Contents

Chapter 0

Preliminars

0.1 L'estructura de cos

Els conjunts dels nombres racionals $\mathbb{Q}$, reals $\mathbb{R}$ i complexos $\mathbb{C}$, amb les operacions ordinàries d'addició i multiplicació, són exemples de cossos. Amb això volem dir que cadascun d'aquests conjunts amb les operacions esmentades presenta diverses propietats que són les que apareixen a la següent definició general.

Definició 0.1
Sigui K un conjunt dotat de dues operacions, addició $(+)$ i multiplicació $(\cdot)$. Direm que K és un cos si es compleixen les condicions següents:

1) $a+b \in K$ *i* $a \cdot b \in K$ *(és a dir $+$ i $\cdot$ són operacions internes sobre K),*

2) $a+b = b+a$ *i* $a \cdot b = b \cdot a$ *($+$ i $\cdot$ són operacions commutatives),*

3) $(a+b)+c = a+(b+c)$ *i* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*, per tots* $a, b, c \in K$ *($+$ i $\cdot$ són operacions associatives),*

4) (a) Hi ha un element neutre per a l'addició: $a+0 = 0+a = a$*, per tot* $a \in K$*.*

(b) Hi ha un element neutre per a la multiplicació (distint del neutre de l'addició): $a \cdot 1 = 1 \cdot a = a$*, per tot* $a \in K$*.*

5) (a) Per a cada $a \in K$ *hi ha un altre element* $-a \in K$ *tal que* $a+(-a) = (-a)+a = 0$*. Direm que* $-a$ *és l'oposat de* a*.*

(b) Per a cada $a \in K$ *hi ha un altre element* $a^{-1} \in K$ *tal que* $a \cdot a^{-1} = a^{-1} \cdot a = 1$*. Direm que* a^{-1} *és l'invers de* a*.*

6) $a \cdot (b+c) = a \cdot b + a \cdot c$ *i* $(a+b) \cdot c = a \cdot c + a \cdot b$*, per tots* $a, b, c \in K$ *($\cdot$ és distributiva respecte de $+$).*

Quan no pugui haver confusió llevarem el signe $\cdot$ per denotar l'operació de multiplicació, és a dir denotarem $a \cdot b$ per ab.

Exemples 1

(a) El conjunt $\mathbb{N} = \{1, 2, 3, \ldots\}$ *dels nombres enters positius no és un cos (amb l'addició i multiplicació ordinàries). Ens fallen les condicions 4.a), 5.a) i 5.b).*

(b) El conjunt $\mathbb{Z}$ *dels nombres enters no constitueixen tampoc un cos (amb l'addició i multiplicació ordinàries). No es verifica la condició 5.b (els únics nombres enters que tenen invers són 1 i -1).*

(c) Els cossos $\mathbb{Q}$*,* $\mathbb{R}$ *i* $\mathbb{C}$ *són exemples de cossos infinits:* $\mathbb{Q}$*,* $\mathbb{R}$ *i* $\mathbb{C}$ *tenen infinits elements.*

(d) Hi ha també cossos finits. Uns exemples en són els cossos $\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}$*, on* p *és un nombre primer, amb les operacions addició,* $\oplus$*, i multiplicació,* $\otimes$*, següents:* $a \oplus b$ *és el residu de dividir el nombre enter* $a+b$ *entre* p*. Anàlogament,* $a \otimes b$ *és el residu de dividir* ab *entre* p*. Així, si* $p = 5$*, tenim* $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$*, i per exemple,* $2 \oplus 4 = 1, 3 \oplus 2 = 0, 2 \oplus 1 = 3$*, etc. També podem escriure* $2 \otimes 3 = 1, 3 \otimes 3 = 4, 4 \otimes 2 = 3, 2 \otimes 0 = 0$*, etc.*

Proposició 0.1 (Propietats dels cossos)
En un cos qualsevol K es verifiquen les propietats següents:

1) *$a+b=a+c$ implica $b=c$ (propietat de simplificació per la suma).*
   $ab=ac$, amb $a\neq 0$, implica $b=c$ (propietat de simplificació pel producte).

2) *Els neutres (0 i 1) són únics.*
   Cada element té un únic oposat, i si és diferent de 0 té un únic invers.

3) *$a\cdot 0=0$ per tot $a\in K$ (0 és absorbent per la multiplicació).*

4) *$ab=0$ implica $a=0$ o $b=0$ (K no té divisors de zero)*

□

0.2 Polinomis

Sigui K un cos qualsevol. Podem construir a partir de K polinomis en una indeterminada, que són objectes de la forma $p(x)=a_0+a_1x+a_2x^2+...+a_nx^n$ on $a_i\in K$ per tot $i, i:0,1,...,n$. Un polinomi $a_0+a_1x+a_2x^2+...+a_nx^n$ es pot escriure també en forma de successió: $(a_0,a_1,a_2,\ldots,a_n,0,0,\ldots)$. Dos polinomis són iguals si tenen els mateixos coeficients (són iguals com a successions). Si $a_n\neq 0$ deim que el grau del polinomi és n. El polinomi 0 ($a_i=0$ per tot $i, i:0,1,...,n$) i els polinomis de grau 0 són els polinomis constants. Per conveni, direm que el polinomi 0 té grau $-\infty$ ($-\infty<n$, per tot n). Indicarem per $K[x]$ el conjunt de polinomis en una indeterminada x i amb coeficients de K.

Sobre $K[x]$ es poden considerar l'addició i la multiplicació definides a partir de les operacions de K de la manera següent:

- $p(x)+q(x)$ és el polinomi que té per coeficients la suma (dins K) dels coeficients de $p(x)$ i $q(x)$. Més clarament, si $p(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ i $q(x)=b_0+b_1x+b_2x^2+\ldots+b_mx^m$, llavors $p(x)+q(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\ldots$
- El producte $p(x)q(x)$ és el polinomi $c_0+c_1x+c_2x^2+\ldots+c_{nm}x^{n+m}$ on $c_j=a_0b_j+a_1b_{j-1}+a_2b_{j-2}+\ldots+a_{j-1}b_1+a_jb_0, j:0,1,\ldots n+m$.

Amb aquestes operacions el conjunt $K[x]$ presenta una sèrie de propietats importants que no permeten però dir que és un cos. La condició de cos que ens falla aquí (igual que en el cas dels nombres enters) és únicament la 5.b). De fet els únics polinomis que tenen invers són els constants i diferents de 0.

De la mateixa manera que per nombres enters disposam d'un resultat important, anomenat teorema Fonamental de l'Aritmètica, que ens permet descompondre de forma única qualsevol nombre en producte de nombres primers, pel cas dels polinomis amb coeficients en un cos, podem parlar d'un resultat semblant. En aquest cas, un polinomi deim que és primer (o irreductible) si no és constant i no es pot descompondre en producte d'uns altres dos polinomis sense que aquesta descomposició sigui trivial. Així, per exemple, a $\mathbb{R}[x]$ el polinomi $p(x)=1+x^2$ és primer ja que $1+x^2$ no es pot escriure en la forma $r(x)s(x)$, a no ser que facem $1+x^2=\frac{1}{2}(2+2x^2)$ o $1+x^2=(-1)(-1-x^2)$, etc. En canvi $q(x)=1-x^2$ no és primer ja que $1-x^2=(1-x)(1+x)$.

Donat un polinomi $p(x)\in K[x]$, podem associar a $p(x)$ una aplicació o funció $K\to K$ definida de la manera següent: a cada element $\alpha\in K$ li feim correspondre $p(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\ldots+a_n\alpha^n$ (valor numèric de $p(x)$ quan $x=\alpha$). Hem de fer notar que diferents polinomis poden tenir funcions associades iguals, així per exemple: els polinomis de $\mathbb{Z}_2[x], p(x)=1+x$ i $q(x)=1+x+x^2+x^3$ tenen la mateixa funció associada: $0\to 1, 1\to 0$. Aquesta anomalia no passa quan K és un cos infinit. Així, en el cas que K sigui $\mathbb{Q},\mathbb{R}$ o $\mathbb{C}$, podem identificar polinomi amb funció associada. Siguin $p(x)\in K[x]$ i $\alpha\in K$, direm que α és una arrel de $p(x)$ si $p(\alpha)=0$. s ben conegut el resultat que ens diu que $\alpha\in K$ és una arrel de $p(x)$ si, i només si, $p(x)=(x-\alpha)q(x)$, amb $q(x)\in K[x]$. D'això es pot dedur que si un polinomi de $K[x]$ de grau major que 1 té una arrel (dins K) llavors no és primer. Cal observar que el recíproc no és cert: el polinomi $(1+x^2)^2$ no és primer sobre $\mathbb{R}$ i no té cap arrel dins $\mathbb{R}$.

0.3 Operacions externes

DEFINICIÓ 0.2
Sigui K un cos qualsevol i E un conjunt qualsevol no buit. Una operació externa sobre E amb domini K és una aplicació (funció) entre $K \times E$ i E.

Per tant, el que fa una operació externa és associar a cada parella ordenada (a, x) amb $a \in K$ i $x \in E$ un únic element de E, que representam per ax. Les operacions que fins ara hem tractat són internes, és a dir, associen a cada parella ordenada d'elements d'un mateix conjunt K un altre element únic del mateix conjunt: són aplicacions del tipus $K \times K \to K$.

Per exemple, $a*(x, x') = (ax, ax')$ és una operació externa sobre $E = K \times K$ amb domini el mateix K. Un altre exemple d'operació externa podria ser $a * x = xa$ on $a \in \mathbb{R}$ i $x \in \mathbb{R}^+$ (nombres reals estrictament positius). Aquesta operació és sobre $E = \mathbb{R}^+$ i té domini $K = \mathbb{R}$.

0.4 Matrius. Representació matricial d'aplicacions lineals

En aquesta secció estudiarem aquelles aplicacions entre dos $K-$e.v. que en conserven l'estructura vectorial i la seva relació amb les matrius.

Recordam la definició d'aplicació lineal.

DEFINICIÓ 0.3
Si E i F són espais vectorials sobre K, una aplicació $f : E \to F$ direm que és lineal si es verifiquen les condicions:

1) $f(x + y) = f(x) + f(y)$, per tots $x, y \in E$. (additivitat)

2) $f(ax) = af(x)$, per tot $x \in E$ i tot $a \in K$. (homogeneïtat de grau 1)

Si f és lineal i $E = F$, direm que f és un endomorfisme de E.
Si f és lineal i injectiva direm que f és un monomorfisme.
Si f és lineal i exhaustiva direm que f és un epimorfisme
Si f és lineal i bijectiva direm que f és un isomorfisme. Un endomorfisme bijectiu direm que és un automorfisme.

Comentari: Demostrau que a la definició 0.3 les condicions 1) i 2) es poden substituir per l'única condició $f(ax + by) = af(x) + bf(y)$, per tots $x, y \in E$ i tots $a, b \in K$.

És important conèixer com són les aplicacions lineals entre els espais K^n i K^m. En aquest sentit, podem demostrar el següent resultat.

PROPOSICIÓ 0.2
Una aplicació $f : K^n \to K^m$ és lineal si i només si és de la forma

$$f(x_1, \ldots, x_n) = (a_{11}x_1 + \cdots + a_{1n}x_n, a_{21}x_1 + \cdots + a_{2n}x_n, \ldots, a_{m1}x_1 + \cdots + a_{mn}x_n)$$

on $a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{m1}, \ldots, a_{mn} \in K$.

Prova. Si $f : K^n \to K^m$ és lineal, siguin

$$f(1, 0, \ldots, 0) = (a_{11}, \ldots, a_{m1}),\ f(0, 1, \ldots, 0) = (a_{12}, \ldots, a_{m2}), \ldots, f(0, 0, \ldots, 1) = (a_{1n}, \ldots, a_{mn}).$$

Llavors

$$\begin{aligned} f(x_1, \ldots, x_n) &= f\Big((x_1, 0, \ldots, 0) + (0, x_2, \ldots, 0) + \cdots + (0, 0, \ldots, x_n)\Big) = \\ &= f(x_1, 0, \ldots, 0) + f(0, x_2, \ldots, 0) + \cdots + f(0, 0, \ldots, x_n) = \\ &= x_1 f(1, 0, \ldots, 0) + x_2 f(0, 1, \ldots, 0) + \cdots + x_n f(0, 0, \ldots, 1) = \\ &= (a_{11}x_1 + \cdots + a_{1n}x_n, a_{21}x_1 + \cdots + a_{2n}x_n, \ldots, a_{m1}x_1 + \cdots + a_{mn}x_n). \end{aligned}$$

El recíproc és de demostració immediata: Si f té la forma

$$f(x_1,\dots,x_n)=(a_{11}x_1+\cdots+a_{1n}x_n,a_{21}x_1+\cdots+a_{2n}x_n,\dots,a_{m1}x_1+\cdots+a_{mn}x_n),$$

llavors satisfà les dues condicions exigides de linealitat.

Observau que si $f(x_1,\dots,x_n)=(a_{11}x_1+\cdots+a_{1n}x_n,a_{21}x_1+\cdots+a_{2n}x_n,\dots,a_{m1}x_1+\cdots+a_{mn}x_n)$ i $g(x_1,\dots,x_n)=(b_{11}x_1+\cdots+b_{1n}x_n,b_{21}x_1+\cdots+b_{2n}x_n,\dots,b_{m1}x_1+\cdots+b_{mn}x_n)$, llavors $f=g$ si i només si $a_{ij}=b_{ij}$ per tot $i=1,\dots,m;j=1,\dots,n$. ■

Si indicam per $L(K^n,K^m)$ el conjunt de les aplicacions lineals entre K^n i K^m, podem establir l'aplicació $\mu:L(K^n,K^m)\to M_{m\times n}(K)$ que fa correspondre a cada $f\in L(K^n,K^m)$, $f(x_1,\dots,x_n)=(a_{11}x_1+\cdots+a_{1n}x_n,a_{21}x_1+\cdots+a_{2n}x_n,\dots,a_{m1}x_1+\cdots+a_{mn}x_n)$, la matriu de $M_{m\times n}(K)$

$$A=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{m1}&\cdots&a_{mn}\end{pmatrix} \tag{1}$$

PROPOSICIÓ 0.3
L'aplicació $\mu:L(K^n,K^m)\to M_{m\times n}(K)$ definida just abans és bijectiva.

Siguin E i F dos $K-$e.v. i $f:E\to F$ una aplicació lineal. Suposem també que $\dim E=n\geq 1$ i $\dim F=m\geq 1$. Sigui $\{e_1,\dots,e_n\}$ una base ordenada de E i $\{v_1,\dots,v_m\}$ una base ordenada de F. Pert tant, pel resultat anterior, sabem que f està determinada per llurs imatges sobre la base donada: si $f(e_j)=a_{1j}v_1+a_{2j}v_2+\ldots+a_{mj}v_m, j=1,\dots,n$, llavors podem construir la matriu $A=(a_{ij})$ de tipus $m\times n$, que explícitament tendrà la forma de la matriu donada a (1).

Observau que a la primera columna de A hi ha les coordenades de $f(e_1)$ respecte de la base $\{v_1,\dots,v_m\}$, i així successivament per a les altres columnes. Així l'element a_{ij} de la matriu A és la $i-$èsima coordenada del vector $f(e_j)$ respecte de la base $\{v_1,\dots,v_m\}$. Direm que A és la matriu de f respecte de les bases fixades. És clar que així ens queda definida una correspondència entre $L(E,F)$ i $M_{m\times n}(K)$: a cada aplicació lineal $f\in L(E,F)$ li associam la seva matriu; aquesta correspondència és bijectiva: a tota matriu $A\in M_{m\times n}(K)$ li correspon una única aplicació lineal $f\in L(E,F)$ que té per matriu A. Direm que aquesta f és l'aplicació lineal determinada per A.

EXEMPLES 2

(a) Considerem l'aplicació lineal $f:\mathbb{R}^3\to\mathbb{R}^2$, definida per $f(x,y,z)=(2x+3y+z,-x+y)$. La seva matriu és

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

(b) $h(x,y,z)=(y,x)$. La matriz de h és

$$\begin{pmatrix}0&1&0\\ 1&0&0\end{pmatrix}.$$

(c) L'aplicació $f:\mathbb{R}^3\to\mathbb{R}^2$ definida per $f(x,y,z)=(x+5y,x+y+1)$ no és lineal.

(d) L'aplicació $f(x,y,z)=(x^2+y,x+y)$ tampoc no és lineal.

(e) L'aplicació $f:\mathbb{R}_2[x]\to\mathbb{R}^2$ definida per $f(a_0+a_1x+a_2x^2)=(a_0+a_2,a_1)$ si és una aplicació lineal. La seva matriu, si consideram les bases canòniques d'ambdós espais, la calculam de la següent manera:

$$\begin{aligned}f(1)&=(1,0)=1\cdot(1,0)+0\cdot(0,1),\\ f(x)&=(0,1)=0\cdot(1,0)+1\cdot(0,1),\\ f(x^2)&=(1,0)=1\cdot(1,0)+0\cdot(0,1).\end{aligned}$$

Per tant, la seva matriu associada és: $\begin{pmatrix}1&0&1\\ 0&1&0\end{pmatrix}$.

En el cas $E = F$, basta utilitzar una base. Això és el que farem si no deim res en contra.

PROPOSICIÓ 0.4
La correspondència definida entre $L(E,F)$ i $M_{m\times n}(K)$ a més de ser bijectiva, conserva les operacions vectorials de cada espai.

Això vol dir que $L(E,F)$ i $M_{m\times n}(K)$ són isomorfs i, per tant, $\dim L(E,F) = \dim M_{m\times n}(K) = mn$.

PROPOSICIÓ 0.5
Sigui $f \in L(E,F)$ amb matriu associada A respecte d'unes bases $\{e_1,\dots,e_n\}$ i $\{v_1,\dots,v_m\}$. Es verifica $\operatorname{rang} f = \operatorname{rang} A$.

Prova. En efecte, tenim

$$\operatorname{rang} f = \dim \operatorname{Im} f = \dim \langle f(e_1),\dots,f(e_n)\rangle = \dim \langle \sum a_{i1}v_i,\dots,\sum a_{in}v_i\rangle =$$
$$\dim \langle (a_{11},\dots,a_{m1}),\dots,(a_{1n},\dots,a_{mn})\rangle = \operatorname{rang} A.$$

Observau que feim ús de l'isomorfisme $\sigma : F \to K^m$ que transforma cada vector de F en les seves coordenades respecte de la base $\{v_1,\dots,v_m\}$. Evidentement es verifica

$$\sigma(\langle \sum a_{i1}v_i,\dots,\sum a_{in}v_i\rangle) = \langle (a_{11},\dots,a_{m1}),\dots,(a_{1n},\dots,a_{mn})\rangle$$

i, per tant, $\dim \langle \sum a_{i1}v_i,\dots,\sum a_{in}v_i\rangle = \dim \langle (a_{11},\dots,a_{m1}),\dots,(a_{1n},\dots,a_{mn})\rangle$. ■

Si $A = (a_{ij})$ és la matriu de $f : E \to F$ respecte de les bases $\{e_1,\dots,e_n\}$ i $\{v_1,\dots,v_m\}$, llavors si $x \in E$ té coordenades $(x_1,\dots,x_n)$ respecte de la base $\{e_1,\dots,e_n\}$, les coordenades $(y_1,\dots,y_m)$ de $f(x)$ respecte de la base $\{v_1,\dots,v_m\}$ es poden calcular fent el producte de la matriu A per la matriu columna de les coordenades $x_1,\dots,x_n$:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Aquesta equació, que abreujadament podem escriure $Y = AX$, li direm equació matricial de f (respecte de les bases fixades).

Un resultat important en aquest tema és el següent:

PROPOSICIÓ 0.6 (MATRIU DE LA COMPOSICIÓ DE DUES APLICACIONS LINEALS)
Siguin $f : E \to F$ i $g : F \to G$ aplicacions lineals. Siguin $\{e_1,\dots,e_n\},\{v_1,\dots,v_m\}$ i $\{u_1,\dots,u_s\}$ bases de E, F i G respectivament. Siguin A, B i C les matrius de f, g i $g\circ f$ respecte d'aquestes bases. Aleshores $C = BA$.

Cal recordar aquí com es defineix el producte de dues matrius $B = (b_{ij})$ i $A = (a_{ij})$ de tipus $s\times m, m\times n$ respectivament: els elements del producte diguem-li $C = (c_{ij})$ es calculen així

$$c_{ij} = \sum_{p=1}^{m} b_{ip}a_{pj}, \quad i = 1,\dots,s; j = 1,\dots,n.$$

Observau que la matriu producte C és de tipus $s \times n$. Observau també que dues matrius es poden multiplicar si el nombre de columnes de la matriu de l'esquerra coincideix amb el nombre de files de la matriu de la dreta. És clar que en el conjunt $M_{n\times n}(K)$ el producte de matrius és una operació interna. En general, aquesta operació no és commutativa: $AB \neq BA$, però, com veurem ara és associativa.

PROPOSICIÓ 0.7
El producte de matrius és associatiu, és a dir $C(BA) = (CB)A$.

Prova. En efecte, això és causa que una vegada associades aplicacions lineals a cada matriu (s'han de fixar espais vectorials de dimensions adequades a la mida de les matrius i de les bases a cada espai), sabem que $h\circ(g\circ f) = (h\circ g)\circ f$ i pel resultat anterior podem escriure $C(BA) = (CB)A$. ■

Del que acabam de dir es pot extreure que el conjunt $M_{n\times n}(K)$ de les matrius quadrades d'ordre n sobre un cos K, a més de tenir estructura vectorial, és també un anell unitari (no commutatiu) que pel que hem vist és isomorf (fixada una base) a l'anell $L(E,E)$, on E és un $K-$e.v. de dimensió n.

DEFINICIÓ 0.4
Si $A \in M_{n\times n}(K)$, direm que és invertible si existeix una altra matriu B (també de $M_{n\times n}(K)$) tal que $AB = BA = I$ (I és la matriu identitat $n \times n$).

Matriu regular o no singular són sinònims de matriu invertible. Sovint indicarem per $MR_{n\times n}(K)$ el conjunt de les matrius regulars $n\times n$ sobre K. En cas d'existir la matriu B, aquesta és única i l'anomenam la inversa de A, i escriurem $B = A^{-1}$.

EXEMPLE 3: *La matriu 2×2 de nombres reals $A = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$ és invertible, ja que plantejada l'equació*

$$\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

resulta que té solució, aquesta és $B = \begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}$.

En canvi, la matriu $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ no és invertible ja que la condició $AB = BA = I$ condueix a un sistema d'equacions lineals que és incompatible.

PROPOSICIÓ 0.8
Si A i B són invertibles, llavors AB també és invertible i es verifica $(AB)^{-1} = B^{-1}A^{-1}$.

De la proposició anterior es dedueix que el conjunt $MR_{n\times n}(K)$ és un grup no commutatiu amb la multiplicació.

DEFINICIÓ 0.5 (MATRIU D'UN CANVI DE BASE)
Siguin $\{e_1,\dots,e_n\}$ i $\{e'_1,\dots,e'_n\}$ bases d'un espai vectorial E. Podem escriure

$$e'_j = \sum_{i=1}^{n} p_{ij}e_i.$$

Direm que $P = (p_{ij})$ és la matriu del canvi de base (de la base (e) a la base (e')).

Anàlogament, podem escriure

$$e_j = \sum_{i=1}^{n} q_{ij}e'_i.$$

Direm que $Q = (q_{ij})$ és la matriu del canvi de base (de la base (e') a la base (e)).

PROPOSICIÓ 0.9
Les matrius P i Q definides a la definició anterior són inverses una de l'altra.

Prova. En efecte, sigui l'esquema

$$E \xrightarrow{id} E \xrightarrow{id} E$$

i considerem a cada espai les bases $\{e_1,\dots,e_n\}$, $\{e'_1,\dots,e'_n\}$ i $\{e_1,\dots,e_n\}$ respectivament. Llavors és clar que les matrius de id respecte de les bases assenyalades són Q i P, per tant es compleix $I = PQ$. Igualment s'obté $I = QP$. ■

PROPOSICIÓ 0.10
Sigui E un $K-$e.v. i $\{e_1, \ldots, e_n\}$ una base de E i $f : E \to E$ l'aplicació lineal que correspon en la base fixada a la matriu $A \in M_{n\times n}(K)$. Llavors, f és bijectiva si, i només si, A és invertible.

Prova. En efecte, si f és bijectiva llavors $\{f(e_1), \ldots, f(e_n)\}$ és també una base de E i, per tant, A és la matriu d'un canvi de base i segons la proposició anterior és invertible. Recíprocament, si A és invertible existeix B tal que $AB = BA = I$. Si g és l'endomorfisme que correspon a la matriu B, llavors podem escriure $f \circ g = g \circ f = id$, i per tant f és bijectiva. ■

PROPOSICIÓ 0.11
Sigui E un $K-$e.v i $\dim E = n$. Llavors el grup lineal $GL(E)$ és isomorf al grup $MR_{n\times n}(K)$ de les matrius invertibles.

PROPOSICIÓ 0.12
Sigui A una matriu quadrada $n \times n$. A és invertible si, i només si, $\operatorname{rang} A = n$.

Prova. En efecte, sabem que A és invertible si, i només si, l'endomorfisme associat f (fixada una base) és bijectiu, i això és així si, i només si, $\operatorname{rang} f = n$. Però $\operatorname{rang} f = \operatorname{rang} A$. ■

Un altre resultat important és el que ens diu com canvia la matriu d'una aplicació lineal quan es fa un canvi de bases.

PROPOSICIÓ 0.13
Sigui $f : E \to F$ una aplicació lineal amb matriu A respecte de les bases $\{e_1, \ldots, e_n\}$ i $\{v_1, \ldots, v_m\}$, i amb matriu B respecte de les bases $\{e'_1, \ldots, e'_n\}$ i $\{v'_1, \ldots, v'_m\}$. Considerem f com la composició següent

$$E \xrightarrow{id_E} E \xrightarrow{f} F \xrightarrow{id_F} F$$

i considerem a cada un dels espais les bases $\{e'_1, \ldots, e'_n\}, \{e_1, \ldots, e_n\}, \{v_1, \ldots, v_m\}$ i $\{v'_1, \ldots, v'_m\}$ respectivament. En aplicar el resultat vist anteriorment, resulta $B = Q^{-1}AP$, on $P = (p_{ij})$ és la matriu del canvi de base (e) a (e'), i Q la matriu del canvi (v) a (v').
En el cas $E = F$, la fórmula ens queda més simple: $B = P^{-1}AP$.

Una altra qüestió que hem de resoldre és la següent: si en un espai vectorial es fa un canvi de base amb matriu de canvi $P = (p_{ij}), e'_j = \sum_{i=1}^{n} p_{ij}e_i$, com canvien les coordenades d'un vector qualsevol d'aquest espai? La reposta és clara:

PROPOSICIÓ 0.14
Sigui x un vector, i siguin X, X' les matrius columna de les coordenades de x respecte de les bases $\{e_1, \ldots, e_n\}$ i $\{e'_1, \ldots, e'_n\}$, aleshores es verifica $X = PX'$ o, també, $X' = P^{-1}X$.

Per acabar aquesta secció estudiarem la transposició de matrius.

DEFINICIÓ 0.6
Si $A \in M_{m\times n}(K)$, anomenam transposada de A, A^T, a la matriu que té per files les columnes de A : $A^T = (b_{ij})$ on $b_{ij} = a_{ji}, i = 1, \ldots, n, j = 1, \ldots, m$.

Així aquesta operació (unària) ens defineix una aplicació $M_{m\times n}(K) \to M_{n\times m}(K)$ amb les propietats següents.

PROPOSICIÓ 0.15
1) L'aplicació transposada és bijectiva.

2) És involutiva: $(A^T)^T = A$.

3) $(A + B)^T = A^T + B^T$; $(aA)^T = aA^T$.

DEFINICIÓ 0.7
Una matriu $A \in M_{n\times n}(K)$ deim que és ortogonal si es verifica $A \cdot A^T = A^T \cdot A = I$. És a dir, si és invertible i la seva inversa coincideix amb la transposada: $A^{-1} = A^T$.

PROPOSICIÓ 0.16
El conjunt de les matrius ortogonals, $MO_{n\times n}(K)$, amb l'operació de multiplicació és un grup, que anomenam grup ortogonal.

0.5 Equacions lineals. Varietats lineals

Una equació lineal amb n incògnites sobre un cos K és una equació del tipus $a_1x_1 + \ldots + a_nx_n = b$, on $a_1, \ldots, a_n, b \in K$.

Una solució de l'equació és una $n-$pla $(x_1, \ldots, x_n) \in K^n$ que satisfà la igualtat. A $a_1, \ldots, a_n$ els direm els coeficients de les incògnites i b és el terme independent. Resoldre una equació lineal vol dir trobar-li totes les solucions. Una equació direm que és compatible si té alguna solució, i incompatible en cas contrari. Una equació amb una única solució és determinada, i amb més d'una solució és indeterminada. Finalment, si $b = 0$, l'equació és homogènia.

EXEMPLE 4: *Si $K = \mathbb{R}$, l'equació $2x + y - 3z = 1$ és compatible indeterminada. El conjunt de solucions és de la forma $(0, 1, 0) + \langle(1, -2, 0), (0, 3, 1)\rangle$. Recordem que aquest conjunt, suma d'un vector i un sub-e.v., l'anomenam varietat lineal. Cal observar també que $(0, 1, 0)$ és una solució (particular) de l'equació $2x + y - 3z = 1$, i el sub-e.v. $\langle(1, -2, 0), (0, 3, 1)\rangle$ és el conjunt de solucions de l'equació homogènia $2x + y - 3z = 0$.*

Un sistema de m equacions lineals amb n incògnites sobre un cos K és

$$\begin{aligned} &a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ &a_{21}x_1 + \ldots + a_{2n}x_n = b_2 \\ &\vdots \\ &a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{aligned}$$

on $a_{ij}, b_i \in K$ per tot $i = 1, \ldots, m; j = 1, \ldots, n$.

Una solució del sistema és un vector $(x_1, \ldots, x_n) \in K^n$ que és solució de totes i cada una de les equacions que formen el sistema. Per altra part, traslladam el mateix vocabulari utilitzat per una equació lineal al cas de sistemes: coeficients, etc. Cal observar que un sistema pot ser escrit en forma matricial:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Aquesta representació matricial ens dóna la idea de poder escriure un sistema d'equacions lineals mitjanant una única equació (lineal) vectorial. Per això, sigui A la matriu formada pels coeficients de les incògnites, és a dir:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

i sigui $f : K^n \to K^m$ l'aplicació lineal associada a la matriu A respecte de les bases canòniques. Indicam per $x = (x_1, \ldots, x_n) \in K^n$ el vector incògnita i per $b = (b_1, \ldots, b_m) \in K^m$ el vector de termes independents. Així el sistema pot ser escrit en la forma $f(x) = b$, i del que es tracta ara és de veure si el sistema és compatible o no i, en cas que sigui compatible, resoldre'l (trobar-li totes les solucions). Per començar, és clar que el sistema és compatible (existeix $x \in K^n$ tal que $f(x) = b$) si, i només si,

$b \in \operatorname{Im} f$, però això equival a la condició $b \in \langle f(u_1), \ldots, f(u_n)\rangle$ on $\{u_1, \ldots, u_n\}$ és la base canònica de K^n. Però també $b \in \langle f(u_1), \ldots, f(u_n)\rangle$ equival a $\dim \langle f(u_1), \ldots, f(u_n)\rangle = \dim \langle f(u_1), \ldots, f(u_n), b\rangle$, el que amb altres paraules equival a dir

$$\operatorname{rang} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} = \operatorname{rang} \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ a_{21} & \cdots & a_{2n} & b_2 \\ \vdots & & & \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix}$$

Hem demostrat, doncs, el resultat fonamental següent:

Teorema 0.1 (Teorema de Rouché, 1832-1910))
Un sistema d'equacions lineals és compatible (té alguna solució) si, i només si, la matriu del sistema (matriu dels coeficients de les incògnites) i la matriu ampliada (afegint a l'anterior la columna de termes independents) tenen el mateix rang. En aquest cas, direm que aquest rang comú de les dues matrius és el rang del sistema.

Suposem ara que tenim un sistema que és compatible de rang igual a r. Vegem com són les solucions d'aquest sistema.

Proposició 0.17
Sigui $x_0 \in K^n$ una solució particular del sistema $f(x) = b$, és a dir, $f(x_0) = b$. Vegem que el conjunt $S = \{x \in K^n; f(x) = b\}$ de les solucions és $S = x_0 + \operatorname{Nuc} f$.

Prova. És clar que qualsevol vector de la forma $x_0 + t$, amb $t \in \operatorname{Nuc} f$ és solució ja que $f(x_0 + t) = f(x_0) + f(t) = b + 0 = b$.

Recíprocament, si x és una solució, llavors de $f(x) = b$ i $f(x_0) = b$ en podem deduir $f(x - x_0) = 0$, és a dir $x - x_0 \in \operatorname{Nuc} f$ o sigui $x \in x_0 + \operatorname{Nuc} f$. ■

Proposició 0.18
Si $f(x) = b$ és un sistema compatible amb S com a conjunt de solucions, llavors $|S| = |\operatorname{Nuc} f|$.

Prova. Es tracta de veure que els conjunts S i $\operatorname{Nuc} f$ són equipotents. Basta demostrar que l'aplicació $\theta : \operatorname{Nuc} f \to S$ definida per $\theta(y) = x_0 + y$ és bijectiva. ■

Definició 0.8
Sigui $f(x) = b$ un sistema compatible amb S com a conjunt de solucions. Direm que és determinat si $|S| = 1$ (té una única solució). En cas contrari $|S| > 1$ (té més d'una solució) direm que és indeterminat.

Proposició 0.19
Si un sistema és compatible de rang r, el conjunt de llurs solucions és una varietat lineal de dimensió igual a $n - r$. Així, el sistema serà determinat si, i només si, $r = n$; i serà indeterminat si, i només si, $r < n$. En aquest darrer cas, direm que el grau d'indeterminació del sistema és $n - r$.

Proposició 0.20
Sigui $f(x) = b$ un sistema compatible indeterminat de rang r. El sistema té infinites solucions si i només el cos K és infinit.

Prova. Si K és finit, llavors K^n és finit i el conjunt S de solucions del sistema també ho serà perquè $S \in K^n$. Suposem ara que K és infinit. Sabem $|S| = |\operatorname{Nuc} f|$, i per altra part $\dim \operatorname{Nuc} f = n - r$, per tant $|\operatorname{Nuc} f| = |K^{n-r}|$. Finalment K^{n-r} és infinit i S també. ■

PROPOSICIÓ 0.21
Si un sistema $f(x) = b$ sobre un cos finit de cardinal q és compatible de rang r, llavors aquest sistema té exactament q^{n-r} solucions.

Prova. Basta aplicar la proposició anterior: $|S| = |\text{Nuc } f| = |K^{n-r}| = q^{n-r}$. ■

EXEMPLE 5: *Sigui $f(x) = b$ un sistema 4×5 sobre $\mathbb{Z}_5$ compatible de rang igual a 3. Tenim $|S| = |\text{Nuc } f| = |Z_5|^{5-3} = 5^2 = 25$. El sistema té 25 solucions.*

Comentari: Òbviament, qualsevol sistema homogeni ($b = 0$) és compatible. El conjunt de les seves solucions és un subespai vectorial de K^n que té dimensió $n - r$.

EXEMPLES 6

(a) El sistema d'equacions lineals sobre $\mathbb{R}$:

$$\begin{aligned} x + y + z &= 0 \\ y - z &= 1 \end{aligned}$$

*és compatible (els rangs de les matrius són 2 i 2) i indeterminat (*rang $= 2 <$ *nombre d'incògnites = 3), amb grau d'indeterminació 3 - 2 = 1.*

Observau que $(-1, 1, 0)$ és una solució del sistema. El conjunt de totes les solucions és $S = (-1, 1, 0) +$ Nuc $f = (-1, 1, 0) + \langle(-2, 1, 1)\rangle$. Notau que calcular Nuc f *és el mateix que resoldre el sistema homogeni associat al sistema donat:*

$$\begin{aligned} x + y + z &= 0 \\ y - z &= 0. \end{aligned}$$

(b) El sistema d'equacions lineals sobre $\mathbb{R}$:

$$\begin{aligned} x + y &= 0 \\ x - y &= 1 \\ -x + 2y &= 0 \end{aligned}$$

és incompatible ja que el rang de la matriu dels sistemes és 2 i el de la matriu ampliada és 3. Naturalment això es pot veure directament sobre les equacions: de la primera i tercera es dedueix $x = y = 0$, valors que no satisfan la segona equació.

Per acabar aquest apartat, vegem que tota varietat lineal és el conjunt de solucions d'un sistema d'equacions lineals.

PROPOSICIÓ 0.22 (REPRESENTACIÓ DE VARIETATS LINEALS))
Sigui $V = x_0 + F$ una varietat lineal de K^n. Existeix un sistema d'equacions lineals sobre K amb n incògnites, $f(x) = b$, tal que el conjunt de les seves solucions és V.

Prova. Sigui $\{e_1, \ldots, e_s\}$ una base de F (suposam $F \neq \{0\}$), sigui $\{e_1, \ldots, e_s, e_{s+1}, \ldots, e_n\}$ una base de K^n i siguin $v_{s+1}, \ldots, v_n \in K^m$ linealment independents (hem de triar, doncs, $m \geq n - s$). Ara consideram $f : K^n \to K^m$ lineal tal que $f(e_1) = \ldots = f(e_s) = 0$ i $f(e_{s+1}) = v_{s+1}, \ldots, f(e_n) = v_n$. És clar que Nuc $f = F$. Per acabar basta definir $b = f(x_0)$; així el sistema $f(x) = b$ és compatible (x_0 és una solució particular), i el conjunt de solucions és $x_0 + \text{Nuc } f = x_0 + F = V$.

Observau que el rang del sistema construït és $n - \dim F$. ■

Comentari: D'acord amb la proposició anterior, per representar una varietat lineal de dimensió s ($s = \dim F$) necessitam com a mínim $n - s$ equacions. Així, per una recta (v.l. de dimensió 1) de $\mathbb{R}^3$ són necessàries com a mínim $3 - 1 = 2$ equacions. Per un pla (v.l. de dimensió 2), $3 - 2 = 1$ equació. Per una v.l. de dimensió 4 dins un espai de dimensió 7, necessitam com a mínim $7 - 4 = 3$ equacions.