De los ejemplos antes vistos queda claro que el concepto de independencia lineal es más complicado en módulos

<u>Prop.</u> Sean F un campo y V un F-espacio vectorial

a) Cualquier vector $\neq \bar{0}$ es linealmente independiente sobre F

b) El conjunto $\{v_1, v_2, \dots, v_n\}$ es linealmente independiente sobre F sii

- $v_1 \neq 0$
- $v_i \notin \langle \{v_1, v_2, \dots, v_{i-1}\} \rangle$ para $i = 2, \dots, n$

c) El conjunto $\{v_1, v_2, \dots, v_n\}$ es linealmente independiente sobre F sii

- $\{v_1, v_2, \dots, v_{n-1}\}$ es linealmente independiente sobre F
- $v_n \notin \langle \{v_1, v_2, \dots, v_{n-1}\} \rangle$

12

- $v_n \notin \langle \{v_1, \dots, v_{n-1}\} \rangle$.

Dem. al Si $\bar{v} \neq 0$ y
$r\bar{v} = \bar{0}$, $r = 0$, pues de no ser este el caso, r tiene inverso multiplicativo

$$\frac{1}{r} \cdot r\bar{v} = \frac{1}{r}\bar{0}$$
$$1 \cdot \bar{v} = \bar{0}$$
$$\bar{v} = \bar{0} \quad \text{↯. una contradicción.}$$

h) $\Rightarrow$) Si $v_1 = 0$, $1 v_1 = 0$ y S es lin. dependiente ↯.

Si $v_i \in \langle \{v_1, v_2, \dots, v_{i-1}\} \rangle$ para alguna $i \geq 2$, entonces

$$v_i = a_1 v_1 + \dots + a_{i-1} v_{i-1}, \quad a_1, \dots, a_{i-1} \in \mathbb{R}$$

lo que da lugar a

$$a_1 v_1 + \dots + a_{i-1} v_{i-1} - 1 v_i = 0$$

en S. En consecuencia, S es linealmente dependiente. ↯.

13

$\Leftarrow$) Supongamos que S es linealmente dependiente, en cuyo caso existe una relación no trivial entre sus elementos. Como $v_1 \neq 0$, y v_1 es l.i. por (a), la relación mencionada debe involucrar otros vectores distintos de v_1.

Supongamos que $a_1 v_1 + \cdots + a_i v_i = 0$ donde $a_i \neq 0$ para algún i con $2 \leq i \leq n$.

Esto implica que

$$v_i = -a_i^{-1}(a_1 v_1 + a_2 v_2 + \cdots + a_{i-1} v_{i-1})$$

$$\in \langle \{v_1, v_2, \ldots, v_{i-1}\} \rangle$$

lo que se opone a la hipótesis

c) Según (a), el conjunto $\{v_1, v_2, \ldots v_{n-1}\}$ es lineal. indep. y $v_n \notin \langle \{v_1, v_2, \ldots, v_{n-1}\} \rangle$

sii
- $v_1 \neq 0$
- $v_i \notin \langle \{v_1, v_2, \ldots, v_{i-1}\} \rangle \quad i = 2, \ldots, n-1$
- $v_n \notin \langle \{v_1, v_2, \ldots, v_{n-1}\} \rangle$

y por (b) otra vez, estas condiciones se cumplen

Sí, $\{v_1, v_2, \ldots, v_n\}$ es lin. indp. ///

Esto nos da la idea de cómo construir un conjunto linealm. indp en un espacio vectorial: empezamos con un vector no trivial y después elegimos elementos consecutivamente que no estén en el subespacio generado por los previos. Esto no es cierto para módulos en general

Ej: El conjunto $\{2,3\}$ es $\mathbb{Z}$-linealmente dependiente ya que

$$3 \cdot 2 + (-2) \cdot 3 = 0$$

No obstante $3 \notin \mathbb{Z}2$, así que el resultado previo no se cumple para módulos en general

EJERCICIOS

1. Considere el $\mathbb{R}$-espacio vectorial $\mathbb{R}^{\mathbb{R}}$. ¿Son $\cos x$ y $\operatorname{sen} x$ linealmente independientes?

2. Sean S un conjunto y $s \in S$. Defina $\chi_s \in R^S$ (R anillo) como la función

$$\chi_s(t) = \begin{cases} 1 & \text{si } t = s \\ 0 & \text{en otro caso} \end{cases}$$

(la función característica en s).
Muestre que $\{\chi_s : s \in S\}$ es un subconjunto linealmente independiente en R^S. Confirme que $R^S = \langle\{\chi_s : s \in S\}\rangle$ si S es un conjunto finito. ¿Es la afirmación cierta cuando S es infinito?

3. Sean M, N submódulos del R-módulo L. Defina $M+N = \{m+n : m \in M, n \in N\}$

16

(la suma de M y N).

a) Verifique que $M+N$ es un submódulo de L

b) Constate que $M+N$ es el menor submódulo en L que contiene a M y a N, esto es, $M+N = \langle M \cup N \rangle$.

c) Suponga que I es un conjunto de índices y que tiene $\{M_i : i \in I\}$ submódulos de L. Defina

$$\sum_{i\in I} M_i = \{ m_{i_1} + \cdots + m_{i_n} : n \in \mathbb{N},\ m_{i_j} \in M_{i_j} \}$$

la suma de los M_i. Cerciórese de que $\sum_{i\in I} M_i$ es un submódulo de L.

4.- Sean $M_1, M_2, \ldots, M_n$ submódulos del R-módulo M y tales que $M = M_1 + \cdots + M_n$. Decimos que los $M_1, M_2, \ldots, M_n$ son

R-independientes si siempre que $m_1 + \cdots + m_n = 0$, $m_i \in M_i$, ocurre que $m_1 = \cdots = m_n = 0$. Se escribe

$$M = M_1 \oplus \cdots \oplus M_n$$

Para expresar que $M = M_1 + \cdots + M_n$ y los $M_1, \ldots, M_n$ son R-independientes. Decimos que M es la suma directa (interna) de los $M_1, \ldots, M_n$. [a] Sean $m_1, m_2, \ldots, m_n$ linealmente R-independientes. Muestre que $Rm_1, Rm_2, \ldots, Rm_n$ son R-independientes.

b) Suponga que $Rm_1, Rm_2, \ldots, Rm_n$ son R-independientes. ¿Es cierto que $m_1, m_2, \ldots, m_n$ son linealmente R-independientes?

5. ¿Se puede encontrar un conjunto generador numerable para $\bigoplus_{i=1}^{\infty} R$?

6.- Sean V un espacio vectorial sobre el campo F, S un subconjunto de V y $v \in V$. Demuestre que $S \cup \{v\}$ es linealmente F-independiente sii S es linealmente F-independiente y $v \notin \langle S \rangle$

Bases

<u>Def</u>: En un R-módulo decimos que B es una base para M o una R-base para M cuando ocurre lo siguiente.

- B genera a M
- B es R-linealmente independiente

<u>Prop</u>: Cualquier elemento en un módulo se puede expresar en forma única como combinación lineal de elementos de la base

<u>Dem</u>: Sean B una base para M y $m \in M$

Como B genera a M, m es combinación lineal de elementos de B

$$m = \sum_{i=1}^{n} r_i b_i \qquad r_i \in R,\ b_i \in B$$

Supongamos que existe otra combinación lineal

$$m = \sum_{j=1}^{l} s_j c_j \qquad s_j \in R,\ c_j \in B$$

Sin perder generalidad alguna suponemos que en ambas expresiones aparecen los mismos elementos b_i, c_j poniendo s_j o r_i igual a cero en caso de necesidad.

Pero $$m = \sum_{i=1}^{p} r_i d_i$$

$$= \sum_{i=1}^{p} s_i d_i$$

restando

$$0 = \sum_{i=1}^{p} (r_i - s_i) d_i$$

que es una combinación lineal de elementos, de la base igualada a 0, por lo que de la definición de Base concluimos que $v_i - s_i = 0$ para $i = 1, \ldots, p$ esto es, $v_i = s_i$ y la representación es única. ///

<u>Def</u> Si un R-módulo M tiene una base, decimos que M es un R-módulo libre.

<u>No</u> todo módulo es libre.

<u>Eje</u> En $\mathbb{Z}_5$ ningún elemento es $\mathbb{Z}$-linealmente independiente pues,

$5\overline{k} = \overline{0}$ para cada $\overline{k} \in \mathbb{Z}_5$

En consecuencia, ningún subconjunto de $\mathbb{Z}_5$ es $\mathbb{Z}$-linealmente independiente.

Por lo que no pueden existir bases en $\mathbb{Z}_5$ sobre $\mathbb{Z}$. 11

Ej. Sea R un anillo

1) El conjunto $\{e_1, e_2, \dots, e_n\}$ es una R-base para R^n. (recuerde $e_i = (0, 0, \dots 1, \dots 0)$)
Se conoce como la base estándar de R^n.

2) El conjunto $\{e_{ij} : i = 1, \dots, m, j = 1, 2, \dots n\}$ es una R-base para $M_{m\times n}(R)$. Ésta es la base estándar para $M_{m\times n}(R)$.

3) Sea S un conjunto finito. El conjunto $\{\chi_s : s \in S\}$ es una R-base para R^S. Ésta es la base estándar de R^S. Note que

$$f = \sum_{s\in S} f(s)\chi_s, \quad \text{para } f \in R^S$$

Conjuntos parcialmente ordenados

12

Def: Sea $(S, \leq)$ un conjunto con una relación $\leq$; decimos que es un conjunto parcialmente ordenado (cpo) si se cumple lo siguiente para cualesquier $a, b, c \in S$.

a) $a \leq a$ Reflexividad

b) Si $a \leq b$ y $b \leq c$, entonces $a \leq c$ (transitividad)

c) Si $a \leq b$ y $b \leq a$, entonces $a = b$ (antisimetría).

$\leq$ se llama un orden parcial.

Note que pueden existir elementos $a, b \in S$ que no se comparan entre sí, de ahí el adjetivo "parcial".

Eje Sean S un conjunto arbitrario y

$Pot(S)$ el conjunto de subconjuntos de S (el conjunto potencia de S).

Entonces, $(Pot(S), \subseteq)$ es un cpo.

Ej. Sea S un conjunto. En $Pot(S)$ definimos la relación $\preceq$ como

$$A \preceq B \text{ si } B \subseteq A$$

en cuyo caso $(Pot(S), \preceq)$ es un cpo

Ej. $a|b$ si a divide a b

$(\mathbb{Z}^+, \leq)$, $(\mathbb{Z}^+, |)$ son cpo

Note que $(\mathbb{Z}, \leq)$ es un cpo, no así $(\mathbb{Z}, |)$ pues

$$1|-1 \quad y \ -1|1 \quad 1 \neq -1.$$

Def. Sean $(S, \leq)$ un cpo, $T \subseteq S$ y $u \in S$. Decimos que u es un cota superior de T si $a \leq u$ para cada $a \in T$

Decimos que $l \in S$ es una cota inferior de T si $l \leq a$ para todo $a \in T$.

$m \in T$ es un elemento mínimo de T cuando no existe $a \in T$ con $a < m$

$M \in T$ es un elemento máximo de T cuando no existe $a \in T$ con $M < a$.

Si $g, l \in T$, decimos que g es el mayor elemento de T si $a \leq g$ para todo $a \in T$.

l es el menor elemento de T si $l \leq a$ para cualquier $a \in T$.

<u>Ejo</u> $(\mathbb{Z}, \leq)$ no hay elemento mínimo o máximo.

<u>Ejo</u> $S = \{1, 2, 3, 4\}$. En $(Pot(S), \subseteq)$ el conjunto $\emptyset$ es el único elemento mínimo. y el menor. En forma similar, S es el

15

el menor elemento y el un elemento mínimo

$(A, \subseteq)$ dado

$A = \{\{1\}, \{3\}, \{1,2\}, \{2,3\}, \{2,4\},$
$\{2,3,4\}\} \subseteq P(S)$

Los elementos $\{1\}$, $\{3\}$ y $\{2,4\}$ son mínimos

$\{1,2\}$ y $\{2,3,4\}$ son máximos

No hay menor o mayor elemento en A