Capítol 4, Estructures algebraiques

4.1 Grups

S'anomena **grup** a *una parella formada per un conjunt G i una operació ^ definida en G que compleixi aquestes tres condicions:*

^ *ha d'estar definida en G*
^ *ha d'ésser associativa*
^ *ha de tenir element neutre.*
^ *ha de tenir elements simètrics.*

Si a més d'aquestes propietats l'operació ^ és commutava al grup se'l anomena **grup commutatiu**, o també es diu **grup abelià**.

Exemples:

Les parelles (**Z**,+), (**Q**,+), (**R**,+) i (**C**,+) són grups commutatius. O sigui els conjunts d'enters, racionals, reals i complexos amb les seves respectives operacions suma són grups.

Altres exemples: Entendrem que **Q***, **R*** i **C*** són els conjunt **Q**, **R** i **C** anterior però sense el zero. Així, les parelles (**Q***, ·), (**R***,·) i (**C***, ·) són grups commutatius. Perquè s'ha tret el zero en aquests conjunt?. Per que a la llista no hi ha **Z**?.

Més exemples: Tots els vectors del pla amb l'operació suma de vectors. Tots els vectors de l'espai amb la suma de vectors. Totes les funcions definides en (a,b) amb l'operació suma de funcions. Totes les funcions bijectives definides entre (a,b) i (a,b) amb la composició de funcions. El conjunt de tots el polinomis amb la suma de polinomis. El conjunt de tots el polinomis, de grau màxim n, amb la suma de polinomis.

Uns exemples geomètrics: Hi ha alguns 'moviments' en el pla que amb l'operació composició de moviments formen grup, com passa amb: les translacions, els girs d'un mateix centre i les homotècies d'un mateix centre.

Un exemple clàssic és el format pel conjunt $\mathbf{R}^n$ (veure paràgraf 2.2) amb l'operació suma següent:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1+b_1, a_2+b_2, \ldots, a_n+b_n)$$

és immediat veure que aquesta operació és commutatita, que l'element neutre és el (0, 0, ... ,0), que el simètric de $(a_1, a_2, \ldots, a_n)$ és $(-a_1, -a_2, \ldots, -a_n)$, i que és associativa. Així ($\mathbf{R}^n$, +) és un grup commutatiu.

Un grup especial és el del conjunt que solament té un element, que haurà d'ésser l'element neutre, i l'operació és simplement 0+0 = 0. Es pot comprovar fàcilment que és un grup commutatiu.

Com a últim exemple de grup proposem el conjunt $\mathbf{Z}_n$, ja vist en molts paràgrafs anteriors, amb l'operació suma (vegeu 3.11) és un grup abelià. En canvi $\mathbf{Z}_n$ amb l'operació producte no ho és, ja que no té la propietat de tenir simètrics (o inversos, en aquest cas). Hi ha elements que no tenen inversos, el zero en tots els casos no té invers, però n'hi ha d'altres. per exemple, en $\mathbf{Z}_4$ el 2 no té invers. Ho podeu comprovar?

4.2 Aïllar canviant de signe

Suposarem que tenim una igualtat del tipus

$$x + a = b$$

I suposem que tots els tres termes que hi figuren són d'un grup (G, +). Com que *a* és del grup ha de tenir simètric *-a*. Com que els dos membres de l'equació són iguals, sumand a cada un *-a* ha de donar igual:

$$(x + a) - a = b - a$$

Com que en grup es compleix la propietat associativa:

$$x + (a - a) = b - a$$

Però operant un terme amb el seu simètric dóna l'element neutre i queda:

$$x + e = b - a$$

I com que sumant un element amb el neutre dóna el primer element:

$$x = b - a$$

Aquest procés es fa normalment d'una forma automàtica i es diu que *un terme es posar a l'altre banda de la igualtat canviant de signe*.

4.3 Subgrups

Si tenim un grup (G,#) i el conjunt G té *un subconjunt S que amb la mateixa operació # forma un grup per sí sol* es diu que (S,#) és un **subgrup** de (G,#)

Una condició necessària i suficient per què S subconjunt de G (grup amb l'operació #) sigui un subgrup és:

$$x, y \in S \Rightarrow x \# y^{-1} \in S \qquad (*)$$

O sigui, que per qualsevol parell d'elements de S, la operació d'un d'ells per simètric de l'altre ha de pertànyer sempre a S.

O dit d'una altre forma, si S és subconjunt d'un grup (G,#), que es compleix:

$$S \text{ és } grup \quad \Leftrightarrow \quad (x, y \in S \Rightarrow x \# y^{-1} \in S) \qquad (**)$$

La demostració de la implicació =>, cap a la dreta, és trivial i la deixem pel lector.

Per veure que es compleix la implicació cap a l'esquerra s'ha de demostrar que S és un grup, o sigui, s'ha de demostrar que l'operació # compleix amb les 4 propietats de grup (4.1), tenint en compte que és certa la condició de la dreta de la implicació (**).

Agafem un element *x*, qualsevol de S, com que *x,x* ε S, es complirà que $x\#x^{-1} = e \in S$. Així es compleix la propietat 3 de grup.

Com que ja sabem que *e* és de S, considerem els dos elements *e* i *x* de S, s'ha de complir que $e\#x^{-1} = x^{-1} \in S$, que demostra la propietat 4.

Si tenim x,y de S, també ho seran *x* i y^{-1}, i per això, $x \# (y^{-1})^{-1} = x \# y \in S$, que és la primera condició de grup.

Falta solament veure la segona propietat. Però aquesta és una propietat general de tot el conjunt G, i també s'ha de complir en S.

I d'aquesta forma queda demostrada l'equivalència de les dues proposicions.

Exemples: S'ha vist que les parelles (**Z**,+), (**Q**,+), (**R**,+) i (**C**,+) són grups, és obvi veure si *x* i *y* són elements de **Z**, el resultat de *x* - *y* també serà de **Z** i com que **Z** està inclòs en **Q**, resulta que (**Z**, +) és un subgrup de (**Q**, +). Exactament el mateix passa per (**Q**, +) i (**R**, +) respecta de (**R**, +) i (**C**, +) respectivament.

Tots els vectors del pla forma un subgrup dels vectors de l'espai amb l'operació suma. Totes les funcions contínues en (a,b) amb l'operació suma de funcions, formen un subgrup de totes les funcions en general, definides en (a,b). Amb la suma usual, els enters formen un subgrup del racionals, i aquest formen un subgrup del real, i aquests dels complexos.

Ja s'ha dit, paràgraf anterior, que els polinomis de grau com a màxim n, que anotem $\mathbf{P}_n$, junt amb la suma formen un grup, i que els polinomis en general, que anotem **P**, amb la suma, també ho són. Anem a demostrar que $\mathbf{P}_n$ és subgrup de **P**.

Per fer-ho, haurem de demostrar que es compleix la implicació anterior (*):

$a_0+a_1x+a_2x^2+ ... +a_nx^n$ i $b_0+b_1x+b_2x^2+ ... +b_nx^n$ pertanyen a $\mathbf{P}_n$

la suma d'un amb el simètric de l'altre dóna

$(a_0+a_1x+a_2x^2+ ... +a_nx^n) + (-b_0-b_1x-b_2x^2- ... -b_nx^n) = (a_0+ b_0)+(a_1+ b_1)x+(a_2+ b_2)x^2+ ..... +(a_n+ b_n) x^n$

que també és un polinomi de $\mathbf{P}_n$ tal com demana la implicació (*). I amb això queda acabada la demostració de que $\mathbf{P}_n$ és subgrup de **P**.

4.4 Anells

S'anomena **anell** a *una terna ordenada formada per un conjunt A i dues operacions (+, ·) que compleixin aquestes cinc condicions*

1. *Les dues operacions han d'estar definides en A*
2. *El parell (A,+) ha d'ésser un grup commutatiu.*
3. *L'operació · ha d'ésser associativa*
4. *L'operació · ha de tenir element neutre, que en aquest cas es diu unitat.*
5. *L'operació · és distributiva respecta de la +*

Fixeu-vos que un anell és una terna, són tres elements alhora. Les operacions les hem indicat per + i · per ser les habituals, però no tenen perquè coincidir amb la suma i el producte coneguts.

A l'operació + d'un anell se li sol dir **primera operació**, o a vegades **operació sumativa** de l'anell. L'operació · se li diu **segona operació**, o també, **operació multiplicativa**.

Encara que l'element neutre i l'element unitat no siguin nombres, és usual indicar per un 0 a l'element neutre i per un 1 a l'element unitat.

Si la segona operació d'un anell fos commutativa es diu que l'**anell** és **commutatiu**.

S'ha de fer notar que entre les condicions exigides per ser anell no hi figura que la segona operació tingui elements inversos, per això, en un anell hi poden haver elements que no tenen invers. Als elements d'un anell que tenen invers es diuen elements **invertibles**.

A vegades no s'exigeix la propietat 4 per ser anell, i es distingeix un anell (sense l'exigència de la propietat 4) d'un **anell amb unitat** (amb la propietat 4).

4.5 Exemples d'anells

Examinen el primer exemple: (**Z**, +, ·). Les operacions + i · estan perfectament definides en **Z** (propietat 1). Ja s'ha vist que (**Z**, +) és un grup commutatiu (propietat 2). El producte d'enters és associatiu (propietat 3). L'element unitat del producte és l'1, que és enter (propietat 4). I el producte és distributiu respecte de la suma (propietat 5).

De la mateixa forma es veu que (**Q**, +, ·), (**R**,+, ·) i (**C**, +, ·) són també anells

La terna (**N**, +, ·) formada pels nombres natural amb la suma i el producte no és un anell, ja que, tot i complint la propietat 1, no compleixen la 2, doncs (**N**, +) no és un grup.

Si designem per **P** al conjunt de tots els polinomis, la terna (**P**, +, ·) és un anell. Les operacions + i · estan definides entre polinomis. (**P**, +) és un grup commutatiu. El producte de polinomis és associatiu. El producte té element unitat, és el polinomi 1. I finalment el producte és distributiu respecte de la suma.

El conjunt $\mathbf{P}_n$ dels polinomis de grau màxim n no pot ser un anell amb les operacions normals de suma i producte de polinomis, ja que el producte no és una operació definida en el conjunt $\mathbf{P}_n$, doncs multiplicant dos polinomis de grau menor o igual a n no sempre dóna menor o igual a n.

Si F indica al conjunt de totes les funcions definides en (a,b) i considerant les operacions normals de suma i producte de funcions

$$(f+g)(x) = f(x) + g(x)$$
$$(f\cdot g)(x) = f(x)\cdot g(x)$$

tindrem que (F ,+ , ·) és un anell. Les operacions estan ben definides. La parella (F ,+) és un grup commutatiu (vist en 4.1). La funció que $f(x)$ =1 per a qualsevol x, és la funció unitat. El producte de funcions és associatiu i és distributiu respecte de la suma.

Considerem el conjunt Fc format per totes les funcions contínues i definides en (a,b). Com que aquest és un subconjunt del conjunt F. Hem de comprovar que si *f* i *g* pertanyen a Fc , també ho ha de fer *f-g*, cosa que és coneguda (la resta de dues funcions contínues és contínua). Amb això s'ha vist que Fc és un grup. La funció, que $f(x)$=1 per a qualsevol *x,* és contínua, per això Fc té element unitat. Les altres propietats com que es compleixen a tot F també es compliran en un subconjunt Fc.

Igual consideració ho podríem fer per les funcions derivables, que ho deixem pel lector.

El conjunt **Z**n amb les seves operacions suma i producte formen un anell, solament cal repassar els exemples dels paràgrafs del 3.11 al 3.17 on hi ha explicades totes les propietats que calen per formar anell.

4.6 Elements invertibles a Zn

Veurem una propietat interessant dels anells **Z**n: *Un element **a** té invers en **Z**n si i solament si **a** ési primer amb **n**.*

Per demostrar-ho procedirem en dues parts, la primera veurem que si ***a*** és primer amb ***n***, aleshores ***a*** té invers:

> Triem un ***a*** ε **Z**n, de forma que ***a*** i ***n*** siguin primers entre sí (recordeu que m.c.m.(***a,n***)=***an***). Suposem que hi ha un element ***x*** de **Z**n que ***ax***=0. Aquesta igualtat traduïda a **Z** queda ***ax*** = ***kn*** (la classe del 0 són tots els múltiples de n). Ens trobem per un costat que ***x*** ha d'ésser menor que ***n***, ja que ***x*** és de **Z**n. Però, per l'altre costat, el m.c.m.(***a,n***) és ***an***, això ens diu que ***x***, o bé, és ***n***, o bé, és zero. D'on es dedueix que ***x*** ha d'ésser 0.
>
> Hem vist que *si **a** és primer amb **n**, no hi pot haver cap valor **x**, diferent de 0, a **Z**n, que **a.x** = 0.*
>
> Suposem, ara que hi ha dos valors ***x*** i ***y***, a **Z**n que **ax = ay**, és clar que ***ax-ay*** = 0, o que ***a(x-y)*** = 0. Però pel que hem vist en el punt de sobre ha d'ésser ***x-y*** = 0, o ***x = y***.
>
> Acabem de veure que, *si **a** és primer amb **n**, no hi pot haver dins **Z**n dos valors diferents que multiplicats per **a** donin el mateix resultat*.
>
> Pel que s'ha vist, la sèria de productes ***a***·0, ***a***·1, ***a***·2, ***a***·3, ... , ***a***·(***n***-1) han de donar valors diferents, però tots han d'estar entre 0 i n-1, ja que sòn de **Z**n. O sigui els dos conjunts {***a***·0, ***a***·1, ..., ***a***·(***n***-1)} i {0,1, ... ,***n***-1} són iguals. D'aquí es desprèn que hi ha algun element en el primer conjunt que és igual a 1, algun element ***x*** que
>
> $$ax = 1$$
>
> evidentment, l'element ***x*** és l'invers d'***a*** dins **Z**n. I així s'acaba la primera part

En la segona part, demostrarem que si ***a*** no és primer amb ***n***, ***a*** no té invers.

> Si ***a*** no és primer amb ***n***, és que m.c.m.(***a,n***)<***an***, el que vol dir que existeixen dos enters ***x*** i ***y*** que ***ax = ny***, però a més, 0<***x***<***n***. Això ens diu que en **Z**n, ***ax*** =0.
>
> Suposem (per reducció a l'absurd) que ***a*** és invertible, això vol dir que en **Z**n hi ha un ***z*** que ***az*** = 1, però si li restem la igualtat anterior (***ax*** =0) tindrem que ***a(z-x)*** = 1. Cosa que diu que ***z-x*** també és l'invers de **a**. Segons el que hem vist en el paràgraf 3.15, en una operació associativa solament hi pot haver un invers, per això, ***z*** = ***z-x***, o sigui que ***x*** ha d'ésser 0, que no és cert, tal com s'ha vist més amunt. Per això la suposició que s'ha fet és falsa, ***a*** no és invertible. I s'acaba la segona part.

Per exemple en Z_6, els valors 0, 2, 3 i 4 no són invertibles, en canvi l'1 i el 5 sí que ho són.

4.7 Propietats que es compleixen en un anell

Primera:

L'element neutre de la suma multiplicat per qualsevol element dóna el mateix element neutre

$$0 \cdot x = 0$$

La demostració és senzilla:

$$0x+x = 0x + 1x = (0+1)x = 1x = x$$

Si al primer membre i a l'últim d'aquestes igualtat se li suma el simètric de x:

$$(0x+x)-x = x-x \Rightarrow 0x+(x-x) = 0 \Rightarrow 0x = 0$$

Segona:

El producte del simètric de l'element unitat per qualsevol element dóna el simètric d'aquest element:

$$(-1) \cdot x = -x$$

es demostra fent:

$$(-1)x+x = (-1)x+1x = (-1+1)x = 0x = 0$$

I si la suma de dos elements dóna zero és que un és el simètric de l'altre, o sigui queda demostrada la propietat.

Tercera:

Sempre que l'anell tingui més d'un element, l'element neutre és diferent de l'element unitat

$$0 \neq 1$$

Agafem un element x qualsevol, diferent de zero, que ha d'existir ja que hi ha més d'un element. Suposem (per l'absurd) que el 0 és neutre i unitat a la vegada, es complirà

$0 \cdot x = x$, ja que 0 es unitat
$0 \cdot x = 0$, ho acabem de veure

d'on es dedueix que

$$0 \cdot x - 0 \cdot x = x$$

O sigui

$$0 = x$$

El que ens diu que si intentem agafar un element diferent de zero, no el trobem, sempre serà el zero, el que demostra la propietat.

4.8 Aïllar dividint

Suposem que tenim la igualtat

$$a \cdot x = b$$

que els termes són d'un anell (K, +, ·) i que a és un element invertible, per això existirà el seu invers a^{-1}. Multiplicant cada membre per a^{-1}, queda

$$a^{-1}.(a \cdot x) = a^{-1} \cdot b$$

Per la propietat associativa de la segona operació

$$(a^{-1} \cdot a) \cdot x = a^{-1} \cdot b$$

Però el producte d'un element pel seu invers dóna l'element unitat

$$1 \cdot x = a^{-1} \cdot b$$

Com que el producte d'elements unitat per un altre dóna aquest altre

$$x = a^{-1} \cdot b$$

Si l'operació de multiplicar és commutativa, el fet de multiplicar per l'invers es diu dividir i s'escriu en forma de trencat

$$x = \frac{b}{a}$$

Aquest procés es sol fer mecànicament i es diu passar un factor a l'altre banda dividint.

Penseu que el zero en els reals no és invertible, per això, passar un zero a dividir és una operació il·legal.

En els nombres enters solament hi ha l'1 i el -1 invertibles, per això si l'equació estigués en els enters no es podrien passa a dividir cap element diferents de l'1 i del -1.

4.9 Equacions diofàntiques

Una equació del tipus $ax + by = c$ es diu diofàntica si tots els seus termes, coeficients, terme independent i incògnites, són nombres enters.

Ens fixarem en les equacions diofàntiques que els coeficients *a* i *b* siguin primers entre sí. D'aquesta forma es pot assegurar que *a* és invertible en $\mathbf{Z}_b$ i també que *b* és invertible en $\mathbf{Z}_a$.

Si l'equació s'expressa en termes de $\mathbf{Z}_a$ queda

$$by = c$$

multiplicant per b^{-1} a cada banda

$$y = b^{-1}c$$

Que tornant a passar a $\mathbf{Z}$

$$y = b^{-1}c + ak$$

Essent *k* un enter qualsevol. Per cada valor enter de *k* tenim una solució per *y*. Per trobar la *x*, sols s'haurà de substituir la *y* en l'equació primera.

$$ax + b(b^{-1}c + ak) = c$$
$$ax = c - bb^{-1}c - abk$$
$$ax = c(1 - bb^{-1}) - abk$$

Com que bb^{-1} és igual a 1 a $\mathbf{Z}_a$, bb^{-1} és un múltiple de *a* més 1. O sigui, hi haurà un cert enter *d* que $bb^{-1} = ad+1$. I l'expressió quedarà

$$ax = -cad - abk$$
$$x = -cd - bk$$

Igualtat que expressa les solucions de *x* depenent, també, del paràmetre *k*. Amb aquest procés hem fet dues coses, una és la de demostrar que les equacions diofàntiques amb coeficients primers entre sí tenen infinites solucions, i l'altre, és el d'obtenir un mètode per solucionar-les.

4.10 Cossos

S'anomena **cos** a *un anell (K, +, ·) de forma que cada element a de K, diferents de l'element neutre 0, tingui invers per la segona operació ·.*

O sigui que en un cos els elements invertibles són tots els de K llevat de l'element neutre. Per això, si d'un cos K li traiem l'element neutre, cosa que ho indiquem com K*, ens queda que (K*, ·) és un grup commutatiu.

Les ternes (**Q**, +, ·), (**R**, +, ·) i (**C**, +, ·) són tres cossos, ja s'ha vist que són anells i és clar que tots el elements, no zeros, tenen invers dins del mateix conjunt. Com a conseqüència, tenim que (**Q***, ·), (**R***, +) i (**C***,+) són grups commutatius.

4.11 El cos (Zn, +, ·)

S'ha vist que (**Z**n, +, ·) és un anell, anem a veure que (**Z**n, +, ·) és cos només en el cas de que n sigui primer.

Pràcticament ja s'ha demostrat en el paràgraf 4.6, que diu, recordem-ho, que un element *a* té invers en **Z**n si, i només si, *a* és primer amb n.

Per ser un cos, acabem de dir que tots els elements diferents de 0 han de tenir invers, per això, per ser **Z**n cos tots els seus elements diferents de 0 han d'ésser primers amb n, des del 2 fins el n-1. O sigui n no pot ser dividit ni per 2, ni per 3, ..., ni per n-1. O sigui n ha d'ésser primer.

Per altre banda si n és primer tots el valors des del 2 fins l' n-1 seran primers amb n, per això tindran inversos. I com que també l'1 en té, **Z**n serà cos.

Conclusió: ***Z****n és un cos si, i solament si, n és primer*.

Les taules de sumar i multiplicar dels conjunts **Z**n són molt fàcils de construir ja que estan perfectament definides les operacions. Posarem aquí com exemples les taules de $\mathbf{Z}_3$ que és un cos i les de $\mathbf{Z}_4$ que no ho és.

$\mathbf{Z}_3$ +	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbf{Z}_3$ ·	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

Z_4 +	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Z_4 ·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

4.12 Espais vectorials

S'anomena **espai vectorial sobre K** a *una terna formada per un conjunt E, una operació +, i una operació externa ·, que compleixin aquestes condicions:*

1. *L'operació + ha d'estar definida en E*
2. *(E, +) ha d'ésser un grup commutatiu.*
3. *K ha de tenir dues operacions, que també es solen indicar per + i ·, de forma que (K, +, ·) sigui un cos.*
4. *L'operació externa · ha d'estar definida entre KxE i E; ·:KxE-----> E*
5. $r\cdot(s\cdot x) = (r\cdot s)\cdot x$
6. $(r + s)\cdot x = r\cdot x + s\cdot x$
7. $1\cdot x = x$
8. $r\cdot(x + y) = r\cdot x + r\cdot y$

Les quatre últimes propietats s'han de complir per qualsevol element x i y de E i per qualsevol r i s de K.

Als elements de E se'ls sol dir **vectors**, siguin quins siguin aquests elements. Pel sol fet de pertànyer a un espai vectorial se'l pot dir vector. Per altre banda, als elements de K, se'ls sol dir **escalars** o també **constants**.

Dins del concepte d'espai vectorial hi ha sortit dues operacions que s'han indicat pel signe +, a les dues se'ls sol dir que són sumes. Una està definida entre els vectors (elements de E) i l'altre està definida entre els escalars (elements de K). Per exemple a la propietat 6, la suma de l'esquerra està entre dos escalars, per això és una **suma d'escalars**, i l'operació de la dreta està entre dos vectors, per això és una **suma de vectors**.

En el concepte d'espai vectorial, també hi entren dues operacions (una interna i una externa) indicades pel símbol ·, a les dues se'ls sol indicar com a producte.

La que està definida en K és una operació definida entre escalar, i se li diu **producte d'escalars.** En canvi l'altre producte està definida entre un escalar i un vector se li sol dir **producte d'un escalar per un vector**.

A la propietat 5, els dos productes de l'esquerra són productes d'un escalar per un vector. En canvi el primer producte de la dreta de la propietat 5 és un producte d'escalars. En general es distingirà el tipus de suma i el tipus de producte, segons els tipus d'elements que enllacin.

4.13 Exemples d'espais vectorials

L'exemple d'on deriva el nom d'espai vectorial, és el de tots els vectors d'un pla, V. Ja hem vist que aquest conjunt amb l'operació suma (V, +) és un grup commutatiu. Els escalar són els reals **R** que ja se sap és un cos amb les operacions normals de suma i producte. En aquest conjunt hi ha definit un producte d'un real per un vector així: **R**xV ---->V, ja que el producte d'un nombre per un vector dóna com a resultat un vector. I les quatre últimes propietats, que en aquest cas es poden escriure com

$$r\cdot(s\cdot\vec{v}) = (r\cdot s)\cdot\vec{v}$$
$$(r+s)\cdot\vec{v} = r\cdot\vec{v} + s\cdot\vec{v}$$
$$1\cdot\vec{v} = \vec{v}$$
$$r\cdot(\vec{v}+\vec{u}) = r\cdot\vec{v} + r\cdot\vec{u}$$

resulten evidentment certes.

Altres exemples de vectors que són espais vectorials sobre el cos **R**, són tots els vector de l'espai (tres dimensions) i tots el vectors d'una recta (una dimensió). El primer conté els vectors del pla i el segon es contingut pels vectors del pla.

Ja hem vist que el conjunt F format per totes les funcions definides en (a,b) amb l'operació suma és un grup commutatiu. Com ja sabeu es pot definir el producte d'un real per una funció **R**x F------> F d'aquesta forma

$$(r\cdot f)(x) = r\cdot(f(x))$$

Es demostra fàcilment que es compleixen les quatre últimes propietats:

$$r\cdot(s\cdot f) = (r\cdot s)\cdot f$$
$$(r+s)\cdot f = r\cdot f + s\cdot f$$
$$1\cdot f = f$$
$$r\cdot(f+g) = r\cdot f + r\cdot g$$

Essent *r* i *s* reals, i *f* i *g* funcions.

Dels tres cossos numèric, **Q**, **R** i **C**, qualsevol d'ells es pot interpretar com a conjunt de vectors sobre algun dels cossos 'menors', o sobre ell mateix. Els reals és un espai vectorial sobre els racionals o també ho és sobre els mateixos reals. El complexes formen un espai vectorial sobre els racional, sobre els reals i sobre el mateixos complexes. I el racionals solament són un espai vectorial sobre els mateixos racionals.

En general un cos qualsevol és un espai vectorial sobre ell mateix. Un exemple d'espai vectorial finit és el dels conjunts **Z**n, amb n primer, sobre el mateix **Z**n.

El conjunt de tots els polinomis constitueixen un grup amb l'operació suma. Es pot definir un producte d'un real per un polinomi de la forma usual. Amb aquesta operació els polinomis són un espai vectorial sobre els reals.

Havíem vist que el conjunt dels polinomis de grau com a màxim n no és un anell, però sí que és un espai vectorial, ja que per la suma formen un grup i el producte d'un real per un polinomi és una aplicació ben definida com **R**x**P**n ------>**P**n, i fàcilment es comprova que compleixen les 4 propietats últimes.

Un exemple clàssic d'espai vectorial el constitueix el conjunt $\mathbf{R}^n$ (veure paràgraf 2.2) que amb l'operació suma (veure paràgraf 4.1):

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1+b_1, a_2+b_2, \ldots, a_n+b_n)$$

forma un grup commutatiu. Definirem l'operació producte per un real així:

$$r(a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n)$$

La comprovació de les propietats d'espai vectorial són immediates.

Un espai vectorial molt petit és el que solament té un element, el 0. Ja s'ha vist com un exemple de grup amb l'operació 0+0 = 0. I ara, falta veure el producte per un escalar, que pot ser d'un cos qualsevol. Aquest producte ha d'ésser $r \cdot 0 = 0$. Les comprovacions de les propietats es deixen pel lector.

4.14 Propietats que es compleixen en els espais vectorials

Primera:

$$0 \cdot x = o$$

El primer 0 és un escalar, el segon un vector. Per veure-ho podem posar que per qualsevol r i qualsevol x

$$r\cdot x = (r+0)\cdot x = r\cdot x + 0\cdot x$$

Passant $r\cdot x$ restant del tercer terme al primer queda

$$o = 0\cdot x$$

Segona:

$$(-r)\cdot x = -(r\cdot x)$$

Que ens diu que el producte del simètric d'un escalar per un vector és igual al simètric del producte de l'escalar pel vector:

$$o = 0\cdot x = (r + (-r))\cdot x = r\cdot x + (-r)\cdot x$$

Si la suma de dos element dóna el neutre és que aquests dos elements són simètrics.

Com a conseqüència immediata d'aquest propietat es veu que

$$(-1)\cdot x = -x$$

Tercera:

$$r\cdot o = o$$

Qualsevol escalar multiplicat per vector neutre dóna l'escalar neutre.

$$r\cdot x = r\cdot(x + o) = r\cdot x + r\cdot o$$

Passant $r\cdot x$ del tercer terme al primer restant, s'obté

$$o = r\cdot o$$

Quarta:

Es tracta d'una generalització de la tercera:

$$r\cdot x = o \quad \Leftrightarrow \quad r = 0 \ \vee \ x = o$$

Per la propietat primera i per la tercera queda demostrada la implicació de dreta a esquerra. Per demostrar-la de d' esquerra a dreta, suposarem que $r\cdot x$ = o i, també suposem que r no és 0.

Si r no és 0, ha de tenir invers r^{-1}, i:

$$x = 1\cdot x = (r^{-1}\cdot r)\cdot x = r^{-1}\cdot(r\cdot x) = r^{-1}\cdot o = o$$

Queda clar que si *r* no és zero ho ha d'ésser *x*.

Tenint en compte el que es va dir en el paràgraf 1.8 sobre equivalència d'aplicacions, la negació de la condició $r \cdot x = 0$ ha de ser equivalent a la negació de (r=0 . x=o), però aquesta negació és igual a $r \neq 0 \wedge x \neq o$ La nova equivalència quedarà:

$$r \cdot x \neq o \quad \Leftrightarrow \quad r \neq 0 \wedge x \neq o$$

Que també es complirà exactament com la primera. O sigui, si el producte d'un vector per un escalar no és zero vol dir que ni l'escalar ni el vector poden ser zero.

4.15 Subespais vectorials

Sigui E un espai vectorial sobre el cos K i F una subconjunt de F, que per les operacions que li provenen de E, és també un espai vectorial sobre K. En aquest cas es diu que F és un **subespai vectorial** de E.

Si es disposa d'un espai vectorial E sobre K i es coneixen els elements d'un subconjunt F de E, per esbrinar si F és o no és, subespai de E, s'ha de comprovar dues coses:

$$1.\ x \in F \wedge y \in F \Rightarrow x - y \in F$$
$$2.\ x \in F \wedge r \in K \Rightarrow r \cdot x \in F$$

La primera condició anterior assegura que F és un subgrup de E amb la suma, i per això, es compleixen les propietats 1 i 2 d'espai vectorial. La propietat 3 d'espai vectorial és òbvia. La segona condició de dalt ens assegura el compliment de la propietat 4. I les 4 últimes propietats són de compliment general i també s'han de complir en F. Per tot això es dedueix que F és un espai vectorial per ell mateix.

És obvi que qualsevol subespai ha de contenir a l'element neutre, sense ell no seria un subgrup per la suma.

Exemples:

El polinomis de grau màxim n, que em anotat com **P**n, constitueixen un subespai vectorial del espai de tots els polinomis **P**. Si m>n tindrem que **P**n és un subespai vectorial de **P**m.

El subconjunt de vectors de l'espai que la seva tercera coordenada és zero Eo, és un subespai vectorial de tots els vectors de l'espai. La comprovació és immediata.

En qualsevol espai vectorial E sobre K, el conjunt de tots els vectors múltiples d'un altre fix, que escriure F, que:

$$F = \{x \in E \mid \exists\, r \in K \quad x = rv\}$$

forma un subespai vectorial de E. La resta de dos múltiples de *v*, també és múltiple de *v*: *rv - sv = (r-s)v*. El producte d'un múltiple de *v* per un escalar, també és múltiple de *v*: *s(rv) = (sr)v.*

Totes les funcions derivables i definides en (a,b) formen un subespai vectorial de totes les funcions contínues i definides en (a,b), i aquestes formen un subespai vectorial de totes les funcions definides en (a,b).

4.16 Estructures algebraiques

Els conceptes explicats en aquest capítol, com el de grup, el d'anell, el de cos o el d'espai vectorial, en el que hi intervenen un, o més d'un conjunt, i unes operacions definides en aquests conjunts, que han de complir unes propietats determinades es diu es tracte d'**estructures algebraiques.**

Una àlgebra de Bool és una altre estructura algebraica que ha sortit en el primer capítol, doncs es tracta d'un conjunt amb tres operacions i una sèrie de propietats que s'han de complir.