Trabajo Final: Módulos

Estructuras Algebraicas

Nicolas Silva Nash

UNCO

Definición de Módulo

Sea R un anillo. Un R-módulo por derecha M es

(I) un grupo abeliano aditivo $(M, +)$ junto con

(II) una aplicación

$$M \times R \ \to \ M \quad \text{con} \quad (m, r) \mapsto mr,$$

llamada *multiplicación de módulo*, para la cual tenemos

1. Ley asociativa: $(mr_1)r_2 = m(r_1 r_2)$.
2. Leyes distributivas:
$$(m_1 + m_2)r = m_1 r + m_2 r, \quad m(r_1 + r_2) = mr_1 + mr_2.$$
3. Ley unitaria: $m \cdot 1 = m$.

Con m, m_1, m_2 elementos arbitrarios de M y r, r_1, r_2 elementos arbitrarios de R.

Módulos

Algunas observaciones:

1. Podemos definir de manera análoga un R-módulo por izquierda.
2. Notamos M_R al R-módulo por derecha y ${}_RM$ al R-módulo por izquierda.
3. Si un módulo verifica ambas condiciones para anillos R (por derecha) y S (por izquierda), y además verifica:

$$s(mr) = (sm)r, \qquad \forall s \in S, r \in R$$

   decimos que es un $S-R$-bimódulo al que notamos ${}_SM_R$.
4. Si 0_M es el cero de M, 0_R es el cero de R, entonces:
   - $0_M \cdot r = 0_M$
   - $m \cdot 0_R = 0_M$, $\forall m \in M, r \in R$

Submódulos

Definición: Sea M un R-módulo por derecha. Un subconjunto A de M se llama un submódulo de M, notacionalmente $A \hookrightarrow M$ (o también $A_R \hookrightarrow M_R$) si A es un R-módulo por derecha con respecto a la restricción de la suma y la multiplicación de módulo de M a A.

Usamos la notación $A \hookrightarrow M$ para la relación de submódulo, para tener disponible $A \subseteq M$ para la inclusión en teoría de conjuntos. Además, denotamos $A \hookrightarrow_{\neq} M$ si y sólo si A es un submódulo propio de M.

Notamos $A \not\hookrightarrow M$ si A no es un submódulo de M. Observamos que de $A \not\hookrightarrow M$ no necesariamente se sigue que $A \not\subseteq M$.

Submódulos

Lema:
Sea M un R-módulo por derecha. Si A es un subconjunto de M y $A \neq \emptyset$, entonces las siguientes afirmaciones son equivalentes:

1. $A \hookrightarrow M$.
2. A es un subgrupo del grupo aditivo de M y para todo $a \in A$ y todo $r \in R$, tenemos $ar \in A$ (donde ar es la multiplicación de módulo en M).
3. Para todos $a_1, a_2 \in A$, $a_1 + a_2 \in A$ (con respecto a la suma en M) y para todo $a \in A$ y todo $r \in R$, tenemos $ar \in A$.

Submódulos: Ejemplos y observaciones

- Todo módulo M posee los submódulos triviales 0 y M, donde 0 es el submódulo que contiene solo el elemento cero de M.
- Sea M arbitrario y sea $m_0 \in M$.

  $$m_0 R = \{m_0 r \mid r \in R\}$$

  es un submódulo de M que se llama el submódulo cíclico de M generado por m_0.
- Si M_K es un espacio vectorial sobre el campo K, entonces los submódulos se laman subespacios (lineales).
- En el anillo $\mathbb{Z}$ de los números naturales, cada ideal es cíclico.
- Los ideales cíclicos de un anillo se llaman ideales principales y un anillo conmutativo se llama anillo de ideales principales si cada ideal es un ideal principal.
- Un campo K tiene solo los ideales triviales 0 y K.

Submódulos: Definiciones

1. Un módulo $M = M_R$ se llama *cíclico* si y solo si
$$\exists m_0 \in M : \; M = m_0 R$$
2. Un anillo R se llama *simple* si y solo si
$$\forall A \hookrightarrow R : \; A = 0 \text{ or} A = R,$$
es decir, 0 y R son los únicos ideales bilaterales de R.
3. Un submódulo $A \hookrightarrow M$ se dice un *submódulo minimal* de M si y solo si
$$0 \hookrightarrow B \hookrightarrow A \;\Rightarrow\; B = 0 \text{ o } B = A,$$
4. Un submódulo $A \hookrightarrow M$ se dice un *submódulo maximal* si y solo si
$$A \hookrightarrow B \hookrightarrow M \;\Rightarrow\; B = A \text{ o } B = M.$$

Submódulos

Lema. M es simple si y solo si

1. $M \neq 0$
2. $\forall m \in M: \; m \neq 0 \Rightarrow mR = M$

Prueba.

- **($\Rightarrow$)**: Supongamos que M es simple. Sea $m \in M, m \neq 0$. Entonces $m = m \cdot 1 \in mR$, luego $mR \neq 0$. Como $mR \subset M$ y M es simple, tenemos que necesariamente $mR = M$.
- **($\Leftarrow$)**: Sea A tal que $0 \hookrightarrow_{\neq} A \hookrightarrow_{\neq} M$ y sea $a \in A, a \neq 0$. Luego $aR \in A$. Además, por la hipótesis, $a \in M$ implica $aR = M$. Sigue que $aR = M \subset A$, luego $A = M$.

Ejemplos

- $\mathbb{Z}$ no contiene ideales minimales (simples), ya que si $n\mathbb{Z} \neq 0$, entonces $2n\mathbb{Z}$ es un ideal no nulo contenido dentro de $n\mathbb{Z}$.
- Los ideales maximales de $\mathbb{Z}$ son exactamente los ideales primos $p\mathbb{Z}$, donde p es un número primo. La prueba de esto sigue del hecho de que

$$m\mathbb{Z} \hookrightarrow n\mathbb{Z} \iff n \mid m.$$

- $\mathbb{Q}_{\mathbb{Z}}$ no tiene submódulos minimales ni maximales.
  Supongamos que A es un submódulo no trivial de $\mathbb{Q}_{\mathbb{Z}}$.
  Sea A tal que $0 \hookrightarrow_{\neq} A \hookrightarrow \mathbb{Q}_{\mathbb{Z}}$. Sea $a \in A$ tal que $a \neq 0$. Entonces

$$0 \hookrightarrow_{\neq} 2a\mathbb{Z} \hookrightarrow_{\neq} a\mathbb{Z} \hookrightarrow A \hookrightarrow \mathbb{Q}.$$

  Por lo tanto, A no puede ser minimal. Más adelante veremos que no existen submódulos maximales.

Definición de Álgebra

Aprovechamos esta oportunidad para recordar la definición de un álgebra.
Definición. Un álgebra es un par (R, K), donde

(I) R es un anillo.

(II) K es un anillo conmutativo.

(III) R es un módulo derecho sobre K para el cual se cumple

$$\forall r_1, r_2 \in R,\ k \in K: \quad (r_1 r_2)k = r_1(r_2 k) = (r_1 k)r_2.$$

Hemos definido a R con un elemento unitario y a K actuando unitariamente sobre R. El par (R, K) también se denomina K-álgebra o álgebra sobre K.
No tiene sentido definir a R como una "álgebra derecha sobre K". Dado que K es conmutativo, podemos, a partir de la definición

$$kr := rk, \quad \forall r \in R, k \in K,$$

pasar inmediatamente a un "álgebra izquierda sobre K".

Suma Interna Directa

Decimos que M es una *suma interna directa* de la familia $\{B_i, i \in I\}$ de submódulos $B_i \hookrightarrow M$, y notamos

$$M = \bigoplus_{i \in I} B_i$$

si y solo si se verifican las condiciones:

1. $$M = \sum_{i \in I} B_i$$

2. $$\forall j \in I : \; B_j \cap \sum_{\substack{i \in I \\ i \neq j}} B_i = 0$$

Suma Interna Directa: Unicidad de representación

Lema: Sea $B_i, i \in I$, un conjunto de submódulos $B_i \hookrightarrow M$ tales que $M = \sum_{i \in I} b_i$. Entonces, la condición (2) de la definición anterior equivale a que la representación de cada $x \in M$ de la forma $x = \sum_{i \in I'} b_i$, con $b_i \in B_i$ y $I' \subseteq I$, I' finito, es única. Esto es

$$x = \sum_{i \in I'} b_i = \sum_{i \in I'} c_i, \qquad b_i, c_i \in B_i \qquad \Rightarrow \qquad b_i = c_i, \ \forall i \in I'$$

Demostración

"$\Rightarrow$" Sea (2) cierto y sea $x = \sum_{i \in I'} b_i = \sum_{i \in I'} c_i$, luego $\sum b_i - \sum c_i = 0$, así $b_j - c_j = \sum_{i \neq j} c_i - b_i$. Entonces, tenemos que

$$\forall j \in I' : \qquad b_j - c_j = \sum_{\substack{i \in I' \\ i \neq j}} (c_i - b_i) \in B_j \cap \left(\sum_{\substack{i \in I' \\ i \neq j}} B_i \right).$$

Dado que $I' \subseteq I$ y que (2) vale, tenemos

$$B_j \cap \left(\sum_{\substack{i \in I' \\ i \neq j}} B_i \right) \hookrightarrow B_j \cap \left(\sum_{\substack{i \in I \\ i \neq j}} B_i \right) = 0.$$

sigue que $b_j - c_j = 0$, esto es, $b_j = c_j$, para todo $j \in I'$.

"$\Leftarrow$": Sea

$$b \in B_j \cap \left(\sum_{\substack{i \in I \\ i \neq j}} B_i \right),$$

entonces $b = b_j \in B_j$ y hay un subconjunto finito $I' \subset I$ con $j \notin I'$ tal que

$$b = b_j = \sum_{i \in I'} b_i, \quad b_i \in B_i.$$

Si añadimos al lado izquierdo los sumandos $0 \in B_i$, $i \in I'$ y al lado derecho el sumando $0 \in B_j$, entonces el mismo conjunto de índices finito $I' \cup \{j\}$ aparece en ambos lados

$$b_j + \sum_{i \in I'} 0 = \sum_{i \in I'} b_i + 0 \;\Rightarrow\; \sum_{k \in I' \cup \{j\}} b_k = \sum_{k \in I' \cup \{j\}} b_k$$

y por unicidad se sigue que $b = b_j = 0$, es decir, (2) se cumple. $\blacksquare$

Definición:

1. Un submódulo $B \hookrightarrow M$ se dice un *sumando directo* de M si existe $C \hookrightarrow M$ tal que $M = B \bigoplus C$
2. Un módulo $M \neq 0$ se dice *no directamente descomponible* si 0 y M son los únicos sumandos directos de M.

Ejemplos:

- Sea $V = V_K$ un espacio vectorial y sea $\{x_i, i \in I\}$ una base de V. Entonces
$$V = \bigoplus_{i \in I} x_i K.$$
Más aún, todo subespacio de V es un sumando directo.
- En $\mathbb{Z}_{\mathbb{Z}}$ el ideal $n\mathbb{Z}$ con $n \notin \{-1, 0, 1\}$ no es un sumando directo. Si suponemos $\mathbb{Z} = n\mathbb{Z} \bigoplus m\mathbb{Z}$ con $n \neq 0$, luego $nm \in n\mathbb{Z} \cap m\mathbb{Z}$ y así $m = 0$, por lo que $\mathbb{Z} = n\mathbb{Z}$.