Capítulo I: MÓDULOS.

⋆ ¿donde aparece el álgebra homológica? [5]

⋆ Vamos a seguir [3], aunque con definiciones de Jacobson [2].

1. NOCIONES PREVIAS

1.1 DEF: Sea R un conjunto no vacío con dos operaciones "+" y " " a la primera operación se la suele denominar suma y a la segunda producto. Diremos que $(R, +, \ )$ es un anillo si:

– $(R, +)$ es un grupo abeliano.

– La segunda operación es asociativa.

– Se verifican las propiedades distributivas: para todo $x, y, z \in R$

$$(x + y)z = xz + yz \qquad z(x + y) = zx + zy.$$

⋆ Diremos que un anillo $(R, +, \ )$ es unitario si la segunda operación posee elemento unidad. A la unidad se la denotará normalmente por 1.

⋆ Diremos que un anillo $(R, +, \ )$ es conmutativo si la segunda operación es conmutativa.

⋆ Diremos que un elemento no nulo $x \in R$ es un divisor absoluto de cero por la izquierda (por la derecha) si existe $0 \neq y \in R$ tal que $xy = 0$ ($yx = 0$). Diremos que $0 \neq x \in R$ es un divisor absoluto de cero si es divisor absoluto de cero por la izquierda o por la derecha. Diremos que un anillo $(R, +, \ )$ es un dominio de integridad si es un anillo conmutativo, unitario sin divisores de cero.

⋆ Diremos que un anillo $(R, +, \ )$ es de división si todo elemento no nulo de R tiene inverso.

⋆ Diremos que un anillo $(R, +, \ )$ es un cuerpo si es un anillo de división conmutativo.

Nota: Al neutro de la suma se le denotará por 0. Al neutro del producto se le denota por 1. La unidad, caso de existir es única y si $a \in R$ es un elemento inversible, el inverso de a es único (al que denotaremos por a^{-1}).

1.2 Proposición Sea R un anillo. Entonces $\mathbb{Z} \times R$ con suma y producto:

$$(\lambda, r) + (\mu, r') := (\lambda + \mu, r + r')$$
$$(\lambda, r).(\mu, r') := (\lambda\mu, \lambda r' + \mu r + r.r')$$

Tiene estructura de anillo unitario. Es más. la aplicación $\psi : R \to \mathbb{Z} \times R$ dada por $\psi(r) = (0, r)$ es un monomorfismo de anillos.

1.3 Def: Sea R un anillo. Se define la unitización de R, y se representa por R^1 como R, si éste ya es un anillo unitario o $\mathbb{Z} \times R$ caso de que R no sea unitario.

1.4 Ejemplos:

I-. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ son anillos unitarios. $2\mathbb{Z} := \{2x \mid x \in \mathbb{Z}\}$ es un anillo no unitario.

II-. Los anillos módulo n. Sea n un número natural y consideremos $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$. Observar que $\mathbb{Z}_n$ tiene n elementos. Dados $a, b \in \mathbb{Z}_n$ definimos:

– La suma de a y b como el resto de dividir $a + b$ por n.

– El producto de a y b como el resto de dividir ab por n.

Entonces $(\mathbb{Z}_n, +,)$ tiene estructura de anillo conmutativo y unitario. Es más, si $n = p$ es un número primo, $(\mathbb{Z}_p, +,)$ es un cuerpo (con p elementos).

Nota: Caso de que nuestro anillo R tenga característica n, podemos hacer la construcción anterior sobre $\mathbb{Z}_n \times R$, lo que nos dará una envolvente unitaria de R conservando la característica.

2. CONSTRUCCIÓN DE NUEVOS ANILLOS.

2.1 proposición Sea I un conjunto de indices y R_i, $i \in I$ una familia de anillos. Entonces $\Pi_{i \in I} R_i$ con su estructura habitual de grupo abeliano:

$$\Pi_{i \in I} R_i := \{(r_i)_{i \in I} \quad \text{con} \quad r_i \in R_i, \quad i \in I\}$$

$\star$ Con suma: $(r_i)_{i \in I} + (r'_i)_{i \in I} = (r_i + r'_i)_{i \in I}$

$\star$ y producto dado por componentes, $(r_i)_{i \in I}.(r'_i)_{i \in I} = (r_i.r'_i)_{i \in I}$

tiene estructura de anillo, llamado el **producto directo** de los R_i.

2.2 PROPOSICIÓN Sea I un conjunto de indices y R_i, $i \in I$ una familia de anillos. Entonces $\bigoplus_{i\in I} R_i$, con su estructura habitual de grupo abeliano:

$$\bigoplus_{i\in I} R_i = \{(r_i)_{i\in I} \in \Pi_{i\in I} R_i \mid r_i = 0 \quad \text{para casi todo } i\}$$

$\star$ Con suma: $(r_i)_{i\in I} + (r'_i)_{i\in I} = (r_i + r'_i)_{i\in I}$

$\star$ y producto dado por componentes, $(r_i)_{i\in I}.(r'_i)_{i\in I} = (r_i.r'_i)_{i\in I}$

tiene estructura de anillo, llamado la **suma directa externa** de los R_i.

2.3 PROPOSICIÓN Sea R un anillo y $n \in \mathbb{N}$. Entonces $\mathcal{M}_n(R)$ con su suma y producto habitual tiene estructura de anillo. Es más,

- $\mathcal{M}_n(R)$ es conmutativo si y sólo si R es conmutativo y $n = 1$.
- $\mathcal{M}_n(R)$ es un anillo de división si y sólo si R es un anillo de división y $n = 1$.
- $\mathcal{M}_n(R)$ es un cuerpo si y sólo si R es un cuerpo y $n = 1$.

2.4 DEF: Sea R un anillo. Se define el anillo de las series formales sobre R y se representa por $R[[X]]$ como:

$$R[[X]] := \{f : \mathbb{N} \to R \mid \text{con } 0 \in \mathbb{N}\} \quad \text{con operaciones:}$$

$$(n)(f+g) := (n)f + (n)g$$
$$(n)(f.g) := \sum_{k=0}^{n} (k)f \ (n-k)g$$

Nota: Un elemento f de $R[[X]]$ se denotan por $p(X) = \sum_{n=0}^{\infty} r_n X^n$ en donde r_n es $(n)f$ y la suma y el producto son los usuales.

2.5 DEF: Sea R un anillo. Se define el anillo de polinomios sobre R y se representa por $R[X]$ como:

$$R[X] := \{f : \mathbb{N} \to R \mid (n)f = 0 \text{ para casi todo } n, \text{ con } 0 \in \mathbb{N}\}$$

$$(n)(f+g) := (n)f + (n)g$$
$$(n)(f.g) := \sum_{k=0}^{n} (k)f \ (n-k)g$$

Nota: Un elemento f de $R[X]$ se denotan por $p(X) = \sum_{i=0}^{n} r_i X^n$ en donde r_i es $(i)f$ y la suma y el producto son los usuales.

2.6 DEF: Dado un anillo R, se define el opuesto de R y se representa por R^{op} como un nuevo anillo en donde el grupo abeliano vuelve a ser $(R, +)$ y el producto se define por

$$x.y := yx.$$

3. LA NOCIÓN DE MÓDULO.

3.1 DEF: Sea R un anillo y M un conjunto no vacío con dos operaciones, una interna $+ : M \times M \to M$ y otra externa $R \times M \to M$. Se dirá que $(M, +, \ )$ tiene estructura de R–módulo por la izquierda si verifica:

$\star$ La operación interna (también llamada suma) tiene estructura de grupo abeliano, es decir,

(1.1) Propiedad asociativa: $(m + n) + u = m + (n + u) \quad \forall\ m, n, u \in M$.

(1.2) Existencia de elemento neutro: $\exists\ \overline{0} \in M$ tal que $\forall\ m \in M, \quad \overline{0} + m = m + \overline{0} = m$.

(1.3) Existencia de elemento opuesto: $\forall\ m \in M, \ \exists\ -m \in M$ tal que $(-m) + m = m + (-m) = \overline{0}$.

(1.4) Propiedad conmutativa: $m + n = n + m \quad \forall\ m, n \in M$.

$\star$ La operación externa verifica,

(2.1) $x(m + n) = xm + xn \quad \forall\ m, n \in M,\ x \in R$.

(2.2) $(x + y)m = xm + ym \quad \forall\ m \in V,\ x, y \in R$.

(2.3) $1m = m \quad \forall\ v \in M$.

(2.4) $x(ym) = (xy)m \quad \forall\ m \in M,\ x, y \in R$.

3.2 DEF: Sea R un anillo y M un conjunto no vacío con dos operaciones, una interna $+ : M \times M \to M$ y otra externa $M \times R \to M$. Se dirá que $(M, +, \ )$ tiene estructura de R–módulo por la derecha si verifica:

$\star$ La operación interna tiene estructura de grupo abeliano,

$\star$ La operación externa verifica,

(2.1) $(m + n)x = mx + nx \quad \forall\ m, n \in M,\ x \in R$.

(2.2) $m(x+y) = mx + my \quad \forall\, m \in V,\ x, y \in R.$

(2.3) $m1 = m \quad \forall\, v \in M.$

(2.4) $(mx)y = m(xy) \quad \forall\, m \in M,\ x, y \in R.$

3.3 Ejemplos 1.- Es claro que todo espacio vectorial por la izquierda (por la derecha) es un módulo por la izquierda (por la derecha).

2.- Sea G un grupo abeliano. Si definimos en G la operación externa $\mathbb{Z} \times G \to G$ definida por

$$ng = \begin{cases} g + g + \ldots + g & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ -g - g - \ldots - g & \text{si } n < 0 \end{cases}$$

tenemos que G es un $\mathbb{Z}$–módulo.

Nota: Aunque todo espacio vectorial tenga estructura de módulo, no podemos esperar que estos últimos tengan propiedades parecidas a los espacios vectoriales. Por ejemplo, no todo módulo posee base.

3.4 Proposición Si M es un R–módulo por la izquierda y definimos la operación externa $M \times R^{op} \to M$ definida por $m.x := xm$. Tenemos entonces que M tiene estructura de R^{op}-módulo por la derecha. De forma simétrica todo R-módulo por la derecha tiene estructura de R^{op}–módulo por la izquierda.

Nota: Si R es un anillo conmutativo ($R \cong R^{op}$), todo R-modulo por la izquierda (por la derecha) tiene estructura natural de R-modulo por la derecha (por la izquierda).

3.5 Def: Sean R y S dos anillos. Diremos que M es un R, S-bimódulo si M tiene estructura de R-módulo por la izquierda, M tiene estructura de S-módulo por la derecha y se verifica la propiedad

(3.1) $(rm)s = r(ms)$ para todo $r \in R$, $m \in M$ y $s \in S$.

Nota: Si M es un R-módulo por la izquierda y S es el centro de R, M tiene estructura de R, S-bimódulo. Cuando estudiemos los homomorfismos de módulos veremos que hay otra estructura natural de bimódulo asociada a un módulo.

4. HOMOMORFISMOS DE MÓDULOS

4.1 Def: Sean M y N dos R-módulos y sea $f : M \to N$ una aplicación. Se dice que f es un **homomorfismo de módulos** si verifica:

(i) $(m_1 + m_2)f = (m_1)f + (m_2)f$ para todo $m_1, m_2 \in M$.

(ii) $(xm)f = x(m)f$ para todo $x \in R$ y $m \in M$.

Nota: Los homomorfismos de R-módulos por la izquierda (por la derecha) los escribiremos por la derecha (por la izquierda).

4.2 DEF: Sean M y N dos R-módulos y $f : M \to N$ un homomorfismo de R-módulos. Entonces:

- ⋆ Si f es inyectivo se dice que f es un **monomorfismo** de R-módulos.
- ⋆ Si f es sobreyectiva se dice que f es un **epimorfismo** dde R-módulos.
- ⋆ Si f es biyectiva se dice que f es un **isomorfismo** de R-módulos.
- ⋆ A un homomorfismo de R-módulos $g : M \to M$ se le denomina un **endomorfismo** (es decir, si tiene el mismo dominio que co-dominio).
- ⋆ Un endomorfismo biyectivo se le denomina un **automorfismo**.

4.3 Diremos que dos R-módulos M y N son **isomorfos** si existe un isomorfismo de R-módulos $f : M \to N$.

Denotaremos por $Hom_R(M, N)$ al conjunto de todos los homomorfismos de R-módulos de M en N y por $End_R(M)$ al conjunto de todos los endomorfismos de M como R-módulo.

⋆ Podemos definir una suma en $Hom_R(M, N)$ que dota a este conjunto de estructura de grupo abeliano: Si $f, g \in Hom_R(M, N)$ definimos

$$(m)(f + g) := (m)f + (m)g.$$

⋆ Podemos definir un producto en $End_R(M)$, la composición, que dota a los endomorfismos de estructura de anillo unitario.

Nota 1: $Hom_R(M, N)$ no tiene que tener estructura de R-módulo.

Nota 2: Si M es un R-módulo por la izquierda, M tiene estructura natural de $End_R(M)$-módulo por la derecha definiendo el producto $mf := (m)f$. Es más, con estas estructuras M es un $R, End_R(M)$-bimódulo.

5. SUBMÓDULOS

Nota: Asociada a cada una de las estructuras que vamos a ir introduciendo

aparecerá un cierto homomorfismo de módulos asociado (o una cierta propiedad fundamental)

5.1 DEF: Sea R un anillo unitario y M un R-módulo por la izquierda. Se dice que $N \subset M$ es un R-submódulo de M, y se representa por $N \leq M$, si tanto la suma como la multiplicación de M son cerradas en N y $(N, +, \ )$ tiene estructura de R-módulo.

Nota: que las operaciones sean cerradas en N significa:

$$\begin{aligned} n_1 + n_2 \in N \quad & \forall\ n_1, n_2 \in N. \\ xn \in N \quad & \forall\ x \in R, n \in N. \end{aligned}$$

5.2 PROPOSICIÓN Sea R un anillo unitario y M un R-módulo por la izquierda. Entonces un subconjunto N de M es un R-submódulo si y sólo si las operaciones son cerradas en N.

5.3 LEMA Sean M y N dos R-módulos y $f : M \to N$ un homomorfismo de R-módulos. Entonces

$$\begin{aligned} Im(f) :=& \{(m)f \quad m \in M\} \leq N \\ Ker(f) :=& \{m \in M \quad (m)f = 0\} \leq M \end{aligned}$$

5.4 LEMA Sea N un submódulo de un R-módulo M. Entonces la aplicación inclusión de N en M es un monomorfismo de módulos, llamado el monomorfismo inclusión. Es más, si $f : N \to M$ es un monomorfismo de módulos, $N \cong Im(f)$ es un submódulo de M.

Nota: Todo submódulo queda determinado a partir de un monomorfismo de módulos y viceversa.

6. MÓDULO COCIENTE

La estructura cociente va a relacionar las relaciones de equivalencia con la estructura de módulo. Así, si R es un anillo unitario y M es un R-módulo por la izquierda, vamos a ver que relaciones de equivalencia en M son compatibles con la suma y el producto por escalares de M (es decir con la estructura de R-módulo). Es decir, si $\cong$ es una relación de equivalencia en M, denotamos la clase

de equivalencia de un $m \in M$ como $\bar{m}$, ¿cuando $\bar{m} + \bar{m}' := \overline{m + m'}$ y $x\bar{m} := \overline{xm}$ están bien definidas y dan estructura de módulo al conjunto cociente $M/\cong$?

Es fácil ver que $\bar{0}$ es un submódulo de M y que la relación de equivalencia es exactamente $m \cong m'$ si y sólo si $m - m' \in \bar{0}$. Por lo que todas estas relaciones de equivalencia quedan determinadas por submódulos de M. Es más, se verifica el recíproco:

6.1 Proposición Sea R un anillo unitario, M un R-módulo por la izquierda y N un submódulo de M. Entonces:

(i) La relación $m \cong m'$ si y sólo si $m - m' \in N$ es una relación de equivalencia en M.

(ii) En el conjunto cociente $M/\cong$, las operaciones:

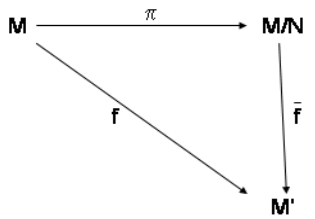
$$\bar{m} + \bar{m}' := \overline{m + m'}$$
$$r\bar{m} := \overline{rm}$$

definen una estructura de R-módulo.

6.2 Def. El módulo definido anteriormente se denomina el módulo cociente de M sobre N y se representa por M/N.

6.3 Def: Sea R un anillo unitario, M un R-módulo por la izquierda y N un submódulo suyo. Entonces la aplicación $\pi : M \to M/N$ definida por $(m)\pi := \bar{m}$ es un epimorfismo de módulos.

6.4 Teorema Sea R un anillo unitario, M un R-módulo por la izquierda y N un submódulo suyo. Entonces, para cada modulo M' y cada morfismo de módulo $f : M \to M'$ tal que $(N)f = 0$ ($N \subset \mathrm{Ker}(f)$) existe un homomorfismo de módulos $\bar{f} : M/N \to M'$ tal que $\pi\bar{f} = f$. Es decir, el siguiente diagrama es conmutativo.



6.5 Def: Sea R un anillo unitario, M, M' dos R-módulos y $f : M \to M'$ un homomorfismo de R-módulos. Se define la coimagen de f y se representa

por $CoIm(f) := M/\operatorname{Ker}(f)$, se define el conúcleo de f y se representa por $CoKer(f) := M'/\operatorname{Im}(f)$.

6.6 TEOREMA Sea R un anillo unitario, M, M' dos R-módulos y $f : M \to M'$ un homomorfismo de R-módulos. Entonces:

(i) f es inyectivo si y sólo si $\operatorname{Ker}(f) = 0$.

(ii) f es sobreyectivo si y sólo si $CoKer(f) = 0$.

6.7 TEOREMA(1^o TEOREMA DE ISOMORFÍA) Sea R un anillo unitario, M, M' dos R-módulos y $f : M \to M'$ un homomorfismo de R-módulos. Entonces $CoIm(f) \cong Im(f)$.

7. PRODUCTO DIRECTO DE MÓDULOS

7.1 PROPOSICIÓN Sea R un anillo unitario, I un conjunto de indices y M_i, $i \in I$ una familia de R-módulos. Entonces

$$\Pi_{i\in I} M_i := \{(m_i)_{i\in I} \quad \text{con} \quad m_i \in M_i, \quad i \in I\}$$

$\star$ Con suma: $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$

$\star$ y producto dado por componentes, $r(m_i)_{i\in I} = (rm_i)_{i\in I}$

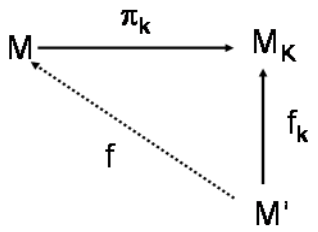
tiene estructura de R-módulo, llamado el **producto directo** de los M_i.

7.2 DEF: Sean $M_i,\ i \in I$ una familia de R-módulos y sea $M = \Pi_{i\in I} M_i$ el producto directo de los M_i. Se define la **proyección "canónica"** de M en M_k, con $k \in I$, como:

$$\begin{array}{rccc} \pi_k : & M & \to & M_k \\ & (m_i)_{i\in I} & \mapsto & m_k. \end{array}$$

Es fácil ver que para cada $k \in I$, π_k es un epimorfismo de R-módulo.

7.3 PROPIEDAD FUNDAMENTAL DEL PRODUCTO DIRECTO DE MÓDULOS. Sean $M_i,\ i \in I$ una familia de R-módulos y sea $M = \Pi_{i\in I} M_i$ el producto directo de los M_i. Entonces para cada R-módulo M' y cada familia de homomorfismos de módulos $f_i : M' \to M_i$ existe un único homomorfismo de módulos $f : M' \to M$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:



Es más, Si $\hat{M}$ es un R-módulo y $\rho_i : \hat{M} \to M_i$ son una familia de epimorfismos de anillos tales que para cada anillo M' y cada familia de homomorfismos de anillos $f_i : M' \to M_i$ existe un único homomorfismo de anillos $f : M' \to \hat{M}$ tal que para cada $k \in I$ el diagrama anterior es conmutativo, entonces $\hat{M}$ es isomorfo a $\Pi_{i\in I} M_i$.

8. SUMA DIRECTA DE MÓDULOS

8.1 PROPOSICIÓN Sea R un anillo unitario, I un conjunto de indices y M_i, $i \in I$ una familia de R-módulos. Entonces

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \in \Pi_{i\in I} M_i \mid m_i = 0 \quad \text{para casi todo } i\}$$

$\star$ Con suma: $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$

$\star$ y producto dado por componentes, $r(m_i)_{i\in I} = (rm_i)_{i\in I}$

tiene estructura de R-módulo, llamado la **suma directa externa** de los M_i.

Nota: Si $\#I < \infty$ se tiene que la suma directa y el producto directo son isomorfos.

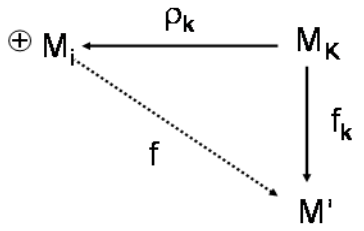
8.2 DEF: Sean $\{M_i\}_{i\in I}$ una familia de R-módulos y sea $\bigoplus_{i\in I} M_i$ la suma directa de éstos. Entonces para cada $k \in I$ se define la **inclusión canónica** de M_k en $\bigoplus_{i\in I} M_i$ y se representa por

$$\rho_k : M_k \to \bigoplus_{i\in I} M_i$$

como $\rho_k(m_k) = (x_i)_{i\in I}$ en donde $x_i = 0$ si $i \neq k$ y $x_k = m_k$. Es decir, el vector de $\Pi_{i\in I} M_i$ que tiene todas las coordenadas cero, salvo la k que vale m_k. Es claro que ρ_k es un monomorfismo de anillos.

8.3 PROPIEDAD FUNDAMENTAL DE LA SUMA DIRECTA DE R-MÓDULOS. Sean $\{M_i\}_{i\in I}$ una familia de R-módulos y sea $\bigoplus_{i\in I} M_i$ la suma directa de éstos.

Entonces para cada R-módulo M' y cada familia de homomorfismos de R-módulos $f_i : M_i \to M'$ existe un único homomorfismo de R-módulos $f : \bigoplus_{i\in I} M_i \to M'$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:



Es más, Si $\hat{M}$ es un R-módulo y $g_i : M_i \to \hat{M}$ son una familia de monomorfismos de R-módulos tales que para cada R-módulo M' y cada familia de homomorfismos de R-módulos $f_i : M_i \to M'$ existe un único homomorfismo de R-módulos $f : \hat{M} \to M'$ tal que para cada $k \in I$ el diagrama anterior es conmutativo, entonces $\hat{M}$ es isomorfo a $\bigoplus_{i\in I} M_i$.

Nota: La suma directa de módulos es la noción "dual" del producto directo de módulos.

9. OPERACIONES CON SUBMÓDULOS

En esta sección va a quedar patente la gran diferencia entre los espacios vectoriales y los módulos. Aquí estudiaremos dependencia e independencia, bases (caso de que existan) y submódulos generados.

9.1 Proposición Sea R un anillo unitario, M un R-módulo por la izquierda y $\{N_i\}_{i\in I}$ una familia de R-submódulos de M. Entonces:

(i) Existe el mayor submódulo de M contenido en todos los N_i, es más, este submódulo es $\bigcap_{i\in I} N_i$.

(ii) Existe el menor submódulo de M que contiene a todos los N_i, es más, este submódulo es

$$\sum_{i\in I} N_i := \{\sum_{i\in I} n_i \quad \text{con } n_i \in N_i \quad \text{casi todos nulos}\}.$$

9.2 Def: Al submódulo dado en (ii) se le denomina la suma (interna) de los submódulos $\{N_i\}$ y se le representa por $\sum_i N_i$. Si para $k \in I$ se verifica que

$N_k \cap \sum_{i \neq k} N_i = \{0\}$, diremos que la suma de los N_i es directa. En este caso, la suma interna de los N_i es isomorfa a la suma directa externa de los módulos $\{N_i\}$.

Nota: La unión de submódulos no tiene que ser un submódulo.

9.3 DEF: Sea R un anillo unitario y M un R-módulo por la izquierda sobre R. Diremos que un submódulo N de M es un sumando directo de M si $M = N \oplus N'$ para N' un submódulo de M.

9.4 DEF: Sea R un anillo unitario y sean M, M' dos R-módulos por la izquierda sobre R. Un monomorfismo de módulos $f : M \to M'$ se dirá que es directo si $\mathrm{Im}(f)$ es sumando directo de M'. Un epimorfismo $f : M \to M'$ se dirá que es directo si $\mathrm{Ker}(f)$ es un sumando directo de M.

9.5 DEF: Sea R un anillo unitario, M un R-módulo por la izquierda y $X \subset M$. Se define una combinación lineal de elementos de X como cualquier elemento $m \in M$ tal que existan $r_i \in R$ y $x_i \in X$ con $m = \sum_{i=1}^{n} r_i x_i$.

Nota: En algunos casos entenderemos por combinación lineal, no al elemento m en si, sino a la expresión formal $\sum_{i=1}^{n} r_i x_i$.

9.6 PROPOSICIÓN Sea R un anillo unitario, M un R-módulo por la izquierda y $U \subset M$. Entonces existe el menor submódulo de M que contiene a U. A este submódulo se le denomina el submódulo generado por U y se le representa por $< U >$. Es más,

$$< U >= \{ \sum_{finitas} x_i u_i \quad u_i \in U, x_i \in R\}$$

Es decir, $< U >$ es el subconjunto de todas las combinaciones lineales de elementos de U.

9.7 DEF: Sea R un anillo unitario y M un R-módulo por la izquierda. Diremos que un subconjunto U de M es un sistema de generadores de M si el submódulo generado por U es M, es decir, $< U >= M$. Es claro que M siempre es un sistema de generadores de M. Diremos que M es finitamente generado si posee un sistema de generadores finito.

9.8 DEF: Sea R un anillo unitario y M un R-módulo por la izquierda. Diremos que un subconjunto U de M es un conjunto independiente si toda combinación lineal de elementos de U igual a cero forzosamente tiene todos sus escalares cero.

Nota: En espacios vectoriales todo vector no nulo forma un conjunto de vectores independientes. En el caso de módulos este resultado no es cierto. Es más, en $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo no hay conjuntos de vectores independientes.

9.9 Def: Sea R un anillo unitario y M un R-módulo por la izquierda de R. Diremos que $B \subset M$ es una base de M si es un conjunto independiente y un sistema de generadores de M.

Nota: No todo R-módulo posee base. Por ejemplo $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo no posee base.

9.10 Def: Sea R un anillo unitario y M un R-módulo por la izquierda de R. Diremos que M es libre, si posee una base.

Nota: en el caso de espacios vectoriales, el cardinal de una base es un invariante, llamado la dimensión, en módulos esto no sucede.

9.11 Proposición Sea R un anillo unitario, M un R-módulo por la izquierda y $\{m_i\}_{i\in I}$ un subconjunto de M. Entonces la aplicación

$$f : \oplus_{i\in I} R \to M, \quad \text{definido por} \quad (\sum_{i\in I}^{finita} x_i)f = \sum_{i\in I}^{finita} x_i m_i$$

es un homomorfismo de R-módulos. Es más,

(i) f es un monomorfismo si y sólo si $\{m_i\}_{i\in I}$ es una familia de vectores independientes.

(ii) f es sobreyectiva si y sólo si esta familia es un sistema de generadores de M.

9.12 Corolario Sea R un anillo unitario y M un R-módulo por la izquierda libre. Entonces, si $B = \{b_i\}_{i\in I}$ es una base para M, $M \cong \pi_{i\in I} R_i$ con $R_i \cong R$ para todo i.

9.13 Teorema Sea M un R módulo libre con base $\{b_i\}_{i\in I}$. Entonces para cada R-módulo N y cada subconjunto $\{n_i\}_{i\in I}$ existe un único homomorfismo de R-módulos $f : M \to N$ tal que $(b_i)f = n_i$.

9.14 Corolario I Sea R un anillo unitario. Entonces todo R-modulo por la izquierda es cociente de un R-módulo libre. Es más, si M es finitamente generado, M es cociente de un módulo libre con base finita.

9.15 Corolario II Sea R un anillo unitario y M un R-módulo por la izquierda Libre. Entonces, para cada par de R-módulos N, N' y homomorfismos de R-módulos $f : M \to N$ y $g : N' \to N$ con g sobreyectivo, existe un homomorfismo de R-módulos (no necesariamente único) $h : M \to N'$ que hace conmutativo el diagrama, $hg = f$.

10. SUCESIONES DE MÓDULOS

10.1 Def: Sea R un anillo unitario. Se define una sucesión de R módulos como una familia $\{M_i\}_{i\in\mathbb{Z}}$ de R módulos junto con una familia $f_i : M_i \to M_{i+1}$ de homomorfismos de R-módulos tales que para cada $i \in \mathbb{Z}$, $f_i f_{i+1} = 0$. Es decir,

$$\cdots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

en donde $\mathrm{Im}(f_i) \subset \mathrm{Ker}(f_{i+1})$. En caso de que $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$, diremos que la sucesión $\{M_i\}_{i\in\mathbb{Z}}$ es exacta. Una sucesión exacta de la forma

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

se dirá exacta corta. Diremos que una sucesión exacta corta de R módulos es escindida si $\mathrm{Ker}(g) = \mathrm{Im}(f)$ es un sumando directo de M.

Nota: Sea M es un R-módulo y N es un submódulo suyo, la sucesión

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} M/N \longrightarrow 0$$

es exacta corta. Si M y M' son dos R-módulos, la sucesión

$$0 \longrightarrow M \xrightarrow{f} M \oplus M' \xrightarrow{g} M' \longrightarrow 0$$

en donde $f(m) = (m, 0)$ y $g(m + m') = m'$ es una sucesión exacta corta escindida.

10.2 Proposición Sea R un anillo unitario y $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ una sucesión exacta corta de R módulos. Las siguientes condiciones son equivalentes:

(i) Existe un homomorfismo de R-módulos $g' : P \to M$ tal que $g'g = \mathrm{Id}_P$.

(ii) La sucesión es escindida.

(ii) Existe un homomorfismo de R-módulos $f' : M \to N$ tal que $ff' = \mathrm{Id}_N$.

Bibliografía

[1] **H. Cartan y S. Eilenberg** " Homological algebra", Princeton U. Press, 1956.

[2] **N. Jacobson** "Basic algebra I y II", W. H. Freeman and company, 1980.

[3] **D.G. Northcott** "An introduction to homological algebra", Cambridge University Press, 1972.

[5] **C.A. Weibel** "History of homological algebra", dirección de internet:

http://www.math.uiuc.edu/K-theory/0245/

[6] **K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov** & **A.I. Shirshov** "Rings that are nearly associative". Academic Press, New York, 1982.