. Procedint de manera anàloga per G, creem la matriu amb els vectors de la base de $F \cap G$ i els vectors de la base de G.

$$\begin{pmatrix} -1 & -2 & 0 & 1 \\ 1 & -1 & -1 & 1 \\ 2 & 1 & -1 & 0 \end{pmatrix} \to \begin{pmatrix} -1 & -2 & 0 & 1 \\ 0 & -3 & -1 & 2 \\ 0 & -3 & -1 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & -2 & 0 & 1 \\ 0 & -3 & -1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Així, una base de G a partir de l'ampliació de la base de $F \cap G$ és $B_{G'} = ((-1,-2,0,1),(0,-3,-1,2))$.

2. Sigui p un primer, i sigui $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ el cos amb p elements, i considerem l'espai vectorial format pels polinomis $\mathbb{F}_p[x]$.

(a) Donat un polinomi $f(x) \in \mathbb{F}_p[x]$, sigui $(f) = \{h(x) \in \mathbb{F}_p[x] \mid h(x) \text{ és múltiple de } f(x)\}$. Demostreu que (f) és un subespai vectorial de $\mathbb{F}_p[x]$.

Per demostrar que (f) és subespai vectorial de $\mathbb{F}_p[x]$ cal veure tres coses:

- $0 \in (f)$:
  Sabem, per definició, que qualsevol $h(x) \in (f)$ el podem escriure de la forma $h(x) = f(x)p(x)$ amb $p(x) \in \mathbb{F}_p[x]$. Així fent $p(x) = 0$ tenim que $h(x) = 0$ i $0 \in (f)$.
- Donats $g(x), h(x) \in (f)$ aleshores $g(x) + h(x) \in (f)$:
  De la mateixa manera que anteriorment, podem escriure els polinomis $g(x)$ i $h(x)$ com $g(x) = f(x)p(x)$ i $h(x) = f(x)q(x)$ amb $p(x), q(x) \in \mathbb{F}_p[x]$. Sumant les equacions tenim que $g(x) + h(x) = f(x)p(x) + f(x)q(x) = f(x)(p(x) + q(x))$ i, per tant, $g(x) + h(x) \in (f)$.
- Donat un $g(x) \in (f)$ i un $\lambda(x) \in \mathbb{F}_p[x]$ aleshores $\lambda(x)g(x) \in (f)$:
  De la mateixa manera que anteriorment, tenim un $g(x) \in (f)$ que podem expressar de la forma $g(x) = f(x)p(x)$ amb $p(x) \in \mathbb{F}_p[x]$. Multiplicant l'expressió per un $\lambda(x)$ tenim que $\lambda(x)g(x) = \lambda(x)f(x)p(x) = f(x)(\lambda(x)p(x))$ i, per tant, $\lambda(x)g(x) \in (f)$.

$\square$

(b) Sigui $L = \mathbb{F}_p[x]/(f)$ l'espai quocient. Trobeu la dimensió i una base de L. Quants elements té L? Comproveu que a L el producte de classes definit a partir del producte de representants ($[g] \cdot [h] = [gh]$) està ben definit.

Com que tots els $h(x) \in (f)$, els múltiples de $f(x)$, tenen grau més gran o igual al grau de $f(x)$, és a dir, gr $h(x) \geq$ gr $f(x)$, aleshores una base de L estarà formada pels elements de la base de $\mathbb{F}_p[x]$ que no siguin a la base de (f). Així com que els $h(x)$ tenen com a mínim el mateix grau que $f(x)$, una base de (f) serà $B_{(f)} = (x^k, x^{k+1}, x^{k+2}, ...)$ on $k =$ gr $f(x)$. És clar que una base de $\mathbb{F}_p[x]$ és $B_{\mathbb{F}_p[x]} = (1, x, ..., x^{k-1}, x^k, x^{k+1}, ...)$. Així, mirant els elements que són a $B_{\mathbb{F}_p[x]}$ i no a $B_{(f)}$ seran els element de la base de L: $B_L = (1, x, ..., x^{k-2}, x^{k-1})$ i, per tant, dim $(L) = k$. Com que cada element de la base el podem multiplicar per p nombres diferents i sabent que hi ha k elements a la base tindrem que L té p^k elements.

Per veure que el producte de classes definit a partir del producte de representants està ben definit, hem de veure que donades dues classes $[g]$, $[h]$ el seu producte és una classe de L. Així, efectuem el producte de dos representants g i h, $q = gh$. Se'ns poden presentar dos casos: si gr $q(x) <$ gr $f(x)$ o gr $q(x) \geq$ gr $f(x)$. Pel primer cas és directe ja que q és un representant de L i, per tant, $[g] \cdot [h] = [q]$. Si se'ns dona el segon cas, hem de mirar el residu de la divisió euclídia de $q(x)$ per $f(x)$. De manera que $q(x) \equiv r(x) \mod f(x)$ per algun $r(x) \in L$. Sabem que $\text{gr}\ r(x) < \text{gr}\ f(x)$ i, per tant, $[g] \cdot [h] = [r]$.

$\square$

(c) Suposem ara que f és irreductible a $\mathbb{F}_p[x]$ (és a dir, que no factoritza com a producte de dos polinomis de grau estrictament menor que el de f). Demostreu que la multiplicació de classes dona una estructura de cos a L. (Indicació: Per $[g] \neq 0$ considereu l'aplicació $\phi_{[g]} : L \longrightarrow L$ donada per $\phi_{[g]}([h]) = [gh]$ i demostreu que és bijectiva).

Perquè L sigui un cos, la multiplicació de classes ha de complir les següents propietats:

- Propietat associativa:
  Siguin $[x], [y], [z] \in L$. Hem de demostrar que $([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$.

$$\begin{aligned}
([x] \cdot [y]) \cdot [z] &= [xy] \cdot [z] && \text{ja que el producte de representants està ben definit a } L.\\
&= [(xy)z]\\
&= [x(yz)] && \text{ja que la propietat associativa està ben definida a } \mathbb{F}_p[x].\\
&= [x] \cdot [yz]\\
&= [x] \cdot ([y] \cdot [z])
\end{aligned}$$

- Propietat commutativa:
  Siguin $[x], [y] \in L$. Hem de demostrar que $[x] \cdot [y] = [y] \cdot [x]$.

$$\begin{aligned}
[x] \cdot [y] &= [xy] && \text{ja que el producte de representants està ben definit a } L.\\
&= [yx] && \text{ja que la propietat commutativa està ben definida a } \mathbb{F}_p[x].\\
&= [y] \cdot [x]
\end{aligned}$$

- Existència de l'element neutre:
  Sigui $[p] \in L$. Llavors $\exists\, i \in L \mid [p] \cdot [i] = [i] \cdot [p] = [p]$. Trobem-lo:
  Aquest element i és la classe dels polinomis $[i(x)] = 1$, ja que $[i(x)] \cdot [p(x)] = [p(x)] \cdot [i(x)] = [p(x)]$ amb $[p(x)] \in L$.
- Existència de l'element invers:
  Per aquesta propietat considerarem l'aplicació $\phi_{[g]} : L \longrightarrow L$ donada per $\phi_{[g]}([h]) = [gh]$. Hem de demostrar que és bijectiva, és a dir, injectiva i exhaustiva. D'aquesta manera podrem definir la seva aplicació inversa i trobar l'element invers de $[g]$.
  - Demostrem que és injectiva:
    Sigui $\phi_{[g]}([h]) = \phi_{[g]}([k])$. Hem de veure que $[h] = [k]$.

$$\begin{aligned}
\phi_{[g]}([h]) &= \phi_{[g]}([k])\\
[gh] &= [gk]\\
[g] \cdot [h] &= [g] \cdot [k]
\end{aligned}$$

    Com que f és irreductible podem multiplicar $m - 1$ vegades l'expressió anterior per $[g]$, on m és l'ordre multiplicatiu de $[g]$ de manera que $[g]^m \equiv 1 \bmod (f)$. Així, tenim que:

$$\begin{aligned}
[g] \cdot [h] &= [g] \cdot [k]\\
[g]^m \cdot [h] &= [g]^m \cdot [k]\\
[h] &= [k]
\end{aligned}$$

    com volíem demostrar.
  - Demostrem que és exhaustiva:
    Sigui $[x] \in L$. Volem veure que existeix un $[h]$ tal que $\phi_{[g]}([h]) = [x]$.

$$\begin{aligned}
\phi_{[g]}([h]) &= [x]\\
[gh] &= [x]\\
[g] \cdot [h] &= [x]
\end{aligned}$$

Com que f és irreductible podem multiplicar $m-1$ vegades l'expressió anterior per $[g]$, on m és l'ordre multiplicatiu de $[g]$ de manera que $[g]^m \equiv 1 \bmod (f)$. Així, tenim que:

$$\begin{aligned} [g] \cdot [h] &= [x] \\ [g]^m \cdot [h] &= [g]^{m-1} \cdot [x] \\ [h] &= [g]^{m-1} \cdot [x] \end{aligned}$$

i hem trobat un $[h]$ tal que $\phi_{[g]}([h]) = [x]$.

Així, com que l'aplicació és bijectiva té sentit parlar de la inversa. Sigui $\varphi_{[k]}$ una aplicació tal que $\phi_{[g]} \circ \varphi_{[k]} = \varphi_{[k]} \circ \phi_{[g]} = id$. Aquesta aplicació $\varphi_{[k]}$ és la definida per $\varphi_{[k]}([h]) = [kh]$. Fent la primera composició tenim que $\phi_{[g]} \circ \varphi_{[k]}([h]) = [kgh] = [h]$ i fent la segona composició tenim que $\varphi_{[g]} \circ \phi_{[k]}([h]) = [gkh] = [h]$. Observant els dos resultats veiem que $[kg] = [gk] = id$, és a dir, $[g] \cdot [k] = [k] \cdot [g] = id$ i, per tant, $[k] = [g]^{-1}$ és l'element invers de $[g]$ com volíem demostrar.

- Propietat distributiva respecte la suma:
Siguin $[x], [y], [z] \in L$. Hem de demostrar que $[x] \cdot ([y] + [z]) = [x] \cdot [y] + [x] \cdot [z]$. Com que de la suma de dos polinomis es realitza coeficient a coeficient, aquesta estarà ben definida a L. Així, demostrem que a L es compleix la propietat distributiva del producte respecte la suma.

$$\begin{aligned} [x] \cdot ([y] + [z]) &= [x] \cdot [y+z] && \text{ja que la suma de representants està ben definida.} \\ &= [x(y+z)] && \text{ja que el producte de representants està ben definit.} \\ &= [xy + xz] && \text{ja que la propietat distributiva està ben definida a } \mathbb{F}_p[x]. \\ &= [xy] + [xz] \\ &= [x] \cdot [y] + [x] \cdot [z] \end{aligned}$$

- $0 \neq 1$:
Aquesta propietat és trivial de demostrar ja que el polinomi neutre per la suma no pot ser el mateix que el polinomi neutre per el producte, vegem-ho:
Raonarem per reducció a l'absurd. Sigui K un cos. Suposem que la suma i el producte tenen el mateix element neutre i. Per definició l'element neutre del producte es comporta de la manera següent: $i \cdot x = x \cdot i = x \quad \forall x \in K$. Però, a més, l'element neutre de la suma és absorbent en el producte, és a dir, $i \cdot x = x \cdot i = i \quad \forall x \in K$. Aleshores, estem dient que $i = x \quad \forall x \in K$, que és absurd. Per tant $0 \neq 1$.

$\square$