14

Lema Sea M un R-módulo, N un submódulo de M y $S, T \subseteq M$. Las siguientes afirmaciones son equivalentes:

a) $S \subseteq N$ si i $\langle S \rangle \subseteq N$

b) Si $S \subseteq T$, entonces $\langle S \rangle \subseteq \langle T \rangle$

c) Sea $m \in M$. Entonces $m \in \langle S \rangle$ si i $\langle S \cup \{m\} \rangle = \langle S \rangle$.

Demo a) $\Rightarrow$) Debemos probar que el submódulo generado por S está contenido en N. Recordemos que N es submódulo de M y que $\langle S \rangle$ es el menor submódulo de M que contiene a S; N es uno de tales submódulos, uno que contiene a S, de modo que $\langle S \rangle \subseteq N$.

$\Leftarrow$) Supongo $\langle S \rangle \subseteq N$ y probemos que $S \subseteq N$. Otra vez, $\langle S \rangle$ es el menor submódulo de M que contiene a S de modo que $S \subseteq \langle S \rangle$ y como $\langle S \rangle \subseteq N$, deducimos $S \subseteq N$,

b) Sabemos que $S \subseteq T$. Por definición $\langle T \rangle$ es el menor submódulo que contiene a T, así que

$$S \subseteq T \subseteq \langle T \rangle$$

y $\langle T \rangle$ contiene a S, es un submódulo de forma que $\langle S \rangle \subseteq \langle T \rangle$.

c) $\Rightarrow$) Sabemos que $m \in \langle S \rangle$, y $\langle S \cup \{m\} \rangle$ es el menor submódulo que contiene a $S \cup \{m\}$. Pero $S \cup \{m\} = S$ pues $m \in S$ por lo que

$$\langle S \rangle = \langle S \cup \{m\} \rangle.$$

$\Leftarrow$) Sabemos que $m \in S \cup \{m\} \subseteq \langle S \cup \{m\} \rangle = \langle S \rangle$.

#

Prop: Sea S un subconjunto de un R-módulo M. Entonces $\langle S \rangle$ consiste en las combinaciones lineales de elementos de S. Esto es, un elemento pertenece a $\langle S \rangle$ sii es de la forma $a_1 m_1 + \dots + a_n m_n$

donde $a_i \in R$, $m_i \in S$.

Def Sea N el conjunto de combinaciones lineales de elementos de S. Nuestra intención es mostrar que $N = \langle S \rangle$

Sean $s_1, \dots s_n \in S$ y tomemos una combinación lineal de ellos

$$r_1 s_1 + \cdots + r_n s_n$$

Ahora, $s_1, \dots, s_n \in S \subseteq \langle S \rangle$

$\langle S \rangle$ es un R-módulo (submódulo de M), de modo que $r_1 s_1, \dots, r_n s_n \in \langle S \rangle$ y más aún,

$r_1 s_1 + \cdots + r_n s_n \in \langle S \rangle$

de suerte que $N \subseteq \langle S \rangle$.

Resta verificar que $\langle S \rangle \subseteq N$.

Verifiquemos dos cosas: i) $S \subseteq N$

ii) N es un submódulo

Recuerde que N consiste en las combinaciones lineales de elementos de S. Tomemos un elemento arbitrario $s \in S$. Considere

$1 \cdot S + 0S + \dots + 0 \cdot S = S$

es una combinación lineal de elementos de S, de modo que pertenece a N, es decir, $S \in N$.

ii) N es submódulo de M.

Recuerde que la suma vacía se define como 0, por lo que $0 \in N$

Si $r_1 s_1 + \dots + r_n s_n \in N$ $r_i, t_i \in R$

$t_1 u_1 + \dots + t_m u_m \in N$ $s_i, u_i \in S$

son combinaciones lineales en N.

Es claro que la suma está en N

Si: $t_1 u_1 + \dots + t_m u_m \in N$ y $r \in R$

$r(t_1 u_1 + \dots + t_m u_m) = r t_1 u_1 + \dots + r t_m u_m$

es un elemento de N

de nuevo, gracias a submódulo, deducimos que N es submódulo.

Por tanto, $S \subseteq N$, N es submódulo y como antes, deducimos que

$\langle S \rangle \subseteq N$. ##

En virtud de esta proposición se acostumbra denotar $\langle m_1, \dots, m_n \rangle$ por $Rm_1 + \dots + Rm_n$

o incluso $m_1R + \dots + m_nR$, en particular cuando $M = \langle m \rangle = Rm$ y decimos que M es un módulo cíclico.

Ej: Sea R un anillo. Como R-módulo, R mismo es cíclico ya que $R = R1$.

Sea I un ideal de R. El ideal I es un R-módulo cíclico si I es un ideal principal. Aclaraciones. R no necesariamente conmutativo

Sea $A \subseteq R$. Mediante (A) denotamos el menor ideal de R que contiene a A

Y se conoce como el ideal generado por A mediante RA donde RA es el conjunto de sumas finitas de elementos de la forma ra con $r \in R$, $a \in A$,

$$RA = \{r_1a_1 + r_2a_2 + \dots + r_na_n : r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$$

donde, por convención, $RA = 0$ si $A = \emptyset$.

En forma similar

$$RAR = \{r_1a_1r_1' + r_2a_2r_2' + \dots + r_na_nr_n' : r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$$

Un ideal generado por un solo elemento se llama ideal principal.
Un ideal generado por un conjunto finito se llama ideal finito generado

Como antes,

$$(A) = \bigcap_{\substack{I \text{ ideal} \\ A \subseteq I}} I$$

(Note que R es un ideal y $A \subseteq R$).

El ideal izquierdo generado por A es la intersección de los ideales izquierdos de R que contienen a A.

$I \subseteq R$ es ideal izquierdo de R cuando

i) I es subanillo de R

ii) I es cerrado respecto a multiplicación por la izquierda por elementos de R

o sea $rI \subseteq I$ para cada $r \in R$

En forma correspondiente se define ideal derecho

Si I es ideal izquierdo y derecho se llama simplemente ideal. Es claro que si R es conmutativo ideal izquierdo y derecho es lo mismo, por lo que

en ese caso hablamos simplemente de ideal.
Cuando R es un anillo,
ideales subanillos R y son ideales. Un
ideal es propio si $I \neq R$. El ideal
trivial y se denota 0.

Así, si $A \subseteq R$, el ideal izquierdo generado
por A es la intersección de los ideales izquierdos
de R que contienen a A.
Para obtener este ideal debemos pensar en
A y quien un conjunto que lo contenga y
se cierre respecto a las operaciones
que definen a un ideal izquierdo

Por definición, RA cerrado respecto a suma
multiplicación a la izquierda por elementos del
anillo. Como $1 \in R$, RA contiene a A, por lo
que RA es un ideal izquierdo de R que contiene
a A.
Ahora, cualquier ideal que contiene a A
debe contener las sumas finitas de elementos

de la forma $ra + r' \in R$ y $a \in A$, de modo que debe contener a RA.

Por consiguiente, RA es precisamente el ideal izquierdo generado por A. En forma similar AR es el ideal derecho generado por A y RAR es el ideal generado por A.

En particular,

Si R es conmutativo, entonces

$$RA = AR = RAR = (A)$$

Cuando R es conmutativo y $a \in R$, el ideal principal (a) generado por a es precisamente el conjunto de los R-múltiplos de a. Cuando R no es conmutativo, el conjunto $\{ras + r' : r, s \in R\}$ no es necesariamente el ideal generado por a ya que no es necesariamente cerrado respecto a la suma. En este caso, el ideal generado por a es RaR que consiste en las sumas finitas de elementos de la forma $ras + r'$, $r, s \in R$.

La formación de ideales principales en un anillo conmutativo es una forma particular-

mente de crear anillos, similar a generar subgrupos cíclicos de un grupo. Nota que el elemento $b \in R$ pertenece a (a) sii $b = ra$ para alguna $r \in R$, es decir, sii b es múltiplo de a, o dicho de otra forma, a divide a b en R. Así, $b \in (a)$ sii $(b) \subseteq (a)$.

Respuesta a lo que ocurre con R conmutativo, $(a) = Ra$, es decir (a) es cíclico.

Ej: Sea R anillo. Definimos el elemento $e_i \in R^n$ como aquel cuya i-ésima entrada es 1 y el resto 0

$$e_i = (0, \dots, 0, 1, 0, \dots, 0)$$

$\downarrow$ i-ésima entrada

Por tanto, R^n está generado por $\{e_1, \dots, e_n\}$ sobre R. De hecho,

$$(a_1, a_2, \dots, a_n) = a_1 e_1 + \dots + a_n e_n$$

Ej: Sean R anillo y $m, n \in \mathbb{N}^+$. Definimos e_{ij} como la matriz en $M_{m \times n}(R)$ cuya

(i,j)-entrada es 1 y el resto 0. Entonces $M_{m\times n}(R)$ está generado por $\{e_{ij} \in M_{m\times n}(R) : i=1,\dots,m,\ j=1,\dots,n\}$ sobre R. Sin duda, una matriz arbitraria $(a_{ij})_{m\times n} = \sum_{ij} a_{ij} e_{ij}$ es una combinación lineal de los e_{ij} sobre R.

Dependencia lineal

Def Sean R un anillo y M un R-módulo. Decimos que $m_1,\dots,m_n$ son linealmente independientes sobre R si para $a_1,\dots,a_n \in R$ ocurre que

$$a_1m_1+\cdots+a_nm_n=0 \Rightarrow a_1=0=a_2=\cdots=a_n$$

En otro caso, decimos que $m_1, m_2,\dots,m_n$ son linealmente dependientes sobre R.

Un subconjunto finito $\{m_1, m_2,\dots,m_n\}$ de M es linealmente independiente sobre R. Un conjunto infinito es linealmente independiente sobre R cuando todos sus subconjuntos finitos son linealmente independientes

sobre R. Un conjunto arbitrario es linealmente dependiente sobre R cuando no es linealmente independiente sobre R.

Una relación de la forma

$$0m_1 + 0m_2 + \cdots + 0m_n = 0$$

es una relación trivial entre $m_1, \ldots, m_n$

Si podemos encontrar $a_1, \ldots, a_n \in R$ no todos cero tales que

$$a_1 m_1 + \cdots + a_n m_n = 0$$

es una relación no trivial entre $m_1, \ldots, m_n$

Teo Sean M un R-módulo, $S, T \subseteq M$, $S \subseteq T$. Las siguientes afirmaciones son ciertas.

a) Si T es linealmente independiente sobre R, así lo es S

b) Si S es l.d. sobre R, así lo es T.

Dem (a) Si S no lo fuera, existiría una relación no trivial entre ciertos elementos de S, que también ocurriría en T

b) Similar. ##

Ejemplo En $\mathbb{Z}^2$ los elementos $(2,3)$ y $(3,-5)$ son l.i. sobre $\mathbb{Z}$. Ciertamente,

$m(2,3)+n(3,-5)=(0,0)$

carece de soluciones no triviales en $\mathbb{Q}$, menos en $\mathbb{Z}$.

Ejemplo Sea R un anillo. En R^n, $e_1, e_2, \dots, e_n$ forman un conjunto l.i. sobre R. Sean $a_1, a_2, \dots, a_n \in R$ tales que

$$(0,\dots,0) = \sum_{i=1}^{n} a_i e_i = (a_1, a_2, \dots, a_n)$$

entonces $a_1 = a_2 = \cdots = a_n = 0$.

Ej El conjunto

$$\{e_{ij} \in M_{m\times n}(R) : i = 1,2,\dots,m,\ j = 1,2,\dots,n\}$$

es R-l.i en $M_{m\times n}(R)$. Sean $a_1,\dots,a_n \in R$ tal que

$$0 = \mathbb{O}_{m\times n} = \sum_{\substack{i=1,\dots,m \\ j=1,\dots,n}} a_{ij} e_{ij}$$

$$= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{m1} & \cdot & \sim & \cdot\, a_{mn} \end{pmatrix}$$

Entonces $a_{ij} = 0$ para cualquier i,j

Ej: Sea n un natural ≥ 2. Considere $\mathbb{Z}_n$ como $\mathbb{Z}_n$-módulo. Se afirma que $\overline{k}$ es l.i. sobre $\mathbb{Z}_n$ sii $(n,k) \sim 1$

Supongo que $(n,k) \sim 1$. Sea $m \in \mathbb{Z}$ tal que $\overline{m}\,\overline{k} = \overline{0}$; esto implica que $n \mid mk$ en $\mathbb{Z}$. Como n y k son primos relativos, se cumple que $n \mid m$ y $\overline{m} = \overline{0}$. Concluimos que $\overline{k}$ es l.i. sobre $\mathbb{Z}_n$.

Por la recíproca, supongo que $d \sim (n,k) \neq 1$. Entonces, $(n \mid d)\,\overline{k} = \overline{0}$. Y como $n \mid d \neq 0$ en $\mathbb{Z}_n$, esto confirma que $\overline{k}$ es l. d. sobre $\mathbb{Z}_n$.

Por otro lado, considere $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo. Ningún elemento en $\mathbb{Z}_n$ es l. i. sobre $\mathbb{Z}$ porque $n\overline{k} = \overline{0}$ es una relación no trivial para cada $k \in \mathbb{Z}$.