Teoría de Módulos

José Luis Tábara

jltabara@gmail.com

Índice

1. Definición de A-módulo

Salvo mención explícita de lo contrario, siempre supondremos que todos los anillos son conmutativos y poseen unidad.

Definición 1.1 *Sea A un anillo, M un grupo abeliano. M posee una estructura de A-*módulo *si está dotado de una operación externa, llamada* multiplicación por escalares *, $\phi : A \times M \to M$ que verifica (denotando $\phi(a, m)$ por am)*

I) $a(m + m') = am + am'$

II) $(a + b)m = am + bm$

III) $a(bm) = (ab)m$

IV) $1m = m$

donde a, b denotan elementos del anillo y m, m' elementos del grupo abeliano M.

Por lo general y siguiendo la notación del Algebra Lineal, los elementos del anillo se llamarán escalares y los elementos del grupo abeliano se denominarán vectores.

Consideremos la aplicación

$$\begin{array}{rccc} \lambda_a & : & M & \to & M \\ & & a & \to & am \end{array}$$

Dicha aplicación se denomina translación a la izquierda por a. La propiedad $i)$ nos dice que λ_a es un morfismo del grupo aditivo M. Esto nos permite construir una aplicación λ que mande el escalar a a la operación λ_a

$$\begin{array}{rccc} \lambda & : & A & \to & \mathrm{End}_{gr}(M) \\ & & a & \to & \lambda_a \end{array}$$

Las tres últimas propiedades nos indican que esta aplicación λ es un morfismo de anillos. Por ello podemos establecer la siguiente

Definición 1.2 *Una estructura de A-*módulo *en un grupo abeliano M es un morfismo de anillos con unidad de A en* $\mathrm{End}_{gr}(M)$.

Para reconstruir la multiplicación por escalares defínase $am = \lambda(a)(m)$ si λ denota el morfismo de anillos.

Visto desde esta perspectiva un módulo es una representación del anillo A en el grupo abeliano M. Emplearemos la notación $\lambda : A \to \mathrm{End}_{gr}(M)$ para referirnos a esta representación.

Ejemplos.

- Si A es un anillo, el producto $A \times A \to A$ define una estructura canónica de A-módulo en el anillo A. Salvo que se diga lo contrario, siempre consideraremos en A esta estructura de A-módulo.
- Si $\mathfrak{a}$ es un ideal, el producto por elementos de A lo dota de una estructura de A-módulo.
- Los módulos sobre un anillo que sea un cuerpo son los espacios vectoriales.
- Cada grupo abeliano admite una estructura natural de módulo sobre el anillo $\mathbb{Z}$ de los enteros. Si g es un elemento del grupo entonces

  $$ng = g + \overset{n)}{\ldots} + g$$

  Esta es la única estructura de $\mathbb{Z}$-módulo que admite pues $1g$ debe ser g, $2g = (1+1)g = g + g$ y se sigue por inducción. Si consideramos el módulo como una representación de A, entonces $\lambda : \mathbb{Z} \to \mathrm{End}_{gr}(M)$ es el morfismo de anillos que nos permite calcular la característica del anillo $\mathrm{End}_{gr}(M)$.
- Sea $k[x]$ el anillo de polinomios sobre el cuerpo k y E un espacio vectorial. Dado un endomorfismo φ del espacio E, existe un único morfismo de k-álgebras que manda el polinomio x al endomorfismo φ. Esto nos da una estructura de $k[x]$-módulo en el grupo abeliano E. Dicho módulo se denotará E_φ.

- Si B es un subanillo de A, todo A-módulo es un B-módulo, sin más que considerar la multiplicación por elementos de B como la restricción de la multiplicación por elementos de A. También se puede entender como la restricción a B del morfismo de anillos que define la estructura de A-módulo.

- El grupo aditivo A^n es un módulo sobre el anillo A, mediante la multiplicación componente a componente

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

- Si $\varphi : A \to A'$ es un morfismo de anillos y M es módulo sobre A', entonces M es un módulo sobre A definiendo

$$am = \varphi(a).m$$

  Se dice que este módulo se ha obtenido por restricción de escalares. Entendiendo el módulo como una representación λ del anillo A', la estructura de módulo sobre A se obtiene componiendo el morfismo λ con φ.

- $A(x_1, \ldots, x_n)$ y $A[[x]]$ (anillo de las series formales) son módulos sobre A de modo natural puesto que A es un subanillo de ambos.

Llamamos anulador de un módulo y denotamos $\mathrm{Ann}(M)$ al núcleo de la representación asociada. Como sabemos por teoría de anillos, el anulador es un ideal del anillo A. Decimos que el módulo es fiel si su anulador es el cero. Si $\mathfrak{a}$ es cualquier ideal de $\mathrm{Ann}(M)$, por el teorema de factorización de anillos, tenemos un morfismo bien definido de $A/\mathfrak{a}$ en $\mathrm{End}_{gr}(M)$. Esto dota a M de una estructura de $(A/\mathfrak{a})$-módulo. En particular M tiene siempre una estructura de módulo sobre $A/\mathrm{Ann}(M)$. Además por la definición de ideal anulador este módulo siempre es fiel.

Desde este punto hasta el final de esta sección, A será un anillo con unidad, pero no conmutativo.

Definición 1.3 *Una estructura de* A-módulo por la izquierda *en un grupo abeliano* M *es la dada por un morfismo de anillos con unidad de* A *en los endomorfismos grupales de* M*.*

Decimos que una función $\phi : A \to A'$ es un antimorfismo de anillos con unidad si:

I) $\phi(x+y) = \phi(x) + \phi(y)$

II) $\phi(1) = 1$

III) $\phi(xy) = \phi(y).\phi(x)$

Definición 1.4 *Una estructura de* A-módulo por la derecha *en un grupo abeliano* M *es la dada por un antimorfismo de anillos con unidad de* A *en los endomorfismos grupales de* M*.*

Ejemplos.

- Todo anillo no conmutativo A está dotado de una estructura natural de A-módulo por la derecha, dada por la multiplicación. En este caso el segundo factor debe entenderse como anillo de escalares y el primero como conjunto de vectores. Cuando se considere en A esta estrucura de A-módulo se denotará por A_A. Análogamente se puede definir una estructura de módulo por la izquierda.
- Todo ideal por la derecha del anillo es un módulo por la derecha.
- De la misma forma A^n, mediante la multiplicación por escalares coordenada a coordenada es A-módulo por la derecha.
- Todo grupo abeliano G es un módulo por la izquierda sobre el anillo no conmutativo $\mathrm{End}_{gr}(G)$. Toda estructura de A-módulo sobre G se obtiene por restricción de escalares de este módulo.

Si en la definición de módulo quitamos la condición $1m = m$ entonces decimos que estamos ante un A-módulo sin unidad. El morfismo de anillos

que define la estructura puede mandar a la unidad de A (si existe) a un operador distinto de la identidad.

El lector interesado intentará encontrar qué construcciones o resultados dados en el texto para anillos conmutativos, son generalizables a los otros tipos de módulos.

Problemas

1 Probar que

- $a \cdot 0 = 0$
- $0 \cdot m = 0$
- $(-a)m = -(am) = a(-m)$
- $z(am) = a(zm)$ donde z es un número entero.

2 Dotar de estructura de A-módulo al grupo aditivo $A/\mathfrak{a}$ donde $\mathfrak{a}$ es un ideal de A.

3 Consideremos en A la estructura natural de A-módulo. Probar que la representación asociada es inyectiva y que por lo tanto A es un subanillo de $\mathrm{End}_{gr}(A)$. Dicha representación se llama *representación regular* del anillo A. Este resultado es el análogo al *teorema de Cayley* para grupos.

4 Sea V un espacio vectorial sobre un cuerpo k. Ver que V es también un módulo sobre el anillo (no conmutativo) $\mathrm{End}(V)$.

5 Dar la definición estandard de módulos por la derecha y por la izquierda.

6 Construir un módulo sin unidad sobre el anillo de los enteros.

7 Probar que M es fiel sobre el anillo $A/\operatorname{Ann}(M)$

8 Sea $m \in M$ un elemento no nulo. Llamamos *anulador de* m y denotamos $\mathrm{Ann}(m)$ al subconjunto de A formado por los escalares que anulan a m.

- Probar que $\mathrm{Ann}(m)$ es un ideal.
- Probar que
$$\mathrm{Ann}(M) = \bigcap_{m \in M} \mathrm{Ann}(m)$$

9 Un módulo es *cíclico* se existe un elemento $m \in M$ de tal forma que todo otro elemento $m' \in M$ sea de la forma $m' = am$.

- Probar que $\mathbb{Z}_n$ es un $\mathbb{Z}$-módulo cíclico.
- Probar que V es un $\mathrm{End}(V)$-módulo cíclico si V es un k-espacio vectorial.
- Ver si existe alguna relación entre el anulador de m y este ejercicio.

10 Sea X un conjunto cualquiera. Consideremos las funciones $f : X \to A$. Dotar a este conjunto de funciones de estructura de A-módulo. Estudiar en particular el caso en que X es finito.

11 Sea el módulo E_φ. El anulador de este módulo es un ideal del anillo de polinomios y como tal está generado por un polinomio cuyo primer coeficiente es 1. Dicho polinomio se denomina *polinomio anulador* del módulo o polinomio anulador del endomorfismo φ. Se sabe por Algebra Lineal que si el k-espacio E es de dimensión finita, el *polinomio característico* de φ anula al módulo. Por lo tanto el anulador debe ser un divisor del polinomio característico. Para más detalles véase el teorema de Cayley-Hamilton en algún libro de Algebra Lineal.

12 Sea $M_{n,m}(A)$ el conjunto de las matrices $n \times m$ con coeficientes en A. Introducir en este conjunto una estructura de A-módulo.

Denotando por $M_n(A)$ al conjunto de matrices cuadradas de orden n, probar que $M_{n,m}(A)$ puede dotarse de una estructura de módulo por la izquierda sobre el anillo $M_n(A)$ mediante la multiplicación matricial.

13 Sea M un A-módulo. Sea $M[x]$ el conjunto de polinomios con coeficientes en M. Probar que $M[x]$ es un A-módulo. Definir en $M[x]$ una estructura de $A[x]$-módulo.

14 Sea $\phi : A \to A$ un antimorfismo de anillos con unidad. Probar que cada estructura de módulo por la izquierda induce una estructura de módulo por la derecha definiendo

$$m.a = \phi(a).m$$

Sea $k(G)$ el álgebra del grupo G sobre el cuerpo k. Este álgebra está formada por las combinaciones lineales finitas de elementos de G con coeficientes en k. Probar que

$$\varphi(\sum_{g\in G} \lambda_g g) = \sum_{g\in G} \lambda_g g^{-1}$$

es un antimorfismo de anillos con unidad.

Consideremos en el conjunto $\mathbb{H}$ de los cuaterniones la conjugación

$$a + xi + yj + zk \to a - xi - yj - zk$$

Probar que es un antimorfismo de anillos con unidad.

2. Morfismos de módulos

Por M y N denotaremos siempre A-módulos.

Definición 2.1 *Una aplicación $\varphi : M \to N$ se dice que es un* morfismo de A-módulos *(aplicación A-lineal o simplemente* aplicación lineal *si se sobreentiende el anillo) si cumple:*

I) *φ es morfismo de los grupos aditivos.*

II) *$\varphi(am) = a\varphi(m)$ para todo a y todo m. Esto equivale a que φ "conmute" con λ_a para todo a. $\varphi\lambda_a = \lambda_a\varphi$*

Si $\varphi : M \to N$ y $\varphi' : N \to P$ son lineales, entonces su composición $\varphi'\,\varphi : M \to P$ es un morfismo de módulos.

Los morfismos se dirán que son inyectivos o epiyectivos cuando lo sean las aplicaciones que los definen. $\varphi : M \to N$ es un isomorfismo cuando la aplicación sea biunívoca. En este caso la aplicación inversa $\varphi^{-1} : N \to M$ es lineal, y por ser biunívoca es un isomorfismo.

En el caso en que $M = N$ normalmente los isomorfismos reciben el nombre de automorfismos. La aplicación identidad de un módulo M en si mismo es siempre un automorfismo, que se denotará por Id (o Id_M si hay riesgo de confusión)

Al ser la composición de automorfismos de nuevo un automorfismo, estos forman un grupo respecto a la composición. Se le denota $\mathrm{GL}(M)$. Es el grupo lineal de M.

Dos módulos se dirán que son isomorfos cuando exista al menos un isomorfismo entre ellos. Es claro que la relación de isomorfía es de equivalencia.

El conjunto de todos los morfismos de A-módulo de M en N se denota $\mathrm{Hom}_A(M, N)$ o simplemente $\mathrm{Hom}(M, N)$ si se sobreentiende el anillo. Este último conjunto tiene una estructura natural de A-módulo definida por las operaciones:

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

$$(af)(m) = a(fm)$$

Teniendo en cuenta la conmutatividad del anillo se prueba que tanto $f+g$ como af son lineales.

En el caso en que $M = N$ la composición introduce una estructura de anillo en $\mathrm{Hom}(M, N)$. La aplicación λ_a es lineal. De esta forma $\mathrm{End}_A(M)$ es un álgebra sobre A, via el morfismo $\lambda : A \to \mathrm{End}_A(M)$.

Ejemplos.

- $\mathrm{Hom}(A, M) = M$. A cada morfismo $\varphi : A \to M$ le corresponde $\varphi(1)$. Recíprocamente, dado $m \in M$ existe un único morfismo de módulos φ tal que $\varphi(1) = m$. Naturalmente este morfismo debe cumplir

$$\varphi(a) = a\varphi(1) = am$$

- Toda aplicación lineal entre espacios vectoriales.
- La inyección canónica de un ideal en el anillo.
- Si φ es A-lineal, entonces φ es B-lineal si B es un subanillo de A.

- Todo morfismo de grupos, entre dos grupos abelianos, entendidos como módulos sobre $\mathbb{Z}$, es lineal.
- $\varphi_0 : M \to N$ definida como

$$\varphi_0(m) = 0 \text{ para todo } m$$

es lineal. φ_0 es el elemento neutro de $\mathrm{Hom}(M, N)$ y por consiguiente lo notaremos como 0.

- Consideremos a $\mathbb{Z}$ como un $\mathbb{Z}$-módulo. La aplicación $n \to 2n$ es morfismo de módulos pero no de anillos. Debemos diferenciar claramente la estructura que consideramos en $\mathbb{Z}$ para poder hablar de morfismos sin ambigüedad.
- Sea $\mathbb{C}$ un módulo sobre si mismo. La conjugación compleja $z \to \overline{z}$ es morfismo de anillos pero no lo es de módulos.

Problemas

15 Probar que efectivamente la composición de dos aplicaciones lineales es lineal. Lo mismo con la suma y con el producto por un escalar. Comprobar que para que el producto por un escalar sea morfismo es primordial que A sea conmutativo.

16 Una aplicación $\varphi : M \to N$ es un isomorfismo si y solo si existe $\varphi' : N \to M$ tal que $\varphi'\varphi = \mathrm{Id}$ y $\varphi\varphi' = \mathrm{Id}$.

17 Todo morfismo epiyectivo es simplificable por la derecha. En diagramas

$$M \xrightarrow{\phi} N \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} N$$

$$\varphi_1 \, \phi = \varphi_2 \, \phi \quad \Rightarrow \quad \varphi_1 = \varphi_2$$

Todo morfismo inyectivo es simplificable por la izquierda. Dar nuevas definiciones de inyectividad y epiyectividad.

18 Sea E_φ el $k[x]$-módulo asociado a un endomorfismo φ. Probar que la multiplicación por x es una aplicación lineal de dicho módulo.

19 Sean E_φ y $E_{\varphi'}$ dos $k(x)$-módulos. Probar que los módulos son isomorfos si y solo si existe un automorfismo τ del espacio vectorial que cumple $\varphi' = \tau\,\varphi\,\tau^{-1}$. Así los dos endomorfismos son equivalentes y existen bases donde tienen la misma matriz.

20 Demostrar los siguientes enunciados:

- Todo endomorfismo de $\mathbb{Z}$ es la multiplicación por un escalar. Demostrar que $\mathrm{End}(\mathbb{Z})$ y $\mathbb{Z}$ son isomorfos como anillos.
- A todo endomorfismo de $\mathbb{Z}^2$ se le puede asociar una matriz 2×2 con coeficientes enteros. Ver que esta correspondencia es biunívoca. Dar la condición para que un endomorfismo de $\mathbb{Z}^2$ sea invertible.
- Calcular los endomorfismos del grupo cíclico $\mathbb{Z}_n$. Calcular los automorfismos de dicho grupo abeliano.

21 Probar que si el anillo no es conmutativo, en general la aplicación af no será lineal.

Si A no es conmutativo $\mathrm{Hom}_A(M, N)$ tiene una estructura de módulo por la izquierda sobre el anillo $\mathrm{End}_A(M, M)$.

3. Submódulos y cocientes

Sea M un módulo. Se dice que un subgrupo M' de M es un submódulo si $am' \in M'$ cuando $m' \in M$ y esto ocurra para todo a.

Proposición 3.1 *Un conjunto $M' \subset M$ es un submódulo si y sólo si es cerrado por combinaciones lineales.*

Si $\varphi : M \to N$ es lineal, entonces la imagen de un submódulo de M es un submódulo de N. La imagen inversa de un submódulo de N es un submódulo de M.

Demostración.

Exactamente igual que para espacios vectoriales. □

En particular la antiimagen del cero (que es siempre un submódulo) es un submódulo de M llamado núcleo de la aplicación φ. Se denota $\mathrm{Ker}(\varphi)$.

Todo submódulo puede considerarse como un A-módulo con las operaciones inducidas.

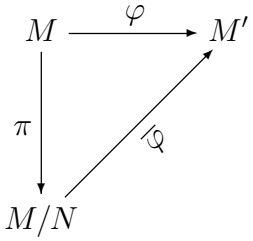
Si N es un submódulo de M, en el grupo abeliano M/N existe una única estructura de A-módulo que hace que el morfismo canónico de paso al cociente $\pi : M \to M/N$ sea una aplicación lineal. Entonces la multiplicación por escalares debe estar definida como

$$a.\pi(m) = \pi(am)$$

La definición anterior es independiente del representante. El módulo que acabamos de construir es el cociente de M módulo N.

El teorema de factorización canónica que se ha visto para otras estructuras, es también válido para los módulos.

Si $\varphi : M \to M'$ es un morfismo cuyo núcleo contenga a un submódulo N, entonces existe una única aplicación lineal $\overline{\varphi}$ que hace conmutativo el diagrama



Por lo tanto $\overline{\varphi}$ debe actuar de la siguiente manera

$$\overline{\varphi}(\pi(m)) = \varphi(m)$$

y no depende del representante que tomemos.

Proposición 3.2 *Si $\pi : M \to M/N$ es la proyección canónica, los submódulos de M/N se corresponden canónicamente con los submódulos de M que contienen a N. A cada submódulo N' le hacemos corresponder $\pi^{-1}(N')$.*

Los submódulos de A son precisamente los ideales. Entonces en el caso particular de que $M = A$ se reencuentra el resultado conocido de Teoría de anillos.

Proposición 3.3 *Un morfismo es inyectivo si y sólo si su núcleo es el submódulo cero.*

Ejemplos

- Un ideal de A es un submódulo y recíprocamente.
- Si $\mathfrak{a}$ es un ideal de A entonces existe una estructura natural de módulo en $A/\mathfrak{a}$.
- Todo subgrupo es un $\mathbb{Z}$-submódulo y recíprocamente.
- El conjunto de las funciones infinitamente diferenciables sobre $\mathbb{R}$ es un subespacio del de todas las funciones continuas en $\mathbb{R}$.
- Sea G un grupo abeliano. El conjunto de los elementos de G cuyo orden es una potencia de un primo p forman un submódulo G_p.
- Los espacios cocientes y los subespacios.
- $n\mathbb{Z}$ es un submódulo de $\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ es el módulo cociente. El cardinal de $\mathbb{Z}_n$ es n, que es menor que $\aleph_0$. Así encontramos un módulo distinto de cero que es "más pequeño" que el anillo. Como sabemos esto no ocurría nunca en los espacios vectoriales.

- Sea $m \in M$ no nulo. El conjunto

$$Am = \{a.m \quad \text{con } a \in A\}$$

es un submódulo de M.

- En E_φ un submódulo es un subespacio V que cumple $\varphi(V) \subset V$. En álgebra lineal V se denomina subespacio invariante por φ.

Definición 3.1 *Decimos que un módulo es* cíclico *si existe un vector $m \in M$ de tal manera que $M = Am$.*

Proposición 3.4 *Todo módulo cíclico es isomorfo al cociente del anillo módulo un ideal.*

Demostración.

Definimos $\rho_m : A \to M$ por la fórmula $\rho_m(a) = am$. Esta aplicación es un morfismo de módulos. Al ser cíclico ρ_m es epiyectivo. Su núcleo es un ideal y por el teorema de factorización M es isomorfo a $A/\mathfrak{a}$. □

Seguiremos con algunos isomorfismos canónicos entre módulos que generalizan lo obtenido para grupos. Se deben a Emmy Noether.

El primero es de factorización canónica y a estas alturas ya es suficientemente conocido.

Teorema 3.5 *Sea $\varphi : M \to N$ lineal. Entonces*

$$M/\ker(\varphi) \sim \mathrm{Im}(\varphi)$$

Teorema 3.6 *Sea $N \subset M \subset L$ submódulos*

$$(L/N)/(M/N) \sim L/M$$

Demostración.

Definimos $\varphi : L/N \to L/M$ como $\varphi(\pi_N(x)) = \pi_M(x)$ que es lineal y epiyectiva. $\pi_N(x)$ está en el núcleo de φ si $x \in M$. Entonces el núcleo de la aplicación es M/N. $\square$

Teorema 3.7 *Si M_1, M_2 son dos submódulos de M*

$$(M_1 + M_2)/(M_1) \sim M_2/(M_1 \cap M_2)$$

Demostración.

Definimos el morfismos canónico

$$\overline{\pi} : M_2 \to (M_1 + M_2)/M_1$$

$\overline{\pi}(x) = 0 \Leftrightarrow x \in M_2$ y $x \in M_1 \Leftrightarrow x \in M_1 \cap M_2$. Como $\overline{\pi}$ es epiyectivo terminamos aplicando el teorema de factorización. $\square$

Definición 3.2 *Un módulo es* simple *si sus únicos submódulos son el mismo M y el cero.*

Definición 3.3 *Si M es un módulo, decimos que un submódulo N es* máximal *si para todo submódulo N' que contenga a N se tiene que o bien $N' = N$ o bien $N' = M$.*

Proposición 3.8 *Un submódulo $N \subset M$ es maximal $\Leftrightarrow$ M/N es simple.*

Demostración.

Nos basamos en la proposición 3.2.

Si N es maximal, entonces en M/N sólo pueden existir dos submódulos. Por lo tanto M/N es simple.

Si M/N es simple cualquier submódulo N' que contenga a N tiene como imagen un submódulo de M/N. Pero como este es simple necesariamente N' debe ser igual a N o a M. $\square$

Lema 3.9 (Schur) *Si M es simple, entonces* $\mathrm{End}(M)$ *es un* anillo con división.

Demostración.

Sea $\varphi \in \mathrm{End}(M)$ no nulo. $\mathrm{Ker}(\varphi)$ no es todo el espacio, luego por ser M simple debe ser cero. Así φ es inyectivo.

$\mathrm{Im}(\varphi)$ es un submódulo y como φ no es nulo necesariamente $\mathrm{Im}(\varphi) = M$. Luego φ es epiyectivo. Así concluimos que φ es invertible siempre que no sea nulo. □

Debemos tener cuidado pues en general el anillo con división no será conmutativo.

Corolario 3.10 *Si M es simple, entonces es un espacio vectorial sobre el cuerpo (posiblemente no conmutativo)* $\mathrm{End}(M)$.

Proposición 3.11 *Todo A-módulo simple es el cociente de A por un ideal maximal.*

Demostración.

Sea M simple, $m \in M$ y distinto de cero. La aplicación lineal $\rho_m : A \to M$ que manda el 1 hasta m es epiyectiva por ser M simple. Su núcleo es un ideal (o sea un submódulo de A) y debido a la correspondencia entre submódulos de M y submódulos(= ideales) de A, debe ser maximal. Se acaba aplicando el teorema de factorización. □

De este teorema se deduce que la variedad de módulos simples no isomorfos dependerá en gran medida de la cantidad de ideales maximales del anillo.

Problemas

22 Si M es simple $\Rightarrow$ $\mathrm{Ann}(m)$ es un ideal maximal para todo $m \in M$. Si M es simple entonces es cíclico. Ver si el recíproco es cierto.

23 Sea A un dominio de integridad y M un módulo. Un vector $m \in M$ es de *torsión* si existe un escalar a tal que $am = 0$. Designamos por M_τ al conjunto de todos los vectores de torsión de M. Decimos que M es un *módulo de torsión* si $M = M_\tau$. Decimos que no tiene torsión si $M_\tau = 0$.

- M_τ es un submódulo.
- M/M_τ tiene torsión cero.
- Los submódulos y los cocientes de módulos de torsión son de torsión.
- En un grupo abeliano un elemento es de torsión si y solo si es de orden finito.
- Probar que $\mathbb{Q}$ entendido como $\mathbb{Z}$-módulo no tiene torsión.
- Probar que $\mathbb{Q}/\mathbb{Z}$ es un módulo de torsión sobre $\mathbb{Z}$.
- Ver si la condición de que A sea dominio de integridad es o no fundamental para los resultados de este problema.

24 Sea $\mathfrak{a} \subset A$ un ideal. M un A-módulo. El conjunto de todas las sumas finitas $\sum' a_i m_i$ con $a_i \in \mathfrak{a}$ es un submódulo de M. Denotamos este submódulo por $\mathfrak{a}M$. Hacer lo mismo con un submódulo $M' \subset M$.

¿Ocurre siempre que e $\mathfrak{a}M$ es distinto de cero si $\mathfrak{a}$ lo es?

25 Sea M un A-módulo. Sea $N_1 \subset N_2 \subset \cdots \subset N_n \subset \ldots$ una cadena de submódulos. Probar que la unión de esos submódulos es un submódulo.

26 Sea $\mathfrak{m}$ un ideal maximal de A. Probar que $M/\mathfrak{m}M$ es un espacio vectorial sobre el cuerpo $A/\mathfrak{m}$ definiendo

$$\pi(a)\pi(m) = \pi(am)$$

Utilizar esto para probar que si $A^m \sim A^n$ entonces $n = m$.

4. Retículo de submódulos

El conjunto de submódulos de M es un subconjunto de la clase de las partes de M.

$$Submodulos(M) \subset Partes(M)$$

Por lo tanto hereda una estructura de orden y es esa estructura natural la que consideraremos en lo que sigue.

Diremos que un submódulo N es menor que otro submódulo N' cuando $N \subset N'$. Se debe observar que en general el orden no es total.

La clase de todos los submódulos de M admite un máximo (o último elemento) y un mínimo (o primer elemento). El primer elemento es el módulo cero que es menor que cualquier submódulo. El último elemento es el propio M que contiene, como es obvio, a todo submódulo. Este conjunto además admite la siguiente estructura reticular.

Sea $\{N_i\}$ una familia, posiblemente infinita, de submódulos de M. Se define la suma de estos submódulos como el conjunto de todos los vectores de M que son combinación lineal finita de elementos de $\bigcup N_i$. Se denotará $\sum N_i$ y es un sumódulo. Entonces todo vector de $\sum N_i$ se puede escribir de la forma $\sum' n_i$ con $n_i \in N_i$, donde el apóstrofe indica que la suma es finita (casi todos los n_i deben ser cero).

Es evidente que $\sum N_i$ es mayor que todos los submódulos N_i y que si H es un submódulo que contiene a todos los N_i, necesariamente contiene a $\sum N_i$, puesto que debe contener a todas las combinaciones lineales formadas con elementos de los submódulos. Por lo tanto $\sum N_i$ es el supremo de los N_i respecto al orden dado por la inclusión natural.

Dados $\{N_i\}$, su intersección conjuntista es un submódulo contenido en todos los N_i. Si H es un submódulo contenido en todos los N_i, necesariamente está contenido en $\bigcap N_i$. Así $\bigcap N_i$ es el ínfimo de la familia $\{N_i\}$.

Esto se resume en la siguiente

Proposición 4.1 *El conjunto de submódulos de M es un* retículo completo *con elemento máximo y mínimo.*

Como en todo retículo con primer y último elemento, existe la noción de

suplementario.

Definición 4.1 *$N \subset M$ admite un* suplementario *si existe otro submódulo N' tal que se tenga:*

I) $N + N' = M \Leftrightarrow \sup(N, N') =$ *elemento máximo*

II) $N \cap N' = 0 \Leftrightarrow \text{ínf}(N, N') =$ *elemento mínimo*

El suplementario, caso de existir, no tiene porqué ser único, contrariamente a lo que ocurre en el retículo de todas las partes de M. Si un submódulo admite un suplementario se dice que ese submódulo es un sumando directo.

Es un resultado conocido de Algebra Lineal, que todo subespacio vectorial admite al menos un suplementario. Es una consecuencia del lema de Zorn. Sin embargo esta afirmación es falsa, en general, para módulos.

Ejemplos.

- Sea $n\mathbb{Z}$ un submódulo de $\mathbb{Z}$. Este submódulo no admite suplementario puesto que si $m\mathbb{Z}$ es otro submódulo siempre se tiene que $n\mathbb{Z} \cap m\mathbb{Z}$ es no nulo.
- El mismo razonamiento se aplica al anillo de polinomios sobre un cuerpo.

Definición 4.2 *Se dice que un módulo es* semisimple *si todo submódulo es un sumando directo. Se dice que un módulo es* simple *si sus únicos submódulos son el cero y el total.*

Es claro que todo módulo simple es semisimple. Recordemos (véase proposición 3.11) que todo módulo simple es el cociente del anillo módulo un ideal maximal.

Enunciemos ahora un resultado de Algebra Lineal en nuestro lenguaje.

Teorema 4.2 *Sea k un cuerpo. Todo k-espacio vectorial es semisimple y todo k-módulo simple es isomorfo a k.*

Este par de propiedades son las que hacen tan sencillo el estudio lineal de los módulos sobre cuerpos. Todo anillo que goze de las mismas propiedades será asimismo de fácil estudio.

Sea ahora S un subconjunto arbitrario de M. Llamaremos submódulo generado por S, al mínimo submódulo que contiene a S. Coincide con la intersección de todos los submódulos que contienen a S, o también con el submódulo formado por todas las combinaciones lineales de elementos de S. Debido a esto último, el submódulo generado por S también se llama envolvente lineal de S.

Definición 4.3 *Un módulo M es de* generación finita *si es la envolvente lineal de algún subconjunto finito de M.*

Corolario 4.3 *Si k es un cuerpo y M un k-módulo. M es de generación finita si y solo si es de dimensión finita*

Teorema 4.4 *Un A-modulo M es de generación finita si y solo si existe un $n \in \mathbb{N}$ y un morfismo epiyectivo $\phi : A^n \to M$.*

Demostración.

$\Rightarrow$)$(m_1, \ldots, m_n)$ una familia generadora. El morfismo que manda a e_i hasta m_i es epiyectivo. Dicho morfismo se extiende por linealidad. Por e_i denotamos al elemento con todas las componentes nulas, salvo la que ocupa la posición i que es 1.

$\Leftarrow$)$\{e_i\}$ generan A^n. Entonces sus imagenes por una aplicación epiyectiva generan M. $\square$

Proposición 4.5 *Se cumplen los siguientes enunciados:*

I) *Si M es módulo y $\{N_i\}$ una colección finita de submódulos de generación finita, su suma $\sum N_i$ es también de generación finita.*

II) *El cociente de un módulo finito generado es finito generado.*

III) *Un sumando directo de un módulo finito generado es también finito generado.*

Demostración.

I) Tomamos un conjunto generador de cada N_i. La unión de todos esos generadores es finita y generan la suma.

II) Las imagenes de una familia generadora genera el cociente.

III) Si N es un sumando directo entonces $M = N + N'$ y $N \sim M/N'$ y se concluye por el apartado anterior. $\square$

Problemas

27 Sean $A \subset B$ dos anillos. Supongamos que M es de generación finita como módulo sobre el anillo B. Supongamos también que B es de generación finita como A-módulo. Probar que el A-módulo obtenido por restricción de escalares es finito-generado.

28 Sean $A \subset B$ dos anillos. M un módulo sobre B y sobre A por restricción de escalares. Ver la relación que hay entre sus retículos de submódulos. ¿Coinciden en general el A-módulo generado por una parte S y el B-módulo generado por el mismo conjunto?

29 Si N y M/N son de generación finita demostrar que M también.

30 ¿$\mathbb{Q}$ es finito-generado sobre $\mathbb{Z}$ o no lo es?

31 Si $M_1 \subset M_2 \subset \cdots \subset M_n \subset \ldots$, demostrar que la unión de submódulos coincide con la suma de dichos submódulos.

5. Categorías y functores

En esta sección daremos una pequeña introducción a la teoría de categorías y functores. El material cubierto en este capítulo no es imprescindible para comprender los siguientes. Sin embargo es muy conveniente su estudio, pues introduce al lector en un mundo nuevo para él, donde la abstracción alcanza un grado muy elevado. La teoría de categorías y functores invade actualmente gran parte del enorme reino de las matemáticas.

A partir de los años 40 del siglo XX, se trató de sistematizar el estudio de todas las estructuras matemáticas conocidas. Asociadas a esas estructuras tenemos siempre unos morfismos. Estos morfismos normalmente son funciones entre los conjuntos soporte de las estructuras. Por ello la composición funcional de morfismos es una operación válida y además lo normal es que nos de otro morfismo. Todo ello se encuentra recogido dentro del cálculo categórico.

La teoría de functores representables es la asociada a los problemas de las propiedades universales.

Nosotros partiremos de la definición "clásica" de categoría, que es la más intuitiva. Debemos señalar que todo este capítulo, a excepción del teorema de Grotendieck, es simplemente notación.

Definición 5.1 *Una* categoría $\mathcal{C}$ *consta de:*

- *Una clase* $\mathrm{Ob}(\mathcal{C})$ *cuyos elementos llamaremos* objetos *de* $\mathcal{C}$. *En general* $\mathrm{Ob}(\mathcal{C})$ *será una clase y no un conjunto.*
- *Para cada par de objetos de la categoría* M *y* N, *existe un conjunto* $\mathrm{Hom}(M,N)$ *que son los* morfismos *de* M *en* N.
- *Para cada trio de objetos* M, N, P *una aplicación*

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(M,N) \times \mathrm{Hom}_{\mathcal{C}}(N,P) & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(M,P) \\ (f,g) & \longrightarrow & gf \end{array}$$

que llamaremos composición de morfismos y que debe cumplir:

I) *Asociativa, cuando esto tenga sentido (o sea cuando la composición esté definida).*

II) *Para cada objeto M, existe un morfismo de M en si mismo,* Id_M *y que actua como identidad a la derecha y a la izquierda, siempre que la composición tenga sentido. Este morfismo se llama "identidad del objeto M".*

$$f\,\mathrm{Id}_M = f \quad f \in \mathrm{Hom}(M,P) \text{ para todo } P \in \mathrm{Ob}(\mathcal{C})$$

$$\mathrm{Id}_M\, g = g \quad g \in \mathrm{Hom}(P,M) \text{ para todo } P \in \mathrm{Ob}(\mathcal{C})$$

Dada una categoría, podemos hablar de una subcategoría.

Definición 5.2 $\mathcal{C}'$ *es una* subcategoría *de* $\mathcal{C}$ *si:*

I) $\mathrm{Ob}(\mathcal{C}') \subset \mathrm{Ob}(\mathcal{C})$

II) $\mathrm{Hom}_{\mathcal{C}'}(M,N) \subset \mathrm{Hom}_{\mathcal{C}}(M,N)$

y la composición en $\mathcal{C}'$ es la restricción de la composición en $\mathcal{C}$.

En el caso en que $\mathrm{Hom}_{\mathcal{C}'}(M,N) = \mathrm{Hom}_{\mathcal{C}}(M,N)$ para todo par de objetos de $\mathcal{C}'$, la subcategoría se dirá que es completa o plena. En estas subcategorías sólo quitamos objetos, pero no morfismos entre los objetos que nos quedan.

Ejemplos.

- Categoría de conjuntos. Los objetos son los conjuntos y los morfismos entre dos conjuntos son las funciones entre ellos. La composición es la habitual entre aplicaciones. Como es bien sabido, el conjunto de todos los conjuntos no es un conjunto. En realidad es una clase. Sin embargo no tendremos en cuenta nunca este tipo de problema, que lo dejaremos para los "fundamentalistas" de la matemática.
- Categoría de grupos, anillos, k-espacios vectoriales, A-módulos . . ., junto con los morfismos propios de la estructura y la composición habitual como funciones.

- Categoría de grupos abelianos o categoría de grupos finitos. Son subcategorías plenas de la categoría de gupos. Sin embargo la categoría de k-álgebras no es completa en la de k-espacios, pues en general una aplicación lineal no tiene por qué ser un morfismo de anillos.
- Las variedades diferenciales y las aplicaciones C^∞.
- Los espacios topológicos y las aplicaciones continuas.
- Los espacios métricos y los morfismos que conservan las distancias.
- Los espacios normados sobre el cuerpo $\mathbb{R}$, junto con las aplicaciones lineales que conservan la norma.

Veamos ahora ciertas definiciones referentes a los morfismos. Son simple traducción a nuestro lenguaje de propiedades que caracterizan a los morfismos que hemos estudiado en otras estructuras.

Decimos que $f : M \to N$ es un isomorfismo si existe $g : M \to N$ tal que $gf = \mathrm{Id}_M$ y $fg = \mathrm{Id}_N$. El lector puede probar que este g, caso de existir es único. Se dirá que es el inverso de f y se denotará f^{-1} como norma general.

A los morfismos de un objeto en si mismo los llamaremos endomorfismos. A los endomorfismos que sean isomorfismos los llamaremos automorfismos.

Un morfismo $f : M \to N$ es inyectivo si para todo par de morfismos

$$g, \overline{g} : P \to M$$

que cumplan $fg = f\overline{g} \quad \Rightarrow \quad g = \overline{g}$.

Un morfismo $f : M \to N$ es epiyectivo si para cualquier par de morfismos

$$g, \overline{g} : N \to P$$

que cumpla $\overline{g}f = gf$ se tiene que $g = \overline{g}$.

Debido a esto todo monomorfismo (= inyectivo) es simplificable por la izquierda y cualquier epimorfismo es simplificable por la derecha. Estas definiciones coinciden con las conocidas.

Como no podía ser menos, existen unos morfismos entre categorías. Para evitar complicaciones de lenguaje se les llama functores.

Definición 5.3 *Sean $\mathcal{C}$ y $\mathcal{D}$ categorías. Un* functor covariante *de $\mathcal{C}$ en $\mathcal{D}$ es una regla que asigna a cada objeto M de $\mathcal{C}$ un objeto $F(M)$ de $\mathcal{D}$, y a cada morfismo $f : M \to N$ un morfismo $F(f) : F(M) \to F(N)$ de modo que se cumpla:*

- $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$
- $F(gf) = F(g)F(f)$

Un functor se denota $F : \mathcal{C} \to \mathcal{D}$

Definición 5.4 *Un* functor contravariante *es una ley que asigna a cada objeto M de $\mathcal{C}$ un objeto $F(M)$ de $\mathcal{D}$ y a cada morfismo $f : M \to N$ un morfismo $F(f) : F(N) \to F(M)$ (observese que cambia el orden) de modo que se verifique:*

- $F(\mathrm{Id}_M) = \mathrm{Id}_M$
- $F(gf) = F(f)F(g)$

También se denota $F : \mathcal{C} \to \mathcal{D}$.

Si hubiesemos estudiado la teoría de categorías, entendiendolas como semigrupoides, el concepto de functor aparecería de modo natural.

Ejemplos.

- El paso al dual. Si E es un espacio vectorial $F(E) = E^*,\ F(\varphi) = \varphi^*$. A cada espacio le asociamos su dual y a cada aplicación su transpuesta. Así hemos construido un functor contravariante de la categoría de los k-espacios vectoriales en si misma.
- Si X es un espacio topológico o una variedad, asociamos a X el anillo de funciones reales continuas o diferenciables. A cada morfismo f le asociamos f_*. f_* consiste en componer con f por la izquierda. Este functor covariante valora en la categoría de $\mathbb{R}$-álgebras.

- M un A-módulo. $F(M) = \{\text{Submódulos de } M\}$, $F(f) = f^{-1}$. f^{-1} es la imagen inversa. Tenemos entonces un functor de la categoría de A-módulos en la categoría de conjuntos ordenados.

- Si A es un anillo $F(A) = \{\text{Ideales primos de } A\}$, $F(f) = f^{-1}$. Es un functor de la categoría de anillos conmutativos en la de conjuntos ordenados. Este functor se denomina functor espectro y $F(A)$ se denota $\text{Spec}(A)$. Este functor es contravariante.

- Si X es una variedad diferenciable. $\tau(X)$ el álgebra tensorial y para cada apliación diferenciable $f : X \to Y$ sea $f^* : \tau(Y) \to \tau(X)$ la imagen inversa, también llamada pull-back.

- Sea N un objeto. $F(M) = \text{Hom}_{\mathcal{C}}(N, M)$. Es un functor covariante de la categoría $\mathcal{C}$ en la de conjuntos. Naturalmente $F(f) = f_*$ que consiste en componer por la izquierda con f. Este functor se suele denotar H_N.

- Si N es un objeto, $F(M) = \text{Hom}_{\mathcal{C}}(N, M)$ es un functor contravariante.

Sean ahora F y G dos functores de $\mathcal{C}$ en $\mathcal{D}$

Definición 5.5 *Una* transformación natural *entre los functores F y G es dar una ley que asigne a cada objeto M de $\mathcal{C}$ un morfismo $\tau_M : F(M) \to G(M)$ de tal modo que sea conmutativo el diagrama*

$$\begin{array}{ccc} F(M) & \xrightarrow{F(f)} & F(N) \\ \Big\downarrow{\scriptstyle \tau_M} & & \Big\downarrow{\scriptstyle \tau_N} \\ G(M) & \xrightarrow{F(g)} & G(N) \end{array}$$

La transformación natural se denotará $\tau : F \to G$.

Diremos que esa ley es una equivalencia o un isomorfismo de functores si todos los morfismos τ_M son isomorfismos.

Todo lo dicho se aplica a functores covariantes. El lector intentará traducir estos conceptos a los functores contravariantes.

Ejemplos.

- Sea la categoría de los espacios vectoriales de dimensión finita sobre un cuerpo. El funtor tomar doble dual es equivalente al functor identidad, pues es sabido que dado E, existe un isomorfismo canónico de E en E^{**} que hace el diagrama conmutativo.
- Las equivalencias naturales entre functores, son la realización abstracta de los isomorfismos canónicos.

Una vez dado el concepto de equivalencia de functores, podremos hablar de functores representables, que es el tema del resto del capítulo.

Consideremos el ejemplo dado anteriormente de functor H_N. Sea F un functor arbitrario de la categoría $\mathcal{C}$ en la de conjuntos. Cada elemento $\varphi \in F(M)$ define una equivalencia natural entre el functor H_M y F:

$$\varphi : H_M \to F$$

$$\varphi(f) = F(f)(\varphi)$$

Definición 5.6 *Diremos que la pareja (M, φ) representa al functor F, si la transformación natural construida anteriormente es un isomorfismo de functores. Diremos que un functor es* representable *si existe alguna pareja que lo represente.*

De modo análogo se define la representatividad de los functores contravariantes.

Todos los teoremas de factorización canónica y de propiedades universales afirman que cierto functor es representable.

Si existe un pareja (M, φ) que representa a F, y si suponemos que existe un objeto M' isomorfo a M, mediante un isomorfismo $f : M \to M'$, entonces la pareja $(M', F(f)\varphi)$ también representa a F. Estas parejas serán consideradas equivalentes

Definición 5.7 *Dos parejas (M, φ) y (M', φ') que representan a F son equivalentes si existe un isomorfismo $f : M \to M'$ que cumpla $\varphi' = F(f)\varphi$.*

Veamos el importante teorema de unicidad de la pareja representante de un functor.

Teorema 5.1 (Grotendieck) *Si un functor representable está representado por dos parejas, estas son equivalentes.*

Demostración.

(M, φ) y (M', φ') dos parejas que representan a F. Existe un único morfismo $f : M \to M'$ que cumple $\varphi' = F(f)(\varphi)$. Del mismo modo, existe un único morfismo $g : M' \to M$ que cumple $F(g)(\varphi') = \varphi$. Entonces $\varphi = F(gf)(\varphi)$ y $\varphi' = F(fg)(\varphi')$. Se puede concluir que $F(gf) = \mathrm{Id}_M$ y que $fg = \mathrm{Id}_{M'}$. Por lo tanto f es un isomorfismo. □

Ejemplos de functores representable se dan en el texto, aunque no se mencionan explicitamente. Simplemente probamos las "propiedades universales".

Otros ejemplos de functores representables pueden ser:

- Construcción de $\mathbb{Z}$ a partir de $\mathbb{N}$.
- Construcción de las estructuras cociente.
- Construcción del anillo de fracciones de un anillo íntegro.
- Localización de un anillo por un subconjunto multiplicativamente cerrado.
- Algebra envolvente de un álgebra de Lie.
- Algebra de Clifford asociada a un tensor métrico.
- Completación de un espacio métrico.
- Construcción del anillo de polinomios sobre un cuerpo.
- k-álgebra de un grupo.

Problemas

32 Pruébese la verdad o falsedad de las afirmaciones que siguen:

i) Los $\mathbb{R}$-espacios normados se pueden considerar una subcategoría de los espacios topológicos.

ii) Los $\mathbb{R}$-espacios normados son una subcategoría plena en los $\mathbb{R}$-espacios vectoriales.

iii) Los conjuntos ordenados, junto con los antimorfismos forman una categoría. (f es es antimorfismo si $f(x) \leq f(y)$ cuando $y \leq x$).

33 f es isomorfismo. Entonces es inyectivo y epiyectivo. ¿Es cierta la afirmación recíproca?

¿Es siempre cierto, cuando los morfismos son funciones, que los isomorfismos son los morfismos biunívocos?

Los automorfismos de un objeto forman un grupo.

34 Probar que todo grupo puede considerarse una categoría con un único objeto y los elementos del grupo como morfismos. La composición es el producto del grupo. Hállense los isomorfismos, monomorfismos y epimorfismos.

35 Probar que Id_M es necesariamente único. Además es un isomorfismo. Debido a ello los objetos de la categoría se pueden inyectar en la colección de todos los morfismos de la categoría. Ello lleva a la conclusión de que en la categoría los elementos que tienen importancia son los morfismos, pues un objeto no es más que un morfismo con ciertas propiedades. Esta última afirmación se ve reforzada al estudiar el teorema de Grotendieck de functores representables.

36 Dos objetos de una categoría se dice que son equivalentes o isomorfos, si existe algún isomorfismo entre ellos. Esto introduce una relación de equivalencia en la clase de todos los objetos de la categoría. Formamos una nueva categoría, donde los nuevos objetos serán las clases de equivalencia de los antiguos. Intente el lector construir los morfismos y verificar si es cierto que forman una categoría.

37 Los functores transforman isomorfismos en isomorfismos. Además $F(f^{-1}) = F(f)^{-1}$.

Si dos objetos son isomorfos en $\mathcal{C}$ sus imágenes por un functor son isomorfas en $\mathcal{D}$.

Si tenemos un funtor de $\mathcal{C}$ en $\mathcal{D}$ y sabemos que $F(N)$ y $F(M)$ no pueden ser isomorfos en $\mathcal{D}$, entonces M y N no pueden ser equivalentes en $\mathcal{D}$. Esta idea está latente en muchos problemas de clasificación.

38 Si F es un functor de $\mathcal{C}$ en $\mathcal{D}$ y G es un functor de $\mathcal{D}$ en $\mathcal{E}$, construir la composición de functores.

¿Cuál sería el functor identidad?

¿Cuándo dos categorías son isomorfas o antiisomorfas?

La composición de dos functores contravariantes, ¿qué tipo de functor dá?

39 Definimos el espectro maximal de un anillo como el conjunto de los ideales maximales. Por analogía con uno de los ejemplos dados todo parece indicar que estamos construyendo un functor. Pruebese que esto es falso.

6. Suma y producto directo

Sea $\{N_i\}$ una familia de módulos sobre el mismo anillo A. Sea $\oplus N_i$ es conjunto de las sucesiones $\{e_i\}$, $e_i \in N_i$ casi nulas. Esto quiere decir que en una sucesión todos los elementos, salvo un número fínito, son el cero del correspondiente módulo. En $\oplus N_i$ existe una estructura natural de módulo, mediante las operaciones "componente a componente":

$$\{e_i\} + \{e_i'\} = \{e_i + e_i'\}$$

$$a\{e_i\} = \{ae_i\}$$

que son sucesiones casi nulas.

El módulo $\oplus N_i$ que se acaba de construir se llamará suma directa de la familia $\{N_i\}$. No es dificil probar la asociatividad de la suma directa. Asimismo cambiar el orden de los módulos lo único que hace es construir otro módulo isomorfo al anterior.

Si quitamos la condición de casi nulidad de las sucesiones tenemos, con las mismas operaciones, otro módulo, que en general no será el mismo que el módulo suma directa. Este nuevo módulo se denota $\prod N_i$ y sus elementos son las sucesiones $\{e_i\}$. Este nuevo módulo se llama producto directo de la familia $\{N_i\}$. En el caso en que el conjunto de módulos sea finito, la suma y el producto directo coinciden. En el caso general la suma es un submódulo del producto directo.

La suma y el producto directo están dotados de las siguientes aplicaciones

$$i_j : N_j \to \oplus N_i$$

$$i_j : N_j \to \prod N_i$$

i_j hace corresponder a cada $e \in N_j$ la sucesión donde todos los elementos son cero, salvo el que ocupa el lugar j que es justamente e.

Estas aplicaciones son claramente morfismos de módulo. Es más, en la suma directa se ha definido la suma y el multiplicación por escalares del modo indicado, precisamente para que las aplicaciones i_j sean morfismos de módulo. Estas aplicaciones se llaman inyecciones canónicas. Via esta inyección N_j se puede considerar un submódulo de la suma o del producto directo. Con estas identificaciones resulta que $\oplus N_i$ coincide con $\sum N_i$. La suma directa es el menor submódulo que contiene a toda la familia de módulos.

Otras aplicaciones naturales son:

$$\pi_i : \oplus N_i \to N_i$$

$$\pi_i : \prod N_i \to N_i$$

donde $\pi_i(\{e_j\}) = e_i$. De nuevo estas aplicaciones son morfismos de módulo. Se llaman proyecciones canónicas sobre el i-ésimo factor y son epiyectivas.

Ejemplos.

- A^n es el producto directo de n copias de A. También es la suma directa de n copias de A.

- El conjunto de polinómios $A[x]$ es isomorfo a la suma directa de $\mathbb{N}$ copias de A pues todo polinómio tiene un número finito de términos.
- El anillo de las series formales $A[[x]]$ es isomorfo al producto directo de $\mathbb{N}$ copias de A.

Vamos a ver ahora las propiedades universales del producto y de la suma directa. Estas propiedades caracterizan a estos módulos salvo un isomorfismo.

Sea M un módulo arbitrario y $\{\varphi_i\}$ un conjunto de morfismos lineales

$$\varphi_i : M \to N_i$$

Entonces existe un único morfismo de A-módulos

$$\varphi : M \to \prod N_i$$

tal que $\pi_i \circ \varphi = \varphi_i$.

Esto nos dice que para dar una aplicación lineal de un módulo en un producto directo basta darla componente a componente.

Sea ahora una familia $\{\varphi_i\}$ de morfismos

$$\varphi_i : N_i \to M$$

Entonces existe una única aplicación lineal

$$\varphi : \oplus N_i \to M$$

tal que $\varphi \circ i_j = \varphi_j$

Lo anterior nos permite establecer los siguientes isomorfismos

$$\prod \mathrm{Hom}(M, M_i) \sim \mathrm{Hom}(M, \prod M_i)$$
$$\prod \mathrm{Hom}(M_i, M) \sim \mathrm{Hom}(\oplus M_i, M)$$

Las nociones de producto directo y de suma directa son duales. Se obtiene una de la otra "dando la vuelta a las flechas". Es habitual en libros algo antiguos llamar al producto directo simplemente producto y a la suma directa

coproducto. Las propiedades universales nos dicen que tanto la suma como el producto directo son representantes de functores y como tales, únicos salvo isomorfismos.

Problemas

40 Si N y N' son dos submódulos suplementarios de M probar que $M \sim N \oplus N'$.

41 Si $\varphi : N \to M \quad \varphi' : M \to L$ son tales que $\varphi'\varphi$ sea un isomorfismo, entonces $M \sim \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\varphi')$

Sea $\varphi : M \to N$ idempotente ($\varphi^2 = \varphi$). Entonces $M \sim \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\varphi')$.

42 El anulador de una suma directa es la intersección de los anuladores de los módulos componentes.

Si $\{m_i\}$ es un sistema generador de M, el anulador de M es la intersección de los anuladores de Am_i.

La suma directa de módulos sin torsión no tiene torsión.

43 El anillo de polinomio sobre A es isomorfo a la suma directa de $\mathbb{N}$ copias de A. En cambio el anillo de las series formales sobre A es isomorfo al producto directo de $\mathbb{N}$ copias de A.

44 Demostrar que el submódulo $2\mathbb{Z}$ de $\mathbb{Z}$ no admite suplementario.

Recordando la teoría de grupos demostrar que en $\mathbb{Z}_{p^2}$ el submódulo $\mathbb{Z}p$ no puede ser un sumando directo.

45 Un módulo M es la suma directa de sus submódulos $N_1, \ldots N_n$ si y solo si:

I) $M = N_1 + \cdots + N_n$.

II) Para cada i se cumple $N_i \cap (\sum_{j \neq i} N_j) = 0$.

46 Si $\varphi_i : M_i \to N_i$ es lineal demostrar que existe un morfismo $\varphi : \prod M_i \to \prod N_i$. Analizar el núcleo y la imagen de este módulo. Hacer lo mismo con la suma directa.

47 Un endomorfismo π de M se dice que es un proyector si $\pi^2 = \pi$. Dos proyectores π_1 y π_2 son ortogonales si $\pi_1\pi_2 = 0$. Demostrar que si $\mathrm{Id} = \pi_1 + \cdots + \pi_n$ y los proyectores son ortogonales dos a dos, el módulo M es isomorfo a la suma directa de los submódulos $M_i = \pi_i(M)$.

7. Dualidad

Definición 7.1 *Llamaremos* forma lineal *sobre M a todo morfismo de M en A (A con su estructura natural). Al conjunto de todas las formas lineales sobre M lo llamaremos* módulo dual *de M y lo denotaremos M^*. Se cumple entonces que $M^* = \mathrm{Hom}_A(M, A)$.*

Por lo visto en el capítulo 2, M^* posee en efecto una estructura de módulo dada por las operaciones

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

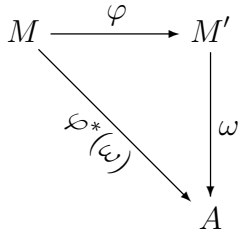
$$(af)(m) = af(m)$$

Si no se dice lo contrario, esta es la estructura que consideraremos en M^*. Como se ve está canónicamente asociada a la de M.

En principio no se puede asegurar que un módulo no nulo, posea más formas lineales que la forma lineal cero. Esto, como sabemos, si ocurre en k-espacios y más en general en los módulos libres (véase capitulo 10).

Las formas lineales las denotaremos por ω siguiendo la notación tradicional en el caso de los k-espacios.

Sea $\varphi : M \to M'$ un morfismo. Definimos $\varphi^* : (M')^* \to M^*$ por la fórmula $\varphi^*(\omega) = \omega\varphi$ (véase diagrama)



Fácilmente se comprueba que φ^* es lineal.

Definición 7.2 *La aplicación φ^* que acabamos de construir se llama dual de φ.*

La aplicación dual tiene una serie de propiedades importantes

- $(\varphi + \mu)^* = \varphi^* + \mu^*$
- $(a\varphi)^* = a\varphi^*$
- $(\varphi\mu)^* = \mu^*\varphi^*$
- $\mathrm{Id}^* = \mathrm{Id}$

De estas propiedades aplicandolas a una expresión de la forma $\varphi \circ \mu = \mathrm{Id}$ se puede concluir que el dual de un isomorfismo es un isomorfismo entre los espacios duales. Además la asociación $M \to M^*, \varphi \to \varphi^*$ es un functor contravariante de la categoría de A-modulos en si misma.

Aplicando la propiedad universal de la suma directa obtenemos

$$(\oplus M_i)^* = \mathrm{Hom}(\oplus M_i, A) = \prod \mathrm{Hom}(M_i, A) = \prod {M_i}^*$$

Por lo tanto el dual de una suma directa es el producto directo de los duales.

Veamos ahora un caso más particular de aplicación de esta propiedad universal. Sea A^n el producto (suma) directa de n copias del módulo A. Como acabamos de ver $(A^n)^* = (A^*)^n$. Pero como $A^* = \mathrm{Hom}(A, A) = A$ ocurre que A^n y su dual son isomorfos. Además este isomorfismo es canónico. Sin embargo si L es un módulo isomorfo a A^n, ocurre también que L y L^* son isomorfos, pero no canóniamente. Veremos en el capítulo 10 que depende de la base elegida en L.

Definición 7.3 *$\omega \in M^*$ es* incidente *con $m \in M$ si $\omega(m) = 0$.*

Si M' es un submódulo, diremos que ω es incidente con M' si es incidente con todos los vectores de M'.

El conjunto de vectores de M^* que son incidentes con un submódulo M', forman un submódulo del espacio dual, llamado incidente con M' y denotado $(M')^\circ$.

Proposición 7.1 *Si $M' \subset M''$ entonces $(M'')^\circ \subset (M')^\circ$.*

La proposición nos dice que tomar incidente es un antimorfismo del retículo de submódulos de M en el retículo de submódulos de su dual.

Problemas

48 Sea $B \subset A$ un subanillo y M un módulo sobre el anillo A. ¿El módulo dual de M, es igual calcularlo entendiendo M como A-módulo que entendiendolo como B-módulo?

49 Si φ es inyectiva, ¿es cierto que φ^* es epiyectiva?
Si φ es epiyectiva, ¿es cierto que φ^* es inyectiva?

50 Comprobar si se cumplen las igualdades:

$$(M' \cap M'')^\circ = (M')^\circ + (M'')^\circ$$

$$(M' + M'')^\circ = (M' \cap M'')^\circ$$

51 Demostrar que todo k-espacio vectorial no nulo, posee al menos una forma lineal no nula.

8. Sucesiones exactas

Diremos que una sucesión de morfismos de A-módulo

$$\cdots \overset{\varphi_n}{\to} M \overset{\varphi_{n+1}}{\to} M_{n+1} \to \cdots$$

es exacta si la imagen de cada morfismo coincide con el núcleo del siguiente

$$\mathrm{Im}(\varphi_n) = \mathrm{Ker}(\varphi_{n+1})$$

Ejemplos.

- $0 \to M' \stackrel{\varphi}{\to} M$ es exacta $\Leftrightarrow \varphi$ es inyectiva.
- $M \stackrel{\varphi}{\to} M'' \to 0$ es exacta $\Leftrightarrow \varphi$ es epiyectiva.
- $0 \to M' \stackrel{\varphi}{\to} M \stackrel{\mu}{\to} M'' \to 0$ es exacta si y solo si φ es inyectiva, μ epiyectiva y $\mathrm{Ker}(\varphi) = \mathrm{Im}(\mu)$. Estas últimas sucesiones se llaman sucesiones exactas cortas.
- Si N es un submódulo de M entonces tenemos la sucesión exacta

$$0 \to N \to M \to M/N \to 0$$

- Sea $\varphi : M \to N$ un morfismo. Llamamos conúcleo de φ a $M/\mathrm{Im}(\varphi)$. Entonces la sucesión siguiente es exacta

$$0 \to \mathrm{Ker}(\varphi) \to M \stackrel{\varphi}{\to} N \to \mathrm{Coker}(\varphi) \to 0$$

La importancia de las sucesiones exactas cortas radica en que toda sucesión "larga" puede descomponerse en sucesiones cortas.

Proposición 8.1 *Dada una sucesión exacta*

$$\cdots \to M_{i-1} \stackrel{\varphi_i}{\to} M_i \stackrel{\varphi_{i+1}}{\to} M_{i+1} \cdots$$

puede descomponerse en sucesiones cortas

$$0 \to N_i \to M_i \stackrel{\varphi_{i+1}}{\to} N_{i+1} \to 0$$

donde $N_i = \mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i+1})$.

Demostración.

En efecto, la sucesión larga es exacta en M_i si y solo si $\mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i+1})$. Pero eso es exactamente la condición de que la sucesión corta sea exacta. □

Proposición 8.2 *Si $M_i \subset M$ son una familia de submódulos la siguiente sucesión es exacta:*

$$0 \to \bigcap M_i \to M \to \prod(M/M_i) \to 0$$

Demostración.

La sucesión es efectivamente epiyectiva puesto que lo son todas las proyecciones canónicas. El núcleo está formado por los vectores que pertenecen a todos los submódulos M_i y por tanto a la intersección de dichos submódulos. □

Proposición 8.3 *Si N_1 y N_2 son submódulos de M la siguiente sucesión es exacta:*

$$0 \to N_1 \bigcap N_2 \to N_1 \oplus N_2 \to N_1 + N_2 \to 0$$

Demostración.

Si $n_1 + n_2 = 0$, entonces $n_1 = -n_2$ y por lo tanto pertenecen a la intersección de los dos submódulos. □

Proposición 8.4 *$M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ es exacta si y solo si para todo módulo N la sucesión*

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{p^*} \mathrm{Hom}(M, N) \xrightarrow{i^*} \mathrm{Hom}(M', N)$$

es exacta, donde $\varphi^*(\mu) = \mu\,\varphi$.

Proposición 8.5 *La condición necesaria y suficiente para que la sucesión*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$$

sea exacta es que para todo módulo N sea exacta

$$0 \to \mathrm{Hom}(N, M') \xrightarrow{i_*} \mathrm{Hom}(N, M) \xrightarrow{p_*} \mathrm{Hom}(N, M'')$$

donde $f_*(g) = fg$.

Demostración.

La demostración de ambas proposiciones no ofrece dificultades relevantes pero es extremadamente tediosa. □

Definición 8.1 *Se dice que una sucesión exacta corta*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

escinde *(o rompe o descompone) si* $i(M')$ *es un submódulo que admite un suplementario.*

Veamos algunas condiciones equivalentes a esta definición. Naturalmente una vez vistas puede tomarse como definición la que más convenga a nuestros propositos.

Teorema 8.6 $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *exacta. Son equivalentes:*

- *La sucesión rompe.*
- *i posee un* retracto *(un inverso por la izquierda). Así r es un retracto si* $r : M \to M'$ *y cumple* $ri = \mathrm{Id}_{M'}$.
- *p tiene una* sección *(un inverso por la derecha). Por lo tanto s es una sección de p si* $ps = \mathrm{Id}_{M''}$.

Demostración.

i) $\Rightarrow$ *ii)* $M' \oplus N = M$. Si π es la proyección en el primer factor, resulta que π es un retracto.

ii) $\Rightarrow$ *i)* Si $ri = \mathrm{Id}$ es fácil (problema 41) probar que $M = i(M) \oplus \mathrm{Ker}(r)$.

Las otras implicaciones siguen los mismos pasos. □

Corolario 8.7 *Si M es semisimple entonces*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

siempre escinde.

Corolario 8.8 *Toda sucesión de espacios vectoriales escinde.*

Designemos por C una clase de A-módulos. Una función λ de C en $\mathbb{Z}$ es aditiva si para toda sucesión exacta corta

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

cuyos términos sean todos elementos de C se cumpla

$$\lambda(M) = \lambda(M') + \lambda(M'')$$

En particular si las sucesiones escindiesen tendriamos que

$$\lambda(M' \oplus M'') = \lambda(M') + \lambda(M'')$$

lo que justifica el apelativo de aditiva que hemos asignado a la función λ.

Conocemos ya una función aditiva, la dimensión definida para los espacios vectoriales sobre un cuerpo. En el capítulo 9 se introducirá la noción de longitud de un módulo que es también aditiva.

Proposición 8.9 *Sea $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ exacta y tal que $M_i \in C$ $\forall i$ entonces*

$$\sum_{i}^{n} (-1)^i \lambda(m_i) = 0$$

Demostración.

Se descompone la sucesión exacta "larga" en sucesiones cortas y se aplica la definición de función aditiva, teniendo en cuenta que $N_0 = N_{i+1} = 0$. □

Problemas

52 Demostrar las afirmaciones:

- $0 \to M \to 0$ es exacta, entonces $M = 0$.
- $0 \to M \xrightarrow{g} N \to 0$ exacta, entonces g es isomorfismo.

53 Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta que escinde. Entonces son exactas las sucesiones:

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{p^*} \mathrm{Hom}(M, N) \xrightarrow{i^*} \mathrm{Hom}(M', N) \to 0$$

$$0 \to \mathrm{Hom}(N, M') \xrightarrow{i_*} \mathrm{Hom}(N, M) \xrightarrow{p_*} \mathrm{Hom}(N, M'') \to 0$$

¿Son ciertos los reciprocos?

54 Demostrar que la siguiente sucesión es exacta.

$$0 \to M_1 \cap M_2 \to M_1 \oplus M_2 \to M_1 + M_2 \to 0$$

donde el vector m lo mandamos a $(m, -m)$ y a (m_1, m_2) lo mandamos a $m_1 + m_2$.

55 Sea $\varphi : M \to N$ un morfismo. Probar que $\varphi(M_\tau) \subset N\tau$.
Si $0 \to M' \to M \to M''$ es exacta, entonces $0 \to M'_\tau \to M_\tau \to M''_\tau$ es exacta.

9. Longitud de un módulo

Una sucesión de inclusiones estrictas

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$$

se llama cadena de submódulos. El módulo cociente M_k/M_{k-1} se dice que es el k-ésimo factor de la serie.

Llamaremos extensión simple a una inclusión $M \subset M'$ tal que M/M' sea un módulo simple. Por la proposición 3.8 ello nos dice que entre M y M' no existe ningún submódulo distinto de ellos mismos.

Llamaremos serie de composición, cadena irrefinable o cadena máximal, a una cadena de submódulos tal que todos los factores sean simples. En dicha cadena no podemos introducir más eslabones, por ello se llama cadena irrefinable o máximal.

Debemos tener en cuenta que pueden existir A-módulos simples no isomorfos entre si, a diferencia de los espacios vectoriales donde el único k-módulo simple es k.

Sea $0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$ una serie de composición. Al número n lo llamaremos longitud de la serie. En general un módulo no posee ninguna serie de composición con un número finito de eslabones.

Definición 9.1 *Se dice que un módulo es de* longitud finita *si posee al menos una serie de composición con un número finito de eslabones. Llamaremos* longitud de un módulo *a la menor de las longitudes de sus series de composición.*

Teorema 9.1 *Sea M un módulo de longitud finita.*

I) *Si $M' \subset M$ entonces M' tiene longitud finita y $l(M') \leq l(M)$. Se tiene que $l(M') = l(M)$ si solo si $M' = M$*

II) *Todas las series de composición tienen la misma longitud.*

III) *La longitud es una función aditiva. Si M, M', M'' son de longitud finita y*

$$0 \to M' \to M \to M' \to 0$$

es exacta, entonces

$$l(M) = l(M') + l(M'')$$

Demostración.

i) Sea $M_0 \subset \cdots \subset M_n$ una serie de composición se M. Sea $M'_i = M_i \cap M'$. Como M'_i/M'_{i-1} se puede inyectar en M_i/M_{i-1} resulta que dicho módulo es un módulo simple o bien es el módulo nulo. Si alguno es nulo entonces $M_i = M_{i-1}$ y podemos quitar un término a la cadena. La serie $\{M'_i\}$ es una serie de composición de M' tras quitar los repetidos. Entonces la longitud

de esta serie es menor que n. Tomando una serie de composición de longitud mínima, se concluye el enunciado para longitudes.

Si $l(M) = l(M')$, entonces ningún factor de $\{M_i\}$ puede ser cero. No se puede verificar $M'_i = M'_{i-1}$, es decir $M'_i = M_i$ para todo i por inducción.

ii) Por inducción sobre la longitud. En el caso de módulos simples el enunciado es claro. Si $M_0 \subset \cdots \subset M_n$ es una serie de composición de M, entonces $\{M_i/M_1\}$ es una serie de composiciónde M/M_1. Todas las series de composición de M/M_1 tienen la misma longitud. Entonces M también.

iii) Sea la sucesión exacta

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

Sean

$$0 \subset M'_1 \subset \cdots \subset M'_n = M'$$

$$0 \subset M''_1 \subset \cdots \subset M''_m = M''$$

series de composición. Entonces

$$0 \subset i(M_1) \subset \cdots \subset i(M'_n) \subset p^{-1}(M''_1) \subset \cdots \subset p^{-1}(M''_m) = M$$

es una serie de composición de M. Por lo tanto

$$l(M) = l(M') + l(M'')$$

y se concluye. □

Problemas

56

$$0 \to M_0 \to M_1 \to \ldots \to M_{n-1} \to M_n \to 0$$

una sucesión exacta. Entonces

$$\sum_{i=0}^{n}(-1)^k l(M_k) = 0$$

57 Si M yN son dos submódulos de longitud finita, entonces $M+N$ y $M \cap N$ son de longitud finita y además

$$l(M+N) + l(M \cap N) = l(M) + l(N)$$

58 Sea una familia finita de módulos de longitud finita. Hallar la longitud de la suma directa de dichos módulos. Demostrar que para espacios vectoriales la longitud y la dimensión son la misma cosa.

59 Sea M de longitud finita. Probar que toda cadena se puede completar para obtener una serie de composición.

60 Sea M de longitud finita n. ¿Ocurre entonces que M^* es de longitud finita n?

61 Este es el $teorema\ de\ Jordan\text{-}Holder$ para módulos.

Si $0 \subset M_1 \subset \cdots \subset M_n$ es una serie de composición, llamamos factores de la cadena a los cocientes M_i/M_{i-1}. Dadas dos series de composición probar que tienen la misma longitud y que tras una permutación los factores son isomorfos. Así los factores son invariantes del módulo y no dependen de la serie elegida.

62 Todo módulo de longitud finita es de generación finita.

*** Problema 63** En todo este ejercicio los grupos serán finitos, aunque posiblemente no conmutativos.

Definición 9.2 *Un grupo G es $simple$ si no posee subgrupos normales.*

Una sucesión de subgrupos

$$e = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

es una serie de composición si todos los grupos factores G_{i+1}/G_i son simples.

Admitamos sin demostración el siguiente teorema de Jordan-Holder:

Dos series de composición de un grupo tienen la misma longitud y factores isomorfos.

Definición 9.3 *La longitud de un grupo es el número de eslabones de una cualquiera de sus series de composición. La denotaremos por* $l(G)$.

Demostrar las siguientes afirmaciones:

- Utilizando inducción probar que todo grupo de orden p^n con p un número primo tiene longitud n y que todos los factores son isomorfos a un grupo cíclico de p elementos.
- Calcular la longitud de un grupo abeliano de orden $p_1^{n_1} \dots p_r^{n_r}$.
- Si H es un subgrupo normal de G entonces $l(G) = lH) + l(G/H)$.

Definición 9.4 *Un grupo es resoluble si todos los factores de una serie de composición son grupos cíclicos.*

- Demostrar que si $H \subset G$ es normal entonces

  G es resoluble $\iff$ H y G/H son resolubles.
- Todo grupo abeliano es resoluble.

10. Módulos libres

Un módulo libre es todo módulo isomorfo a uno de la forma $\oplus_{i \in I} N_i$ donde cada N_i es isomorfo a A como módulo. Se considera en A la estructura natural de módulo.

El cardinal de I está perfectamente determinado. En el caso de un cardinal finito coincide con el rango del módulo.

Sabemos que todo espacio vectorial es libre pues por simple aplicación del lema de Zorn se obtiene la existencia de bases algebraicas (también llamadas bases de Hamel). Cada elección de una base de Hamel nos da un isomorfismo

del espacio vectorial en el producto directo de copias de k. Debemos tener en cuenta que sobre un anillo arbitrario pueden existir módulos que no sean libres. Por ejemplo $\mathbb{Z}_n$ no puede ser libre como $\mathbb{Z}$-módulo.

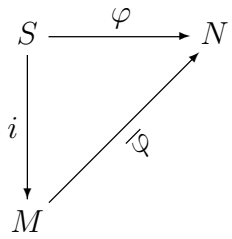
Los módulos libres poseen una propiedad universal que los caracteriza. Son los representantes de un cierto functor. Para ver esta propiedad partimos de la idea de que si tenemos una base del módulo libre y a cada elemento de la base le asignamos un vector de un módulo N, entonces podemos construir una aplicación de todo el módulo libre que sobre la base coincida con la aplicación dada, sin más que extender por linealidad la definición.

Si M es libre, entonces existe al menos un conjunto S verificando la siguiente propiedad.

Si $\varphi : S \to N$ es una función arbitraria de S en un A-módulo, entonces existe un único morfismo de módulos de M en N que sobre S coincide con φ.

Esta es la propiedad universal de los módulos libres.

Ello quiere decir que el diagrama siguiente admite un único $\overline{\varphi}$ que lo hace conmutativo.



Si M es un módulo, una familia finita de vectores $m_1, m_2, \ldots, m_n$ se dice que es linealmente independiente si

$$a_1 m_1 + \ldots + a_2 m_2 = 0 \quad \Rightarrow a_i = 0 \quad \forall i$$

Definición 10.1 *Diremos que un conjunto S de M es una* base *cuando cada subconjunto finito de S sea linealmente independiente y además S genere el módulo M.*

Como S genera M, todo vector es combinación lineal finita de elementos de S. Por ser cada subconjunto finito linealmente independiente, esta combi-

nación lineal es única. Si damos la imagen de los elementos de una base de M en un módulo N, tenemos definido un morfismo de A-módulos, sin más que extender la aplicación por linealidad. Claramente este morfismo es único.

De igual modo si un subconjunto S de M verifica la propiedad universal, necesariamente es linealmente independiente y genera M. Si no fuera linealmente independiente, a veces no existiría el morfismo que lo extiende y si no generará M el morfismo no tendría por que ser único.

Resumiendo obtenemos

Teorema 10.1 *Un A-módulo es libre si y solo si tiene una base.*

Para cada cardinal, existe un único módulo, salvo isomorfismos, que tiene una base con el cardinal dado. Si S es un subconjunto cuyo cardinal conocemos entonces $\oplus_{i\in S} A_i$ con $A_i \sim A$ es un A-módulo cuya base es, por ejemplo, las sucesiones de elementos de A, todas nulas, salvo el lugar i-ésimo donde aparece un 1. $\square$

Ejemplos

- A^n es libre de rango n.
- $M_{n,m}(A)$ es libre de rango mn.
- $A(x)$ es libre de rango infinito. Una base de este módulo está formada por los polinómios $\{1, x, x^2, \dots\}$.
- La suma directa de módulos libres es libre y una base se obtiene uniendo las bases de cada sumando.
- Sea S un conjunto cualquiera sin ninguna estructura. Consideremos el conjunto M de todas las funciones $f : S \to A$ casi nulas. M es un módulo libre. A cada elemento $s \in S$ le podemos asociar una función $\overline{s}$ que cumple $s(s') = 0$ si $s' \neq s$ y $s(s) = 1$. El conjunto de las funciones $\overline{s}$ cuando s recorre el conjunto es una base del módulo. Por abuso de notación, denotarmos directamente a la función por s en vez de por $\overline{s}$.

  El módulo que acabamos de construir se llama módulo libre con base S.

- En un módulo libre sobre un anillo sin divisores de cero no pueden existir vectores de torsión.

Veamos ahora como el estudio de las aplicaciones lineales entre módulos libres es muy sencilla y tiene grandes semejanzas con el estudio que se realiza para los espacios vectoriales. Para no recargar la notación nos ceñiremos a los módulos de rango finito.

Según los propiedades universales del producto y de la suma directa tenemos que el conjunto $\mathrm{Hom}(A^n, A^m)$ es isomorfo al módulo $A^{m\times n}$. A cada aplicación lineal entre estos dos módulos se le puede hacer corresponder una matriz $n \times m$ de la misma forma que en el Algebra Lineal. Reciprocamente, dada una matriz de ese tamaño podemos reconstruir la aplicación lineal sin más que utilizar el producto matricial por vectores columna.

Resumiendo, tenemos la siguiente proposición

Proposición 10.2 $\mathrm{Hom}(A^n, A^m) \sim M_{n,m}(A)$.

Lema 10.3 *Todo módulo es cociente de un módulo libre.*

Demostración.

Sea M el módulo en cuestión. L un módulo libre cuya base tenga por cardinal M. A cada elemento de la base le asignamos un elemento de M, de modo biunívoco, y extendemos por linealidad. Naturalmente este morfismo es epiyectivo.

$$L \to M \to 0$$

es exacta. □

Proposición 10.4 *Sea $N \subset M$ un módulo de tal forma que el cociente M/N sea libre. Entonces tenemos que N es un sumando directo y además*

$$M \sim N \oplus (M/N)$$

Demostración.

Tenemos la sucesión exacta

$$0 \to N \to M \to M/N \to 0$$

Se probará en el capítulo 11 que esta sucesión escinde. Por lo tanto se tiene el isomorfismo del enunciado. □

Corolario 10.5 *Si $\varphi : M \to L$ es una aplicación lineal epiyectiva sobre un módulo libre se tiene el isomorfismo*

$$M \sim \mathrm{Ker}(\varphi) \oplus L$$

Aunque nosotros siempre trabajamos con anillos conmutativos, no es difícil probar que todo módulo a la izquierda sobre un anillo con división (o sea, un cuerpo no conmutativo) es un módulo libre, siguiendo exactamente los mismos pasos que en Algebra Lineal conducen a los resultados análogos en el caso conmutativo (problema 67).

Problemas

64 Probar que si $A^n \sim A^m$ entonces $n = m$. Para espacios vectoriales esta definición coincide con la de longitud. ¿Es cierto esto para un anillo arbitrario? Probar que el rango es una función aditiva.

65 Sea A un anillo que tenga las propiedades:

- Todo A-módulo es semisimple.
- Todos los submódulos simples son isomorfos a A.

¿Se puede concluir que todo A-módulo es libre?

66 Sea A un anillo de ideales principales e íntegro. Probar que todo submódulo de A es libre.

Probar que todo submódulo de A^n es libre. Además el rango de un submódulo es siempre menor o igual que el del módulo.

Este ejercicio se utilizará en el tema de clasificación de módulos de tipo finito sobre un anillo principal.

67 En este ejercicio el lector intentará demostrar resultados que son "evidentes" para espacios vectoriales, pero que no lo son para módulos.

- Sea $m_1, \ldots, m_n$ una base de un espacio vectorial. Entonces

$$\lambda_1 m_a, \ldots, \lambda_n m_n \text{ con } \lambda_i \neq 0 \quad \forall i$$

  es una base. Esto no es cierto para módulos.

- Un submódulo de un módulo de tipo finito generado no tiene por qué ser finito generado.

- Hay submódulos de módulos libres que no son libres.

- Todo espacio vectorial no nulo tenía al menos un subespacio que si era libre. Sin embargo un grupo abeliano finito no puede contener nunca a $\mathbb{Z}^n$.

- En un espacio vectorial todo conjunto linealmente independiente se puede ampliar hasta una base. Esto es falso para módulos.

- Sea $B \subset A$ un subanillo. M es libre como A-módulo. ¿Es libre también como B-módulo?

68 Probar que un módulo de generación finita es un cociente de un módulo libre de rango finito.

69 Sea V un espacio vectorial sobre un anillo posiblemente no conmutativo. Probar las afirmaciones siguientes:

- Todo espacio vectorial es libre.

- Dos bases de un espacio vectorial tienen el mismo número de elementos (Probarlo solo en caso finito).

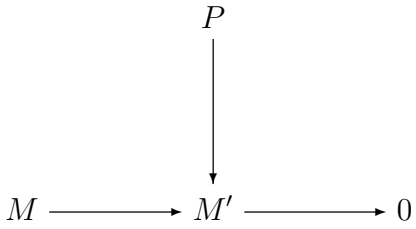
- Si S es un conjunto linealmente independiente, existe una base que contiene a S.

- Un conjunto maximal de vectores linealmente independiente es una base.
- Un conjunto mínimo de vectores que generen el espacio es una base.

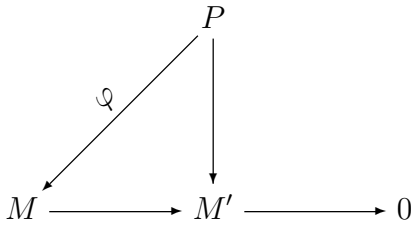
70 Sea A un dominio de ideales principales. Demostrar por inducción que todos los submódulos de A^n son libres y de rango menor o igual a n.

11. Módulos proyectivos e inyectivos

Definición 11.1 *Diremos que un A-módulo P es* proyectivo *si todo diagrama*



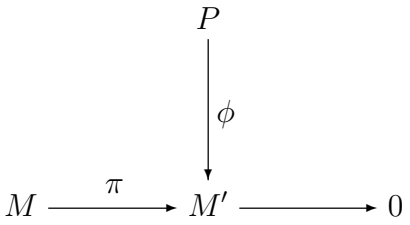
se puede completar con una aplicación lineal φ para obtener un diagrama conmutativo



El morfismo que cierra el diagrama no tiene por que ser único, solo pedimos que exista al menos uno.

Proposición 11.1 *Todo módulo libre es proyectivo*

Demostración.



Si $\{e_i\}$ es una base, asignemosle a cada e_i un elemento de $\pi^{-1}(\phi(e_i))$ (aplicando el axioma de elección). La aplicación lineal φ que extiende a la así definida cierra el diagrama y lo convierte en conmutativo. $\square$

Teorema 11.2 *Los siguientes enunciados son equivalentes:*

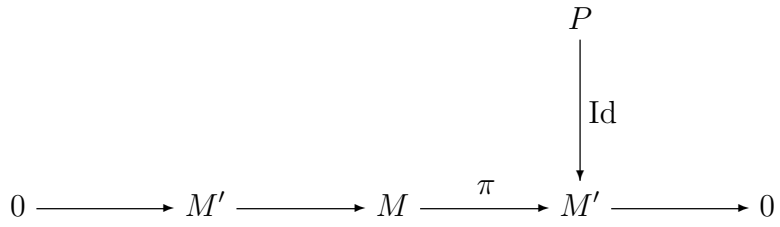
I) *P es proyectivo*

II) *Toda sucesión exacta $0 \to M' \to M \to P \to 0$ escinde.*

III) *Existe un módulo M tal que $P \oplus M$ es libre.*

Demostración.

- $1 \Rightarrow 2$) Considerese el diagrama



  Por ser P proyectivo existe una aplicación s de P en M que cumple $\pi s = \mathrm{Id}$. Por tanto s es una sección y la sucesión escinde.

- $2 \Rightarrow 3$) Sea L libre, de tal modo que P sea un cociente suyo. La sucesión

$$0 \to N \to L \to P \to 0$$

  escinde. Entonces $P \oplus N \sim L$

- $3 \Rightarrow 1)$ Por ser sumando directo de un libre. $\square$

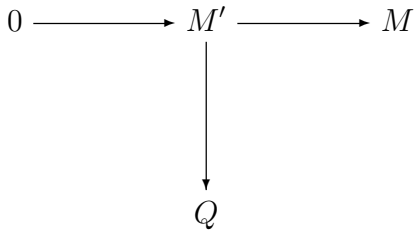
Proposición 11.3 *La condición necesaria y suficiente para que una suma directa de módulos sea un módulo proyectivo es que sea proyectivo cada sumando.*

Demostración.

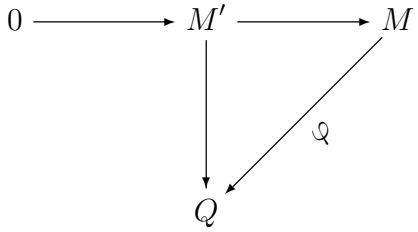
Si $\varphi_i : P_i \to M$ son los morfismos que cierran el diagrama para cada módulo P_i, entonces por la propiedad universal de la suma directa, existe $\varphi : \oplus P_i \to M$ que cierra el diagrama.

La otra implicación es trivial por ser sumando directo de un libre. $\square$

Definición 11.2 *Un módulo Q es* inyectivo *si todo diagrama*



se puede extender hasta completar un diagrama conmutativo



El morfismo φ que cierra el diagrama no tiene por que ser único.

Proposición 11.4 *La condición necesaria y suficiente para que un producto directo de módulos sea inyectivo es que lo sea cada factor.*

Demostración.

Sean $\varphi_i : M \to Q_i$ morfismos que cierran el diagrama. Aplicando la propiedad universal del producto, existe $\varphi : M \to \prod Q_i$ que cierra el diagrama. $\square$

Proposición 11.5 *Un A-módulo inyectivo Q hace que toda sucesión exacta*

$$0 \to Q \to M \to N \to 0$$

escinda.

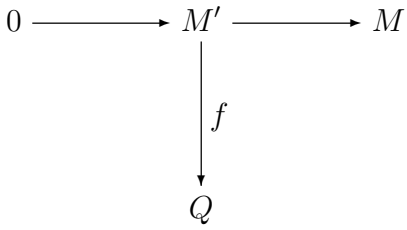
El inverso es también cierto, pero para probarlo debemos demostrar antes que todo módulo M se puede sumergir en uno inyectivo.

Lema 11.6 (Criterio del ideal) *Un A-módulo Q es inyectivo, si y solo si para todo ideal I de A y para todo morfismo $\phi : I \to Q$, existe un morfismo $\overline{\phi} : A \to Q$ que lo prolonga.*

Demostración.

La necesidad es evidente.

Reciprocamente



Sea m un vector de M que no pertenezca a M'. El ideal de A formado por los elemento $\{a \in A$ tales que $am \in M'\}$ lo denotamos por I. Sea ϕ el morfismo de I en Q definido por $\phi(a) = f(am)$.

Existe una extensión a todo el anillo. Denotemos dicha extensión por $\overline{\phi}$. Para todos los vectores de la forma $M' + bm$ con $m \in M'$ definimos

$$\overline{f}(m' + bm) = f(m') + \overline{\phi}(b)$$

Es un morfismo de $M' + < m >$ en Q.

Procediendo mediante el lema de Zorn se concluye.

Si una extensión maximal de f estuviera definida solo en un submódulo, por el procedimiento anterior lo podriamos extender más, en contra de la maximalidad que afirma el lema de Zorn. $\square$

Nota

Decimos que $(\overline{M}, \overline{f})$ es una extensión de de f si $M' \subset \overline{M}$ y $\overline{f}$ restingida a M' coincide con f. Decimos que una extensión es mayor que otra si la primera es extensión de la segunda.

Lema 11.7 (Criterio del ideal II) *Un A-módulo Q es inyectivo si y solo si para todo morfismo f de un ideal I en Q, existe un punto en $X \in Q$ tal que $f(a) = ax$ para todo $a \in I$.*

Demostración.

Todo morfismo de I en Q es la restricción de un morfismo de A en Q. Como $\mathrm{Hom}_A(A, Q) = Q$ se concluye. $\square$

Problemas

71 Probar mediante el criterio del ideal que todo k-espacio es inyectivo
¿Es cierto que todo módulo sobre un anillo principal es inyectivo?

72 Probar las siguientes afirmaciones:

- Todo módulo es cociente de un proyectivo.
- La noción de inyectividad es la noción dual de la de epiyectividad (o sea se obtiene dando la vuelta a las flechas en todas las definiciones)
- Sabemos que para todo módulo M existe una sucesión exacta

$$P \to M \to 0$$

El enunciado dual es que todo módulo se puede sumergir en un módulo inyectivo. Está proposición también es cierta, pero su demostración es de una mayor dificultad. Para la demostración remítase el lector a la bibliografia.

73 Un grupo abeliano M se dice que es *divisible* si para todo $y \in M$ y todo número natural $n \neq 0$ existe $x \in M$ tal que $nx = y$.

- Ver porqué se llama divisible
- $\mathbb{Q}$ es divisible. $\mathbb{Z}$ no lo es.
- La suma directa de divisibles es divisible.
- Una suma directa es divisible si y solo si lo es cada sumando.
- M es divisible si y solo si M es un $\mathbb{Z}$-módulo inyectivo.

74 Sea A un dominio de integridad. Si P es proyectivo, entonces no tiene torsión.

75 Un módulo proyectivo P es de rango finito si y solo si es un sumando directo de un módulo libre de rango finito.

12. Módulos graduados

La intención de este capítulo es introducir unos conceptos que nos serán de gran utilidad al estudiar los tensores sobre un módulo. Daremos una visión un poco más general que la estrictamente necesaria para ese propósito. También es útil este tema para el estudio de los polinomios de varias variables sobre un anillo y de la cohomología y homología.

Definición 12.1 *Dado un grupo conmutativo G, se llama* graduación de tipo Δ *a una colección de subgrupos $\{G_i\}\, i \in \Delta$ tales que G es la suma directa de esos subgrupos (suma directa como $\mathbb{Z}$-módulos).*

Δ es el conjunto de los grados del grupo. Se dice que un elemento x de G es homogéneo de grado i si $x \in G_i$. El cero del subgrupo es un elemento homogéneo de todos los grados. Los otros elementos solo pueden tener un grado.

Todo elemento $x \in G$ se puede escribir de modo único en la forma $x = \sum' x_i$ donde cada x_i es homogéneo de grado i. El apóstrofe indica que la suma es finita. x_i se llama componente homogénea de grado i de x. $x_i = \pi_i(x)$ donde π_i es la proyección canónica en el factor G_i.

Ejemplos.

- Los polinomios en una variable sobre un cuerpo k, con la graduación habitual sobre $\mathbb{N}$ dada por $k(x)_n = kx^n$.
- Los tensores de un k-espacio vectorial. También las formas exteriores o las simétricas.
- Los polinomios sobre k en m variables

$$k(x_1, \ldots, x_m)_n = \{\text{Polinomios homogéneos de grado n}\}$$

Si sobre el anillo A se ha dado una graduación de tipo Δ, estando dotado Δ de una estructura de monoide conmutativo, se dice que esta estructura es compatible con la estructura anular si

$$A_i \cdot A_j \subset A_{i+j}$$

Definición 12.2 *Un anillo con una estructura graduada compatible se llama* anillo graduado.

Si M es un A-módulo y tanto A como M poseen una graduación de tipo Δ, se dice que estas graduaciones son compatibles con la estructrura de módulo si

$$A_i \cdot M_j \subset M_{i+j}$$

Un A-módulo que cumpla lo anterior se dice que es un módulo graduado de tipo Δ.

Si A no es un anillo graduado un módulo graduado sobre A debe cumplir

$$A \cdot M_j \subset M_j$$

Si denotamos por $grad(x)$ al grado del elemento homogéneo x, entonces las definiciones se reducen a la conocida fórmula

$$grad(x \cdot y) = grad(x) + grad(y)$$

Ejemplos.

- El álgebra de polinomios $A(x)$ con el concepto de grado habitual es un módulo graduado con $\mathbb{N}$ como monoide de grados.
- El algebra exterior de un espacio vectorial es un módulo graduado con $\mathbb{N}$ como monoide de grados. Si el espacio vectorial es de dimensión finita n, entonces no hay elementos homogéneos de grado mayor que n.
- El conjunto de tensores covariantes y contravariantes de un espacio vectorial estan graduados sobre $\mathbb{N} \times \mathbb{N}$.

Lema 12.1 *Si M es un módulo graduado de tipo Δ y N es un submódulo de M, son equivalentes las afirmaciones siguientes:*

a) N es suma directa de $(N \cup M_i)$ $i \in \Delta$.

b) Las componentes homogéneas de todo elemento de N, pertenecen también a N.

c) N está engendrado linealmente por elementos homogéneos.

Demostración.

Al lector. □

Definición 12.3 *Un* submódulo graduado *es aquel que cumple alguna de las condiciones del anterior lema.*

Definición 12.4 *Sean M y M' dos módulos graduados de tipo Δ. Se dice que un morfismo de módulos*

$$\varphi : M \to M'$$

es de grado *j si $\varphi(M_i) \subset M'_{i+j}$.*

Fácilmente se comprueba que la composición de dos morfismos de grado definido nos da otro morfismo cuyo grado se obtiene sumando los grados de los dos morfismos.

Ejemplos

- La contracción interior con un vector es un morfismo del álgebra tensorial de un k-espacio. Su grado es -1.
- La diferencial exterior que se estudia en geometria diferencial es un morfismo entre las álgebras exteriores de las variedades y tiene grado $+1$. Se cumple que su cuadrado es nulo. Estas son las condiciones preliminares que nos van a servir para estudiar una teoría de cohomología. En este caso la cohomología resultante se denomina cohomología de De Rham.
- Multiplicar en un algebra por un elemento homogéneo de grado i, es un morfismo de grado i.

Proposición 12.2 *Sea M, M' módulos graduados. $\varphi : M \to M'$ un morfismo de grado r. Entonces* $\mathrm{Ker}(\varphi)$ *e* $\mathrm{Im}(\varphi)$ *son submódulos graduados.*

Demostración.

Sea $e' \in \mathrm{Im}(\varphi)$. Existe $e \in M$ tal que $\varphi(e) = e'$. Descomponemos e en sus componentes homogéneas $e = \sum e_i$. Por lo tanto $e' = \sum \varphi(e_i)$ que es la descomposición en componentes homogéneas de e'. Así las componentes homogéneas están en la imagen y el submódulo es graduado.

La otra parte de la demostración utiliza argumentos análogos. □

Problemas

76 Defínanse los cocientes de módulos graduados de tal forma que la proyección canónica sea de grado cero.

77 Sea A un anillo y I un ideal. Formamos el anillo graduado $A^* = \oplus_{n=0}^{\infty} I^n$, definiendo de modo natural la multiplicación.

Sea M un A-módulo, $M_n = I^n M$ son submódulos. $M^* = \oplus_{n=0}^{\infty} M_n$ puede dotarse de una estructura de A^*-módulo graduado.

78 Las componentes de grado cero de un anillo forman un subanillo.

79 Supongamos un anillo graduado sobre $\mathbb{N}$ o $\mathbb{Z}$. Entonces existe una graduación asociada sobre $\mathbb{Z}_2$, sin más que considerar los elementos de grado par y los elementos de grado impar.

80 Si M, N son dos módulos graduados sobre un conjunto Δ, introducir una graduación en la suma directa.

13. Producto tensorial

Construiremos un módulo que satisfaga cierta propiedad universal referente a las aplicaciones bilineales. La existencia de este módulo está garantizada por teoremas "fuertes" de la teoría de categorías. Nosotros no emplearemos esos argumentos, sino que seguiremos una línea más rupestre y menos elegante, pero a la vez más constructiva.

Definición 13.1 *Sean M, N, P tres módulos. Una función $\varphi : M \times N \to P$ es* A-bilineal *si:*

I) $\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$

II) $\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$

III) $\varphi(am, n) = a\varphi(m, n) = \varphi(m, an)$

El conjunto de todas la aplicaciones bilineales de $M \times N$ en P se denotará por $\mathrm{Bil}(M \times N, P)$ o por $L_2(M \times N, P)$. La suma y el producto por escalares dotan de estructura de A-módulo a este conjunto.

Ejemplos.

- El producto de un anillo

$$\begin{array}{rccc} \varphi: & A \times A & \to & A \\ & (a,b) & \to & ab \end{array}$$

  es una aplicación bilineal de $A \times A$ en A.

- El producto por escalares de un módulo M

$$\begin{array}{rccc} \varphi: & A \times M & \to & M \\ & (a,m) & \to & am \end{array}$$

  es una aplicación bilineal de $A \times M$ en M.

- Dados M y su dual M^* la aplicación

$$\begin{array}{rccc} \varphi: & M \times M^* & \to & A \\ & (m,\omega) & \to & \omega(m) \end{array}$$

- Dado un espacio vectorial E, el producto escalar es una aplicación bilineal de $E \times E$ en el cuerpo base.

- Si B es una A-álgebra, entonces la multiplicación del álgebra define una aplicación bilineal de $B \times B$ en B.

La aplicación $\varphi_m : N \to P$ que manda n hasta $\varphi(m,n)$ es una aplicación lineal. La función $\varphi : M \to \mathrm{Hom}_A(N,P)$ que manda m hasta φ_m es asimismo lineal. Con estas construciones tenemos el siguiente isomorfismo

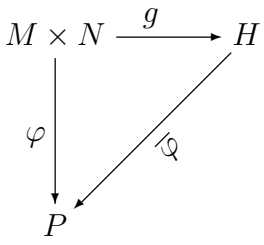
$$L_2(M \times N, P) \sim \mathrm{Hom}(M, \mathrm{Hom}(N,P))$$

El lector puede comprobar que efectivamente es un isomorfismo. Esta construcción no es más que la generalización del concepto de polaridad asociado a una métrica o a una forma cuadrática que se estudia en el Algebra Lineal.

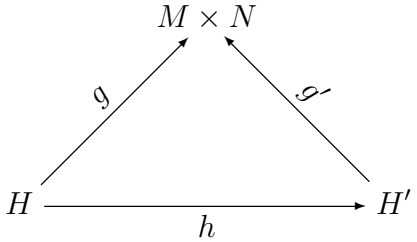
Definición 13.2 *Llamamos* producto tensorial *de M y N a un par (g, H) constituido por una función g y módulo H con las siguientes propiedades:*

I) *$g : M \times N \to H$ es bilineal.*

II) (Propiedad universal) *Si $\varphi : M \times N \to P$ es una aplicación bilineal, existe una única aplicación lineal $\overline{\varphi}$ que hace conmutativo el diagrama*



Veamos que si dos módulos H y H' son un producto tensorial de M yN, con aplicaciones bilineales g y g', entonces existe un único isomorfismo $h : H \to H'$ que hace conmutativo el diagrama



Por lo tanto, el producto tensorial de M y N, si existe, es único salvo isomorfismos.

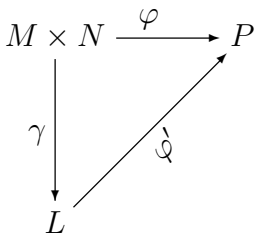
Supongamos que $P = H'$ y $\varphi = g'$. Existe un único morfismo $h : H \to H'$ tal que $gh = g'$. Cambiando los papeles, existe un único morfismo $h' : H' \to$

H que cumple $g'h' = g$. Luego $g'(h'h) = g'$. Así $h'h$ debe ser la identidad de M. Por ello h es inyectivo. El mismo argumento prueba la epiyectividad.

Veamos ahora que efectivamente el producto tensorial existe.

Sea L un módulo libre, con una base cuyo cardinal sea igual al cardinal del producto cartesiano $M \times N$.

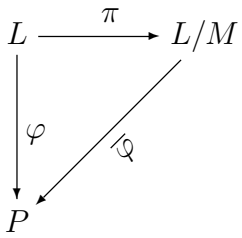
Sea $\gamma : M \times N \to L$ una biyección de $M \times N$ con una base de L. Si $\varphi : M \times N \to P$ es una función arbitraria, existe una única aplicación lineal φ' que cierra el diagrama



Resulta que φ es bilineal si solo si φ' se anula sobre los elementos:

$$\begin{aligned} \gamma(m + m', n) - \gamma(m, n) - \gamma(m', n) \\ \gamma(m, n + n') - \gamma(m, n) - \gamma(m, n') \\ \gamma(am, n) - a\gamma(m, n) \\ \gamma(m, an) - a\gamma(m, n) \end{aligned}$$

Si designamos por M al submódulo generado por estos elementos, φ' se anula sobre todo M. Debido a esto factoriza, de modo único a traves de la proyección canónica dando una aplicación $\overline{\varphi} : L/M \to P$ que hace conmutativo el diagrama



Por ello el par $(\pi\,\gamma,\ L/M)$ satisface la definición de producto tensorial pues $\overline{\varphi}$ es única. Hemos probado entonces la existencia del producto tensorial de dos módulos cualesquiera.

El producto tensorial se denota $M \otimes_A N$ o simplemente $M \otimes N$ si se sobreentiende el anillo A. Existe entonces una aplicación bilineal

$$g : M \times N \to M \otimes N$$

La imagen del par (m, n) por esta aplicación se denota $m \otimes n = g(m, n)$ y leeremos "m tensorial n".

Las propiedades de bilinealidad se traducen en la nueva notación en que $\otimes$ sea un "producto":

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n \\ m \otimes (n + n') &= m \otimes n + m \otimes n' \\ a(m \otimes n) &= (am) \otimes n = m \otimes (an)\end{aligned}$$

Utilizando la definición de base del módulo libre L es fácil comprobar que $g(M \times N)$ genera linealmente el módulo $M \otimes N$. Todo elemento del producto tensorial es combinación lineal finita de elementos de la forma $m \otimes n$. Ello no significa sin embargo que todo elemento del producto tensorial sea de la forma $m \otimes n$, afirmación que en general es falsa.

Sea ahora $\varphi : M \to M'$ y $\phi : N \to N'$ lineales. La aplicación

$$\begin{array}{rccc}\varphi \times \phi : & M \times N & \to & M' \otimes N' \\ & (m, n) & \to & \varphi(m) \otimes \phi(n)\end{array}$$

es bilineal. Existe una aplicación lineal, que denotamos $\varphi \otimes \phi$ que satisface

$$\varphi \otimes \phi \, (m \otimes n) = \varphi(m) \otimes \phi(n)$$

Recordemos que $\varphi \otimes \phi$ es pura y simplemente notación. No debe considerarse como el producto tensorial de dos elementos de los módulos de homomorfismos.

Lema 13.1 $M \otimes_A A \sim M$

Demostración.

La función producto por escalares $\varphi : A \times M \to M$ es bilineal. Existe una única aplicación lineal $\overline{\varphi} : A \otimes M \to M$ que cierra el diagrama. La aplicación es epiyectiva puesto que $m = \overline{\varphi}(1 \otimes m)$.

Todo elemento de $A \otimes M$ es combinación lineal finita de elementos de la forma $a \otimes m$. Si $\overline{\varphi}(a \otimes m) = 0$ entonces am debe ser cero y por lo tanto $a \otimes m = 1 \otimes am = 0$. $\square$

Teorema 13.2 $M' \stackrel{\varphi}{\to} M \stackrel{\phi}{\to} M'' \to 0$ *es exacta si y solo si para todo módulo* N *la sucesión*

$$M' \otimes N \xrightarrow{\varphi \otimes \mathrm{Id}} M \otimes N \xrightarrow{\phi \otimes \mathrm{Id}} M'' \otimes N \longrightarrow 0$$

es exacta.

La suficiencia es consecuencia del lema. La necesidad es puro cálculo. También puede realizarse la demostración teniendo en cuenta el isomorfismo

$$\mathrm{Hom}(M \otimes N, P) \sim \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

y el resultado análogo a este teorema pero utilizando los módulos de homomorfismos. $\square$

Estudiemos ahora algunas propiedades del producto tensorial. Daremos los isomorfismos y la forma en la que se construyen.

Propiedades.

- $(M \otimes N) \otimes P = M \otimes (M \otimes P)$; $\quad (m \otimes n) \otimes p \to m \otimes (n \otimes p)$. Asociatividad. En general dicho módulos se denota simplemente $M \otimes N \otimes P$.
- $M \otimes N = N \otimes M$: $\quad m \otimes n \to n \otimes m$. Conmutatividad.
- $(\oplus_{i \in I} M_i) \otimes N = \oplus_{i \in I} (M_i \otimes N)$; $\quad (\sum m_i) \otimes n \to \sum (m_i \otimes n)$. Distrubutividad (infinita).
- $M \otimes A = A \otimes M = M$. Elemento neutro.

Estas propiedades justifican el nombre de producto que recibe la construcción que hemos realizado.

Problemas

81 Sea A un subanillo de B ($A \subset B$). Comprobar si $M \otimes_A N$ es igual a $M \otimes_B N$ o no lo es.

82 Si p y q son dos números primos entre si entonces

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_q = 0$$

En general $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = \mathbb{Z}_d$ donde d es el máximo común divisor de m y n.

83 Probar que el producto tensorial de módulos libres es libre. Dadas dos bases en los módulos encontrar una base de $M \otimes N$. Determinar la dimensión del producto tensorial.

84 Si una sucesión exacta escinde la sucesión que se obtiene haciendo producto tensorial con otro módulo es también exacta.

85 Probar que $\mathrm{Id} \otimes \mathrm{Id} = \mathrm{Id}$.
Probar que $(f \circ f') \otimes (g \circ g') = (f \otimes g) \circ (f' \otimes g')$.
Probar que si f y g son isomorfismos entonces $f \otimes g$ también.

86 Probar que el producto tensorial de dos módulos M y N está generado por elementos de la forma $m \otimes n$.

Probar que la aplicación $g : M \times N \to M \otimes N$ no es nunca inyectiva, por lo que nunca se puede considerar a $M \times N$ como un submódulo del producto tensorial.

87 Considerense aplicaciones trilineales y construyase del mismo modo un producto tensorial de tres módulos. Probar que el módulo resultante se puede obtener a partir del producto tensorial de aplicaciones bilineales.

88 Sea G un grupo finito. Entonces $\mathbb{Q} \otimes_{\mathbb{Z}} G = 0$. En el capítulo 17 generalizaremos este resultado a todo módulo de torsión.

89 Sea A un anillo y $\mathfrak{a}$ un ideal. Probar que

$$(A/\mathfrak{a}) \otimes_A M \sim M/\mathfrak{a}M$$

14. Extensión de escalares

Sea A y B dos anillos con unidad y $\varphi : A \to B$ un morfismo de anillos con unidad. Si M es un conjunto dotado de estructura de B-módulo, introducimos en él una estructura de A-módulo, asociada al morfismo φ. Por definición

$$am = \varphi(a)m$$

El A-módulo construido se dice que se ha obtenido del B-módulo M por restricción de escalares a través del morfismo φ. Normalmente cometeremos el abuso de notación de sobreentender φ. En muchos casos el morfismo será inyectivo.

Está asociación es un functor covariante de la categoría de A-módulos en la de B-módulos, pues toda aplicación lineal sobre el anillo B también lo es sobre el anillo A.

El problema que nos proponemos ahora es el inverso. Dado un A-módulo construir un B-módulo, de tal manera que la asociación sea un functor covariante entre las categorías de A-módulos y la categoría de B-módulos. Para

no recargar la notación, emplearemos muchas veces 1 en lugar de la identidad Id del respectivo módulo.

Si $\varphi : A \to B$ es un morfismo de anillos, entonces B se puede considerar un A-módulo. Sea $M_B = M \otimes_A B$. Naturalmente este conjunto tiene estructura de A-módulo. Introduciremos en él una estructura de B-módulo.

Dado $b \in B$ se tiene que la aplicación

$$1 \otimes\ b : M_B \to M_B$$

es un morfismo de grupos. Definiendo el morfismo

$$\begin{array}{ccc} B & \to & \mathrm{End}_{gr}(M_B) \\ b & \to & 1 \otimes\ b \end{array}$$

se obtiene una estructura de módulo sobre el anillo B. Esta multiplicación cumple la propiedad

$$b(m \otimes b') = m \otimes bb'$$

que es la propiedad que normalmente empleamos en los cálculos.

Decimos que el B-módulo M_B se ha obtenido del A-módulo M por extensión de escalares o por el cambio de base $\varphi : A \to B$.

Ejemplos.

- El $\mathbb{C}$-espacio vectorial obtenido a partir del $\mathbb{R}$-espacio $\mathbb{R}^n$ es justamente $\mathbb{C}^n$, donde el morfismo de anillos es la inyección natural.
- Del mismo modo a partir de $\mathbb{Z}^n$ se obtiene $\mathbb{R}^n$.
- Si G es un grupo finito entendido como $\mathbb{Z}$-módulo resulta que $G_{\mathbb{Q}} = 0$.
- Sea A un anillo y I un ideal. El morfismo de paso al cociente $\pi : A \to A/I$ sirve para definir una extensión de escalares. En particular cuando el ideal es máximal, sabemos que A/I es un cuerpo y por tanto la extensión de escalares produce un espacio vectorial. Esta construcción se empleará a veces para probar resultados sobre módulos, basandonos en los resultados sobre espacios vectoriales.

Si $\varphi : M \to M'$ es un morfismo de A-módulos entonces

$$\varphi \otimes 1 : M_B \to M_B$$

es un morfismo de B módulos. En general denotaremos $\varphi_B = \varphi \otimes 1$. Se cumple la fórmula $(\varphi\phi)_B = \varphi_B\phi_B$. Ya podemos construir entonces un functor covariante, asociando a cada A-módulo el B-módulo M_B y a cada aplicación lineal sobre A, el B-morfismo φ_B.

Teorema 14.1 (Propiedad universal) *Sea $\varphi : A \to B$ de anillos. M un A-módulo y N un B-módulo, que lo entenderemos también como A-módulo restringiendo escalares. Sea $h : M \to N$ un morfismo de A-módulos. Existe una única aplicación B-lineal $\overline{h}$*

$$\overline{h} : M_B \to N$$

que cumple $\overline{h}(x \otimes 1) = h(x)$.

Demostración.

Como se cumple que $m \otimes b = b(m \otimes 1)$, necesariamente sobre estos elementos debe definirse como

$$\overline{h}(m \otimes b) = b\overline{h}(m \otimes 1) = bh(m)$$

Por la propiedad universal del producto tensorial $\overline{h}$ existe. Unicamente queda probar que en efecto en morfismo de B-módulos, lo cual es sencillo de ver.

Se tiene entonces la igualdad

$$\mathrm{Hom}_A(M, N) = \mathrm{Hom}_B(M_B, N)$$

que es precisamente la propiedad universal. □

Problemas

90 Probar las afirmaciones:

- Si M es finito generado sobre A, entonces M_B es finito generado sobre B.
- Si M es libre sobre A, entonces M_B es libre sobre B.
- Si M es proyectivo sobre A, entonces M_B es proyectivo sobre B.

91 Probar la verdad o falsedad de la afirmación:
El morfismo $\varphi : M \to M_B$ dado por $m \to m \otimes 1$ es inyectivo.

92 Consideremos la aplicación

$$\begin{array}{ccc} B \times B \times M & \to & B \otimes M \\ (a, b, x) & & ab \otimes m \end{array}$$

es trilineal sobre A. Así se induce una aplicación lineal

$$B \otimes (B \otimes M) \to B \otimes M$$

y esta una aplicación bilineal

$$B \times (B \otimes M) \to B \otimes M$$

Comprobar que esta aplicación dota al conjunto $B \otimes M$ de estructura de B-módulo y que tal estructura coincide con la introducida en el texto.

93 Sea $\varphi : A \to B$ y $\mu : B \to C$ morfismo de anillos. Comprobar que se cumple la igualdad $(M_B)_C = M_C$ donde la estructura de C-módulo esta asociada a la composición de aplicaciones.

94 Demostrar que $(M \otimes_A N)_B$ y $(M_B \otimes_B N_B)$ son isomorfos como B-módulos.

95 Sabemos que todo anillo tiene un ideal máximal. Por lo tanto en todo anillo existe al menos un morfismo de anillos $\varphi : A \to k$ valorado en un cuerpo. Utilizar esta extensión para probar que dos bases finitas de un módulo libre de rango finito tienen siempre igual número de elementos.

15. Algebras sobre anillos

Gran parte de los conceptos y construcciones de este capítulo son exactamente iguales a los que se estudian en la teoría de anillos. Muchos resultados se prueban y provienen de esta teoría, que suponemos conocida del lector. Otros resultados se dan en los problemas.

Definición 15.1 *Sea $\mathcal{B}$ un conjunto. Una estructura de A-álgebra sobre $\mathcal{B}$ es la dada por:*

I) *Una estructura de A-módulo sobre $\mathcal{B}$.*

II) *Una aplicación bilineal $\varphi : \mathcal{B} \times \mathcal{B} \to \mathcal{B}$, llamada producto o multiplicación.*

Normalmente $\varphi(a, b)$ se denota $a \cdot b$ o simplemente ab. Esta operación es distributiva respecto a ambos factores y además cumple

$$a(xy) = x(ay) = (ax)y$$

donde $a \in A$ y $x, y \in \mathcal{B}$.

Si la multiplicación es una operación asociativa, el álgebra se denomina álgebra asociativa. Si el producto es conmutativo, el álgebra se llama conmutativa. Si el producto posee un elemento neutro, este necesariamente debe ser único. Este elemento se llama unidad del álgebra y se dice que $\mathcal{B}$ es un álgebra con unidad.

Definición 15.2 *Sean $\mathcal{B}$ y $\mathcal{B}'$ dos álgebras sobre A. Una función $\varphi : \mathcal{B} \to \mathcal{B}'$ es un morfismo de A-álgebras si:*

I) *φ es morfismo de las estructuras de A-módulo.*

II) *$\varphi(xy) = \varphi(x)\varphi(y)$ para todo elemento del álgebra.*

Si las álgebras tienen unidad y se cumple $\varphi(1) = 1$, se dice que es un morfismo de álgebras con unidad.

Tomando las A-álgebras como objetos y los morfismos de A-álgebra tenemos una categoría, la categoría de A-álgebras.

Ejemplos.

- Todo anillo A se puede considerar como una A-álgebra.
- Todo anillo es una $\mathbb{Z}$-álgebra.
- Si X es un espacio topológico, $C(X, \mathbb{R})$ es una $\mathbb{R}$-álgebra.
- El conjunto de tensores sobre un espacio vectorial forman una k-álgebra, el álgebra tensorial del k-espacio.
- Un espacio vectorial junto con un tensor de tipo T_2^1 es un álgebra aunque en general no será ni asociativa ni conmutativa.
- Los endomorfismos de un módulo junto con la composición.
- Los endomorfismos de un módulo, con el producto

$$f \cdot g = [f, g] = fg - gf$$

  forman un álgebra no asociativa, ni conmutativa.
- Los polinomios sobre A, ya sea en una o varias variables.
- Sea k un cuerpo e I un ideal del anillo de polinomios. El conjunto $k(x)/I$ es un álgebra de dimensión finita sobre k. El estudio de las álgebras de dimensión finita sobre un cuerpo es una parte importante de lo que en matemáticas se denomina teoría de Galois.

Nosotros consideraremos solamente álgebras asociativas y con unidad. Por lo tanto de ahora en adelante, cuando nos refiramos a una A-álgebra supondremos implicitamente que es asociativa y que tiene una unidad, que denotaremos 1. Alguna de las álgebras que construiremos no será conmutativa. Por lo tanto podemos dar una nueva definición de A-álgebra:

Definición 15.3 *Un A-álgebra $\mathcal{B}$ es un anillo (posiblemente no conmutativo) que tiene una estructura de A-módulo que verifica:*

$$a(mn) = (am)n = m(an) \quad a \in A, \quad m,\, n \in \mathcal{B}$$

Definición 15.4 *Un subconjunto $\mathcal{C}$ de $\mathcal{B}$ es una subálgebra si:*

I) *$\mathcal{C}$ es un submódulo.*

II) *$\mathcal{C}$ es un subanillo de $\mathcal{B}$.*

Es una subálgebra con unidad si $1 \in \mathcal{C}$.

La intersección de subálgebras es otra subálgebra. Podemos hablar de la subálgebra engendrada por un subconjunto de $\mathcal{B}$. Exactamente igual podemos hablar de la subálgebra con unidad engendrada por un subconjunto. En este caso necesariamente debe contener a 1.

Definición 15.5 *Un subconjunto $\mathcal{I} \subset \mathcal{B}$ es un ideal (bilateral) si:*

I) *$\mathcal{I}$ es un submódulo.*

II) *$\mathcal{I}$ es un ideal de $\mathcal{B}$.*

La intersección de ideales es un ideal. Tiene sentido entonces hablar del ideal engendrado por un subconjunto de $\mathcal{B}$.

Se puede introducir en $\mathcal{B}$ una relación de equivalencia módulo un ideal. El conjunto cociente adquiere entonces una estructura de módulo, pero además también tiene una estructura de álgebra dada por la multiplicación

$$\pi(x)\pi(y) = \pi(xy)$$

que no depende de los representantes que tomemos. La aplicación canónica de paso al cociente es un morfismo de álgebras.

El conjunto de polinomios sobre un anillo A es un objeto libre en la categoría. Para no recargar la notación enunciaremos su propiedad universal para conjuntos finitos, pero es también válida para cualquier conjunto.

Teorema 15.1 (Propiedad universal) *Sea $\mathcal{B}$ un A-álgebra. Sea $\{b_1, \ldots, b_s\}$ un subconjunto de $\mathcal{B}$. Existe un único morfismo de A-álgebras*

$$\varphi : A(x_1, \ldots, x_s) \to \mathcal{B}$$

que cumple $\varphi(x_i) = b_i$.

Demostración.

Como φ es un morfismo de anillos cumple $\varphi(x_i^n) = b_i^n$. Así podemos construir φ aplicando dicho propiedad a cada monomio utilizando la propiedad multiplicativa del morfismo. □

Si $\mathcal{B}$ es una A-álgebra, una graduación del módulo $\mathcal{B}$ de tipo Δ es compatible con la estructura de A-álgebra si:

I) $\mathcal{B}_\lambda \cdot \mathcal{B}_\mu \subset \mathcal{B}_{\lambda+\mu}$

II) $A \cdot \mathcal{B}_\lambda \subset \mathcal{B}_\lambda$

Definición 15.6 *Un* álgebra graduada *es un álgebra con una graduación compatible.*

Llamamos morfismos de álgebras graduadas a los morfismos de álgebra que se sean de grado 0. Podemos entonces formar la categoría de A-álgebras graduadas.

Seab $\mathcal{B}$ y $\mathcal{C}$ dos A-álgebras con unidad. Consideremos la siguiente aplicación

$$\mathcal{B} \times \mathcal{C} \times \mathcal{B} \times \mathcal{C} \to \mathcal{B} \otimes \mathcal{C}$$

$$(e, f, e', f') \to ee' \otimes ff'$$

Esta aplicación es multilineal. Por la propiedad universal del producto tensorial, le corresponde una única aplicación lineal

$$\mathcal{B} \otimes \mathcal{C} \otimes \mathcal{B} \otimes \mathcal{C} \to \mathcal{B} \otimes \mathcal{C}$$

Por la asociatividad, esta aplicación lineal induce una aplicación lineal

$$(\mathcal{B} \otimes \mathcal{C}) \otimes (\mathcal{B} \otimes \mathcal{C}) \to \mathcal{B} \otimes \mathcal{C}$$

De nuevo aplicando la propiedad universal del producto tensorial, a esta función le corresponde una aplicación bilineal

$$(\mathcal{B} \otimes \mathcal{C}) \times (\mathcal{B} \otimes \mathcal{C}) \to \mathcal{B} \otimes \mathcal{C}$$

Definición 15.7 *Llamamos* producto tensorial de las A-álgebras $\mathcal{B}$ *y* $\mathcal{C}$*, al módulo* $\mathcal{B}\otimes\mathcal{C}$ *dotado de la aplicación bilineal que se ha construido anteriormente.*

El álgebra que acabamos de construir es asociativa con unidad. El producto en dicha álgebra cumple la relación:

$$(e \otimes f) \cdot (e' \otimes f') = ee' \otimes ff'$$

Naturalmente la identidad de este álgebra es $1 \otimes 1$ y el inverso de $e \otimes f$ es $e^{-1} \otimes f^{-1}$.

Para cada álgebra $\mathcal{B}$ existe una aplicación canónica de $\mathcal{B} \to \mathcal{B} \otimes \mathcal{C}$ dada por $e \to e \otimes 1$ que es un morfismo de álgebras con unidad. Esta aplicación se denotara $i_{\mathcal{B}}$ y es la inyección natural de $\mathcal{B}$ en $\mathcal{B} \otimes \mathcal{C}$.

Como casi todas las construcciones que realizamos, el producto tensorial de álgebras tiene una propiedad universal que pasamos a enunciar.

Proposición 15.2 *Cada par de morfismos de álgebras con unidad* $\varphi : \mathcal{B} \to \mathcal{G}$ *y* $\phi : \mathcal{C} \to \mathcal{G}$ *define un morfismo de álgebras*

$$\varphi \oplus \phi : \mathcal{B} \otimes \mathcal{C} \to \mathcal{G}$$

mediante la fórmula $\varphi \oplus \phi = m(\varphi \otimes \phi)$*, donde* m *es la aplicación bilineal de* $\mathcal{G} \times \mathcal{G}$ *en* $\mathcal{G}$ *que lo dota de estructura de álgebra.*

Reciprocamente, cada morfismo $h : \mathcal{B} \otimes \mathcal{C} \to \mathcal{G}$ *es de la forma* $\varphi \oplus \phi$ *para un único par de morfismos.*

Demostración.

$\Rightarrow$) Simple comprobación. Solo hay que comprobar que es morfismo de anillos, pues la linealidad se tiene por construcción.

$\Leftarrow$) Si $h : \mathcal{B} \otimes \mathcal{C} \to \mathcal{G}$ es un morfismo de álgebras, entonces $\varphi = h \circ i_{\mathcal{B}}$ cumple $\varphi(x) = h(x \otimes 1)$. Analogamente se construye $\phi = h \circ i_{\mathcal{C}}$. Naturalmente tanto φ como ϕ son morfismos de álgebras y cumplen $h = \varphi \oplus \phi$. $\square$

Este teorema se puede expresar por el isomorfismo

$$\mathrm{Hom}_{A-al}(\mathcal{B} \otimes \mathcal{C}, \mathcal{G}) \sim \mathrm{Hom}_{A-al}(\mathcal{B}, \mathcal{G}) \times \mathrm{Hom}_{A-al}(\mathcal{C}, \mathcal{G})$$

Esta propiedad nos dice que el producto tensorial es justamente la suma directa en la categoría de A-álgebras con unidad. Por eso se utiliza la notación $\varphi \oplus \phi$.

Problemas

96 Por analogía con la teoría de anillos, el lector probará los siguientes resultados referentes a la teoría de A-álgebras:

- Enunciar el teorema de factorización canónica.
- Caracterizar la mínima subálgebra que contiene a un subconjunto.
- Definir centro de un álgebra.
- Construir el producto directo de dos álgebras.
- Suma e intersección de ideales.

97 Definir subálgebra e ideal graduados. Construyase el cociente de un álgebra graduada módulo un ideal graduado.

Calcula el grado de la unidad y del inverso de un elemento homogéneo, naturalmente suponiendo que existen.

98 Resolver las siguientes cuestiones:

- Definir el concepto de álgebra de generación finita.

- Probar que toda A-álgebra de generación finita es isomorfa a un cociente de un anillo de polinomios en un número finito de variables.
- Probar que toda A-álgebra es isomorfa a un cociente de un anillo de polinomios, en general con un número infinito de variables.

99 Calcular el producto tensorial de $A(x)$ con $A(y)$.

100 Resolver las siguientes cuestiones:

- Si $\mathcal{B}$ y $\mathcal{C}$ son conmutativas, ¿lo es $\mathcal{B} \otimes \mathcal{C}$?
- Si $\mathcal{B}$ y $\mathcal{C}$ son asociativas, ¿lo es $\mathcal{B} \otimes \mathcal{C}$?
- Si $A \subset B$ es un subanillo. Calcular $A(x) \otimes B$.

101 Comprobar que $\mathcal{B} \otimes \mathcal{C} \sim \mathcal{C} \otimes \mathcal{B}$.

102 Una subálgebra es graduada si y solo si puede ser generada por elementos homogéneos.

103 Definir el concepto de extensión de escalares para una A-álgebra.

104 Dado un morfismo de álgebras, ver que sucede con las imagenes y anti-imagenes de subálgebras e ideales.

105 Sea $\varphi : A \to B$ un morfismo de anillos con unidad, cuya imagen este en el centro del anillo B. Entonces B es una A-álgebra.

106 Probar los siguientes enunciados:

- Las series formales $A[[x]]$ es un álgebra sobre A.
- Los polinomios $A[x]$ forman una subálgebra. Ver si es un ideal.
- El conjunto de funciones continuas sobre $\mathbb{R}^n$, $C(\mathbb{R}^n, \mathbb{R})$ es un álgebra sobre el cuerpo real. $C^\infty(\mathbb{R}^n, \mathbb{R})$ es una subálgebra. ¿Será un ideal?

- Los cuaterniones son un álgebra no conmutativa sobre el cuerpo de los reales.

107 Probar que el centro de un álgebra es una subálgebra. Comprobar si es o no un ideal bilátero.

108 Sea k un cuerpo y $p(x)$ un polinomio. Calcular la dimensión de la k-álgebra $k[x]/p(x)$.

109 Dada una A-álgebra $\mathcal{B}$ decimos que una aplicación

$$D : \mathcal{B} \to \mathcal{B}$$

es una derivación si

I) $D(a) = 0$ si $a \in A$.

II) $D(bc) = D(b)c + bD(c)$ si $b, c \in \mathcal{B}$.

Dotar de estructura de A-módulo al conjunto de todas las derivaciones.

Probar que si D y D' son dos derivaciones, entonces $[D, D'] = DD' - D'D$ es también una derivación.

Calcular las derivaciones de la k-álgebra $k(x)$.

110 Probar que los elementos invertibles de un álgebra con unidad forman un grupo. Aplicarlo al caso de las matrices con coeficientes en A.

16. Algebra tensorial

Veamos como utilizando el concepto de producto tensorial podemos construir álgebras que contienen de modo natural al anillo al anillo A y al módulo M.

Definición 16.1 *El producto tensorial de p copias de módulo M se llama* potencia tensorial p-ésima *y se denota $T^p(M)$. Por convenio $T^0(M) = A$.*

Definición 16.2 *Llamamos* álgebra tensorial *de M, al módulo suma directa de todos los A-módulos $T^p(M)$ y se denota $\tau(M)$*

$$\tau(M) = \oplus_{p\geq 0} T^p(M)$$

Por definición $\tau(M)$ es un módulo graduado de tipo $\mathbb{N}$. Los elementos del álgebra tensorial se denominan tensores. A las imagenes por las inyecciones canónicas de los elementos de $T^p(M)$ se les llama tensores homogéneos de grado p. Cada elemento del álgebra tensorial se puede escribir de modo único como suma finita de tensores homogéneos.

Los isomorfismos canónicos $T^p(M) \otimes T^q(M) \sim T^{p+q}(M)$ deducidos de la asociatividad del producto tensorial, tienen asociadas aplicaciones bilineales:

$$\varphi_{pq} : T^p(M) \times T^q(M) \to T^{p+q}(M)$$

Extendiendo estas aplicaciones por bilinealidad, tenemos una aplicación bilineal de $\tau(M) \times \tau(M) \to \tau(M)$ que restringida a cada potencia coincide con φ_{pq}. Dicha aplicación se denota $\otimes$ y se llama producto tensorial. Esta aplicación dota a $\tau(M)$ de estructura de A-álgebra asociativa. La asociatividad se deduce de la asociatividad del producto tensorial de módulos. En general este álgebra no será conmutativa.

Es de notar que la expresión $m \otimes m'$ que definimos en el capítulo 13 era pura notación. Sin embargo ahora es el producto de dos elementos del álgebra tensorial y es un elemento homogéneo de grado 2.

Este álgebra contiene a A y a M mediante las inyecciones canónicas de estos módulos en la suma directa, puesto que $T^0(M) = A$ y $T^1(M) = M$.

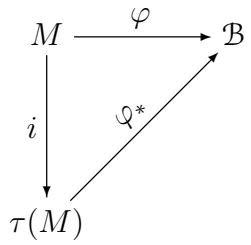
Dicho álgebra está generada por estos dos conjuntos, por lo que para definir aplicaciones que sean morfismos de álgebras, solo necesitamos conocer como actuan sobre ambos conjuntos. En el caso en que los morfismos conserven la unidad, solo es necesario conocer su acción sobre M.

El álgebra tensorial posee una propiedad universal y por lo tanto está definida salvo un isomorfismo.

Teorema 16.1 (Propiedad universal) *Sea $\mathcal{B}$ una A-álgebra con unidad. Cada morfismo de módulos $\varphi : M \to \mathcal{B}$ induce un único morfismo de álgebras con unidad $\varphi_* : \tau(M) \to \mathcal{B}$ que sobre M coincide con φ.*

Demostración.

El teorema afirma que existe un cierto φ_* que cierra el diagrama



Necesariamente $\varphi_*(a) = a$ si $a \in A$. Los elementos de la forma $m_1 \otimes \cdots \otimes m_p$ generan $T^p(M)$. Como φ_* debe mandar el producto al producto y coincidir con φ sobre M, necesariamente

$$\varphi_*(m_1 \otimes m_2 \otimes \cdots \otimes m_p) = \varphi(m_1) \cdot \varphi(m_2) \ldots \varphi(m_p)$$

Estos elementos generan $T^p(M)$, así existe un único morfismo

$$\varphi_p : T^p(M) \to \mathcal{B}$$

La existencia de una aplicación lineal con estas propiedades esta garantizada por la propiedad universal del producto tensorial.

Aplicando la propiedad universal de la suma directa existe $\varphi_* : \tau(M) \to \mathcal{B}$ que sobre cada potencia tensorial coincide con φ_p. Una comprobación rutinaria muestra que en efecto el morfismo φ_* así definido es morfismo de álgebras. □

Corolario 16.2 *Sea $\varphi : M \to N$ un morfismo de A-módulos. Existe una única aplicación*

$$\varphi_* : \tau(M) \to \tau(N)$$

que sobre M coincide con φ.

Demostración.

Consideremos el morfismo φ compuesto con la inyección natural de N en su álgebra tensorial. Aplicando la propiedad universal obtenemos el morfismo φ_* pedido. □

Si ϕ es otro morfismo tenemos que $(\varphi\phi)_* = \varphi_*\phi_*$.

Por lo tanto podemos construir un functor covariante de la categoría de A-módulos en la de A-álgebras asociando a cada módulo su álgebra tensorial y a cada morfismo φ el morfismo φ_*.

Proposición 16.3 *Se cumple la fórmula*

$$\tau(M \oplus N) = \tau(M) \otimes \tau(N)$$

Demostración.

$$\mathrm{Hom}_{A-al}(\tau(M \oplus N), \mathcal{B}) = \mathrm{Hom}(M \oplus N, \mathcal{B}) = \mathrm{Hom}(M, \mathcal{B}) \times \mathrm{Hom}(N, \mathcal{B})$$

aplicando la propiedad universal del álgebra tensorial y de la suma directa de módulos. Esto es igual a

$$\mathrm{Hom}_{A-al}(\tau(M), \mathcal{B}) \times \mathrm{Hom}_{A-al}(\tau(N), \mathcal{B}) = \mathrm{Hom}_{A-al}(\tau(M) \otimes \tau(N), \mathcal{B})$$

Como ambas cumplen la misma propiedad universal concluimos que las dos álgebras son isomorfas. □

Si recordamos que el producto tensorial era la suma directa en la categoría de A-álgebras, esta proposición será más evidente.

Otra propiedad importante del álgebra tensorial es su estabilidad por extensión de escalares.

Proposición 16.4 *Sea $\varphi : A \to B$ un morfismo de anillos, que entenderemos como una extensión de escalares. Se tiene el siguiente isomorfismo:*

$$(\tau(M))_B \sim \tau(M_B)$$

Demostración.

Es consecuencia de la propiedad distributiva del producto tensorial de la que se deduce

$$T^p(M) \otimes B = T^p(M \otimes B)$$

por lo que se concluye que

$$\tau(M)_B = \tau(M) \otimes B = \tau(M \otimes B) = \tau(M_B)$$

que afirma que el álgebra es estable por extensión de escalares. □

El álgebra tensorial tiene muchas propiedades, sin embargo adolece de la falta de conmutatividad. Construiremos un álgebra que si sea conmutativa y que contenga tanto a A como a M.

Definición 16.3 *Sea I el ideal bilatero graduado de $\tau(M)$ generado por los elementos de la forma $m \otimes m' - m' \otimes m$. El álgebra $S(M) = \tau(M)/I$ se llama* álgebra tensorial simétrica *del módulo M. El producto en este álgebra se denotará por un punto y se le llamará* producto simétrico.

Este álgebra admite una graduación inducida por la del álgebra tensorial, pues I es un ideal graduado. En efecto

$$I = \oplus_{p \geq 0} I^p \text{ donde } I^p = I \cap T^p(M)$$

Si denotamos por $S^p = T^p(M)/I^p$ tenemos que $S(M) = \oplus_{p \geq 0} S^p$. El módulo S^p se llama p-ésima potencia simétrica del módulo M.

Este álgebra contiene a A y a M puesto que $I^0 = 0 = I^1$ ya que está generado por elementos homogéneos de grado 2.

Teorema 16.5 (Propiedad universal) *Sea $\mathcal{B}$ un álgebra con unidad. Sea $\varphi : M \to \mathcal{B}$ un morfismo de A-módulos que cumpla $\varphi(m)\varphi(m') = \varphi(m')\varphi(m)$ (lo cual ocurre siempre si $\mathcal{B}$ es conmutativa). Entonces existe un único morfismo de A-álgebras con unidad $\varphi_* : S(M) \to \mathcal{B}$ que sobre M coincide con φ.*

Demostración.

Sea $\varphi_* : \tau(M) \to \mathcal{B}$ el morfismo que sabemos que existe por la propiedad universal del álgebra tensorial. Tenemos que φ_* se anula sobre los generadores del ideal I por la condición de conmutatividad que tenemos como hipótesis. Así φ_* se anula sobre todo el ideal I. Sabemos entonces que factoriza dando una aplicación de $S(M)$ en $\mathcal{B}$. La unicidad es clara pues los elementos de la forma $m_1 \cdot m_2 \dots m_p$ generan el álgebra simétrica. □

Corolario 16.6 *El álgebra simétrica es estable por extensión de escalares. Si $\varphi : A \to B$ es un morfismo de anillos*

$$S(M)_B = S(M_B)$$

Corolario 16.7 *Se tiene la fórmula*

$$S(M \oplus N) = S(M) \otimes S(M)$$

Consideremos ahora el ideal graduado I generado por los elementos de la forma $m \otimes m$. El álgebra cociente $\bigwedge(M) = \tau(M)/I$ se denomina álgebra exterior del módulo M. El producto en este álgebra de denota por el símbolo $\wedge$ y se denomina producto exterior.

Generalice el lector los conceptos de potencia exterior p-ésima, de elemento homogéneo de este álgebra y la inclusión tanto de A como de M en el álgebra exterior. Si ω_p, ω_q son elementos homogéneos de grado p y grado q del álgebras exterior se cumple

$$\omega_p \wedge \omega_q = (-1)^{pq}\, \omega_q \wedge \omega_p$$

Teorema 16.8 (Propiedad universal) *Sea $\varphi : M \to \mathcal{B}$ un morfismo de álgebras que cumpla $\varphi(m)^2 = 0$. Entonces existe una única aplicación de álgebras*

$$\varphi_* : \bigwedge(M) \to \mathcal{B}$$

que sobre M coincide con φ.

Problemas

111 Sea

$$I = \oplus_{p \text{ par}} T^p(M)\,, \qquad P = \oplus_{p \text{ impar}} T^p(M)$$

Entonces el álgebra tensorial admite una graduación sobre el grupo $\mathbb{Z}_2$.

112 Demostrar las siguientes afirmaciones:

- Los morfismo inducidos φ_* son de grado cero. Así podemos construir un functor de la categoría de A-módulos en la de A-álgebras graduadas.
- La restricción de φ_* a cada potencia tensorial coincide con $\varphi \otimes \cdots \otimes \varphi$.
- Si $\varphi : M \to N$ es epiyectiva, también es epiyectiva φ_*.

113 Ver la relación entre las aplicaciones multilineales simétricas y la potencia simétrica. Análogo con las aplicaciones alternadas y la potencia exterior.

114 Calcular el álgebra tensorial, simétrica y exterior del A-módulo A. Relacionar estos resultados con la teoría de polinomios.

Hacer lo mismo con el módulo A^n.

115 Probar que la potencia exterior n-ésima del módulo A^n es libre de rango 1. Sea $\varphi : A^n \to A^n$ un endomorfismo de A^n. La aplicación

$$\varphi_* : \bigwedge^n(A^n) \to \bigwedge^n(A^n)$$

consiste entonces en multiplicar por un cierto escalar. Dicho escalar se denomina determinante de φ y se denota $\det(\varphi)$. Generalizar los resultados conocidos de Algebra Lineal.

17. Localización

Nos vemos obligados en este punto a estudiar con cierto detenimiento una parte de la teoría de anillos, la localización. Después la generalización a los módulos será casi inmediata. Como siempre consideraremos anillos conmutativos y con unidad.

Definición 17.1 *Un subconjunto $S \subset A$ es* multiplicativamente cerrado *si:*

I) $1 \in S$.

II) *Si* $a, b \in S \implies ab \in S$.

En el conjunto $A \times S$ se define la siguiente relación, que el lector comprobará que es de equivalencia:

$$(a, s) \sim (b, t) \iff \text{existe } u \in S \text{ tal que } (at - bs)u = 0$$

La clase de equivalencia de (a, s) se denotará con la fracción a/s.

Con esta notación definimos las siguientes operaciones en el conjunto cociente, que denotaremos en general A_S.

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Las definiciones dadas no dependen de los representante elegidos y dotan al conjunto A_S de estructura de anillo conmutativo y con unidad. Decimos que el anillo A_S es el anillo de fracciones de A con denominadores en S.

La aplicación

$$\begin{array}{rccc} \varphi: & A & \to & A_S \\ & x & \to & x/1 \end{array}$$

es un morfismo de anillos del anillo en su anillo de fracciones. Si existiese confusión lo denotariamos por φ_S. Este morfismo, en general no es inyectivo, por lo que A no puede considerarse un subanillo de A_S.

Ejemplos.

- Sea A un dominio de integridad. Entonces $S = A - \{0\}$ es un subconjunto multiplicativamente cerrado. En este caso A_S es un cuerpo, llamado cuerpo de fracciones de A. Además el morfismo φ es inyectivo. Si $A = \mathbb{Z}$, entonces $A_S = \mathbb{Q}$.

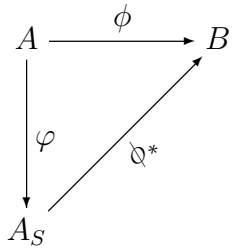
- Sea $a \in A$. Entonces $S = \{a^n\}_{n \geq 0}$ es multiplicativamente cerrado. En este caso A_S se denota A_a.

- Sea S el conjunto de elementos invertibles de A. Calcule el lector A_S.

- Sea $\mathfrak{p}$ un ideal primo de A. Por definición de ideal primo, $A - \mathfrak{p}$ es multiplicativamente cerrado. A se denota en este caso $A_{\mathfrak{p}}$ y se dice que es el localizado de A en el punto $\mathfrak{p}$.

- Sea z un punto del plano complejo. El conjunto de todos los polinomios que no se anulan en z forman un conjunto multiplicativamente cerrado S. $\mathbb{C}(x)_S$ son las funciones racionales sin polo en z.

Teorema 17.1 (Propiedad universal) *Si $\phi : A \to B$ es un morfismo de anillos con unidad y tal que $\phi(s)$ sea invertible en B para todo s de un subconjunto multiplicativamente cerrado S. Entonces existe un único morfismo de anillos ϕ_* que hace conmutativo el diagrama*



Demostración.

Necesariamente se cumple

$$\phi_*\big(1/s)\big) = \big(\phi_*(s)\big)^{-1} = \big(\phi(s)\big)^{-1}$$

Por lo tanto $\phi_*(a/s) = \phi(a)\phi(s)^{-1}$ es la única definición posible. Un par de cuentas prueban que la definición no depende del representante y que ϕ_* es un morfismo de anillos. $\square$

Sea ahora M un módulo y S un subconjunto multiplicativamente cerrado del anillo. En $M \times S$ se introduce la relación de equivalencia

$$(m, s) \sim (m', s') \text{ si } (ms' - m's)u = 0 \text{ para algún } u \in S$$

La clase de equivalencia se denota m/s. Se define la suma en este conjunto como

$$\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + m's}{ss'}$$

El conjunto de las clases de equivalencia tiene estructura de grupo abeliano. Introducimos también la multiplicación por elementos de A_S.

$$\frac{a}{s} \cdot \frac{m'}{s'} = \frac{am}{ss'}$$

Todas las construcciones son independientes del representante y dotan al conjunto cociente, que de ahora en adelante dentoraremos M_S, de una estructura de A_S-módulo. En M_S también se puede considerar la estrutura de A-módulo definida por el morfismo φ:

$$x \cdot \frac{m}{s} = \frac{xm}{s} = \varphi(x) \cdot \frac{m}{s}$$

Como en M_S existe una estructura de módulo sobre dos anillos, siempre que exista una posible confusión se debe decir cual es el anillo considerado.

Cada morfismo de A-módulo $\phi : M \to N$ induce un morfismo de A_S-módulos ϕ_S mediante la fórmula

$$\begin{array}{rccc} \phi_S : & M_S & \to & N_S \\ & m/s & \to & \phi(m)/s \end{array}$$

Si tenemos otro morfismo de módulos γ se cumple la relación $(\phi\gamma)_S = \phi_S\gamma_S$. Tenemos así construido un functor de la categoría de A-módulos en la de
A_S-módulos.

Como en el caso de los anillos, cuando S sea $A - \mathfrak{p}$ con $\mathfrak{p}$ un ideal primo, se dirá que se localiza el módulo en el punto $\mathfrak{p}$.

Proposición 17.2 *Construir el módulo de fracciones es un functor exacto. Si* $M' \xrightarrow{\phi} M \xrightarrow{\gamma} M''$ *es exacta entonces* $M'_S \xrightarrow{\phi_S} M_S \xrightarrow{\gamma_S} M''_S$ *es también exacta.*

Demostración.

$\phi\gamma = 0 \Longrightarrow (\phi\gamma)_S = 0 \Longrightarrow \phi_S\gamma_S = 0$ lo que implica que $\mathrm{Im}(\phi_S) \subset \mathrm{Ker}(\gamma_S)$.

Reciprocamente, si $\gamma(m)/s = 0$ entonces existe $t \in S$ tal que

$$t(\gamma(m)) = 0 \Longrightarrow \gamma(tm) = 0$$

Entonces $tm \in \mathrm{Ker}(\gamma) = \mathrm{Im}(\phi)$. Así $tm = \phi(m')$ lo que conduce a que

$$m/s = \phi_S(m'/s)$$

lo que concluye la demostración. □

Proposición 17.3 *Si* N *y* P *son submódulos:*

$$(N + P)_S = N_S + P_S$$

$$(N \cap P)_S = N_S \cap P_S$$

$$(M/N)_S \sim M_S/N_S$$

Demostración.

Las dos primeras propiedades nos dicen que construir módulos de fracciones induce un morfismo de retículos. La última se deduce de la sucesión exacta

$$0 \to N \to M \to M/N \to 0$$

teniendo en cuenta que se conserva la exactitud. □

El siguiente teorema nos da otro método de construcción del módulo de fracciones.

Teorema 17.4 *Sea M un A-módulo. Existe un único isomorfismo ϕ de A_S-módulos de $A_S \otimes_A M$ en M_S que manda al punto $a/s \otimes m$ hasta am/s.*

Demostración.

La aplicación

$$\begin{array}{ccc} A_S \times M & \to & M_S \\ (a/s, m) & \to & am/s \end{array}$$

es A-bilineal. Por la propiedad universal del producto tensorial existe una aplición $\phi : A_S \otimes M \to M_S$ que satisface el enunciado. Siguiendo las ideas expuestas anteriormente, compruebe el lector que en efecto es un isomorfismo y que además es un morfismo de A_S-módulos. □

Se dice que una propiedad de un A-módulo es una propiedad local, cuando se cumpla lo siguiente:

El A-módulo tiene la propiedad P si y solo si para todo punto del espectro el $A_\mathfrak{p}$-módulo asociado tiene la propiedad P.

Esta definición algebráica de localidad coincide con la idea de localidad en el sentido topológico, tras introducir en el espectro la topología de Zariski.

La importancia de este concepto radica en que las propiedades locales basta estudiarlas sobre anillos locales.

Definición 17.2 *Un anillo conmutativo y con unidad es local si tiene un único ideal maximal $\mathfrak{m}$. El cuerpo $k = A/\mathfrak{m}$ se llama cuerpo residual.*

Lema 17.5 *A es local de ideal maximal $\mathfrak{m}$ si y solo si todos los elementos de $A - \mathfrak{m}$ son invertibles.*

Demostración.

$\Rightarrow$) Si $x \in A$ no es invertible, pertenece a algún ideal maximal.

$\Leftarrow$) Si el complementario de las unidades de A es un ideal, entonces es maximal y es el único ideal maximal. □

Teorema 17.6 *$A_{\mathfrak{p}}$ es local.*

Demostración.

Los elementos de la forma a/s con $a \in \mathfrak{p}$ forman un ideal. Si s/s' no pertenece a ese ideal, este elemento es invertible y su inverso es s'/s. $\square$

Lema 17.7 (Nakayama) *Sea A local, $\mathfrak{m}$ su ideal maximal. Si M es de generación finita y $\mathfrak{m}M = M$, entonces $M = 0$.*

Demostración.

Sea $(m_1, \ldots, m_n)$ un conjunto mínimo de generadores. Como dicho conjunto genera M y además $\mathfrak{m}M = M$ tenemos que

$$m_n = a_1 m_1 + \cdots + a_n m_n \text{ con } a_i \in \mathfrak{m}$$

Entonces deducimos que

$$m_n(1 - a_n) = a_1 m_1 + \cdots + a_{n-1} m_{n-1}$$

Como $1 - a_n$ es invertible, tenemos que $(m_1, \ldots m_{n-1})$ generan M. Esto solo es posible si $M = 0$. $\square$

Corolario 17.8 *$M_{\mathfrak{m}} = 0 \Longleftrightarrow M = 0$.*

Demostración.

$M_{\mathfrak{m}} = M/\mathfrak{m}M$. $\square$

Corolario 17.9 *La condición necesaria y suficiente para que una familia genere M es que sus imagenes generen $M_{\mathfrak{m}}$.*

Demostración.

$\Leftarrow$) $M_{\mathfrak{m}} = M \otimes k$. Si $\{m_i\}$ generan M como A-módulo $\Rightarrow$ $\{m_i \otimes 1\}$ generan $M_{\mathfrak{m}}$ como k-espacio.

$\Leftarrow$) Sea N es submódulo generado por los elementos $\{m_i\}$

$$0 \to N \to M \to M/N \to 0$$

Localizando esta sucesión tenemos

$$N_{\mathfrak{m}} \to M_{\mathfrak{m}} \to (N/M)_{\mathfrak{m}} \to 0$$

$N = M$ si solo si $N_{\mathfrak{m}} \to M_{\mathfrak{m}}$ es epiyectiva y lo es pues las imagenes de m_i generan $M_{\mathfrak{m}}$. $\square$

Veamos ahora algunas propiedades locales.

Proposición 17.10 *Sea M un A-módulo. Son equivalentes.*

I) $M = 0$.

II) $M_{\mathfrak{p}} = 0 \quad \forall\ \mathfrak{p}$ *primo.*

III) $M_{\mathfrak{m}} = 0 \quad \forall\ \mathfrak{m}$ *maximal.*

Demostración.

Solo tenemos que demostrar una implicación pues las otras son evidentes.

Sea I el anulador de M. Como $m/1 = 0$ en $M_{\mathfrak{m}}$, entonces existe un u que no pertence a $\mathfrak{m}$ tal que $um = 0$. El anulador no está contenido en ningún ideal maximal. Por lo tanto el anulador es A. Entonces $1m = 0 \Longrightarrow m = 0$. $\square$

Proposición 17.11 *Sea $\phi : M \to N$ A-lineal. Son equivalentes:*

1. *ϕ es inyectiva.*
2. *$\phi_{\mathfrak{p}}$ es inyectiva para todo ideal primo.*
3. *$\phi_{\mathfrak{m}}$ es inyectiva para todo ideal maximal.*

Demostración.

Localizamos la sucesión

$$0 \to \mathrm{Ker}(\phi) \to M \to N$$

y aplicamos la proposición anterior. □

Tenemos otra proposición si sustituimos inyectiva por epiyectiva.

Corolario 17.12 *$\phi : M \to N$ es isomorfismo si y solo si lo es al localizar en cada ideal primo.*

Corolario 17.13 *Una sucesión $M \to N \to M'$ es exacta si y solo si lo es al localizarla en todos los ideales primos.*

Problemas

116 Probar que el localizado de una suma directa es la suma directa de los localizados.

117 Probar el siguiente isomorfismo

$$M_S \otimes_{A_S} N_S \sim (M \otimes N)_S$$

118 Calcular el núcleo de la aplicación canónica $m \to m/1$.

119 Llamamos soporte de un módulo M al conjunto de ideales primos tales que $M_{\mathfrak{p}} \neq 0$. Calcular el soporte de $k(x)/p(x)$.

120 Probar que $(M_S)_\tau = (M_\tau)_S$.

Deducir que la caracteristica de ser sin torsión es una propiedad local.

121 Localizando en un ideal maximal probar:

- $A^m \sim A^n$ entonces $n = m$.
- $\varphi : A^m \to A^n$ epiyectiva $\Rightarrow m \geq n$.
- $\varphi : A^m \to A^n$ inyectiva $\Rightarrow m \leq n$.

18. Módulos noetherianos

Comenzaremos este capítulo con un teorema de teoría de conjuntos ordenados.

Proposición 18.1 *Sea Σ un conjunto dotado de una relación de orden. Entonces son equivalentes las condiciones que siguen:*

I) *Cada sucesión creciente de elementos de Σ*

$$x_1 \leq x_2 \leq \cdots \leq x_n$$

es estacionaria, que quiere decir que existe un n tal que $x_n = x_{n+i}$ para todo $i > 0$.

II) *Cada subconjunto no vacio de Σ admite un elemento maximal.*

Demostración.

$i) \Rightarrow ii)$ Si no existiera elemento maximal para el subconjunto Σ, entonces por inducción crearíamos una cadena que no estaciona.

$ii) \Rightarrow i)$ $\{x_n\}_{n\geq 1}$tiene elemento maximal. $\square$

La condición $i)$ se denomina condición de cadena ascendente y la condición $ii)$ la condición maximal.

Para todo lo que sigue, Σ será el retículo de submódulos de un módulo dado.

Definición 18.1 *Un módulo M es* noetheriano *si el conjunto Σ de sus submódulos satisface alguna de las condiciones equivalentes de la proposición anterior. El orden considerado en Σ es el de la inclusión.*

Si $A \subset B$ son anillos y M es un B-módulo, puede ocurrir que M sea noetheriano como B-módulo y lo no sea como A-módulo. Esto ocurre por ejemplo en el caso $A = k$, $B = k(x)$.

Ejemplos.

- Todo grupo finito abeliano es noetheriano como $\mathbb{Z}$-módulo.
- Todo módulo simple es noetheriano.
- Todo módulo M cuyo cardinal sea finito es noetheriano sobre cualquier anillo.
- Todo k-espacio de dimensión finita.
- Si A es un dominio de ideales principales, entonces es noetheriano como A-módulo.

La importancia de los módulos noetherianos radica en el siguiente teorema

Teorema 18.2 *M es un A-módulo noetheriano si y solo si todo submódulo de M es de generación finita.*

Demostración.

$\Rightarrow$) Sea N un submódulo de M y sea Σ' el conjunto de todos los submódulos menores que N y que además sean finito generados. Como Σ cumple la condición de cadena ascendente, lo mismo le ocurre a Σ'. Sea N' un elemento maximal de Σ'. Veamos que $N' = N$. Si esto no ocurriera, existiría un vector $m \in N - N'$. Entonces $N' + < m >$ sería de generación finita y estaría contenido en N, contradiciendo la maximalidad de N.

$\Leftarrow$) Sea $N_1 \subset \cdots \subset N_n \ldots$ una cadena ascendente de submódulos. Tenemos que $\cup_i N_i$ es un submódulo. Sea $\{m_i\}$ $(i = 1, \ldots, k)$ un conjunto generador del módulo unión. Sea N_n el primer submódulo que contenga a todos los m_i. La sucesión estaciona en N_n. $\square$

Teorema 18.3 *Si $0 \xrightarrow{i} M' \to M \xrightarrow{\pi} M'' \to 0$ es exacta, entonces M es noetheriano si y solo si M' y M'' son noetherianos.*

Demostración.

$\Rightarrow$) Los submódulos de M' son submódulos de M. Entonces M' es noetheriano. Por π^{-1} los submódulos de M'' se pueden considerar incluidos en los submódulos de M. M'' es noetheriano.

$\Leftarrow$) Si $\{N_i\}$ es una cadena es M, entonces $\{i^{-1}(N_i)\}$ y $\{\pi^{-1}(N_i)\}$ son cadenas que estacionan. Entonces la cadena $\{N_i\}$ estaciona y M es noetheriano. $\square$

Corolario 18.4 *La suma directa finita de noetherianos es un módulo noetheriano.*

Demostración.

La sucesión

$$0 \to M_n \to \oplus_1^n Mi \to \oplus_1^{n-1} M_i \to 0$$

es exacta. Se deduce del teorema anterior por inducción. $\square$

Corolario 18.5 *Si A es noetheriano como A-módulo, entonces A^n es noetheriano. Si M es de generación finita es un cociente de A^n y por lo tanto es noetheriano.*

Proposición 18.6 *Si M tiene longitud finita, es noetheriano.*

Demostración.

Cada cadena se puede extender hasta una cadena irrefinable y esta es finita puesto que M es de longitud finita. Así toda cadena estaciona. $\square$

Definición 18.2 *Un anillo A se llama* noetheriano *cuando sea un módulo noetheriano con A como anillo de escalares.*

Las tres condiciones siguientes son equivalentes y definen un anillo noetheriano:

i) Cada ideal de A es de generación finita.

ii) Toda cadena ascendente de ideales estaciona.

iii) Todo conjunto no vacio de ideales posee al menos un elemento maximal.

Los anillos noetherianos son de gran importancia en álgebra y en geometría algebráica, pues incluyen a todos los anillos de polinomios en n variables sobre un cuerpo (Teorema de la base). Además los anillos noetherianos son cerrados bajo ciertas operaciones de interés.

Proposición 18.7 *Todo cociente de un anillo noetheriano es noetheriano.*

Demostración.

Sea A un anillo e I un ideal. $\pi : A \to A/I$ la proyección canónica. Mediante π^{-1} se puede suponer inyectado el conjunto de ideales de A/I en el retículo de ideales de A. □

Proposición 18.8 *Si A es noetheriano y S un conjunto multiplicativamente cerrado, A_S es noetheriano.*

Demostración.

De nuevo los ideales de A_S se pueden suponer incluidos en los ideales de A. Los ideales de A_S se identifican con los ideales de A que tienen intersección nula con S. □

El siguiente teorema es de importancia clave en geometría algebráica clásica, pues nos dice que toda subvariedad de k^n definida por un conjunto de polinomios en n variables es la intersección de un número finito de hipersuperficies definidas por los ceros de un polinomio.

Teorema 18.9 (de la base de Hilbert) *Sea A un anillo noetheriano, entonces $A[x]$ es un anillo noetheriano.*

Demostración.

Consultar la bibliografía ([**?**]).

Corolario 18.10 *Si A es noetheriano, entonces $A(x_1, \ldots, x_n)$ también.*

Demostración.

$A(x_1, \ldots, x_n) = A(x_1, \ldots, x_{n-1})(x_n)$ e inducción. □

Corolario 18.11 *Si $A \subset B$ noetheriano y B es de generación finita como álgebra sobre A, entonces B es un anillo noetheriano.*

Demostración.

B es un cociente del anillo de polinomios. □

Problemas

122 Probar la siguiente proposición:

Sea Σ un conjunto dotado de una relación de orden. Entonces son equivalentes las condiciones que siguen:

I) Cada sucesión decreciente de elementos de Σ

$$x_1 \geq x_2 \geq \cdots \geq x_n$$

es estacionaria, que quiere decir que existe un n tal que $x_n = x_{n+i}$ para todo $i > 0$.

II) Cada subconjunto no vacio de Σ admite un elemento mínimo.

Un módulo que satisfaga alguna de las condiciones procedente se llama módulo artiano. Ver que resultados del texto son generalizables a módulos artianos.

123 Veamos que el anillo $C(\mathbb{R}^n)$ no es noetheriano.

Sea B_n la bola cerrada centrada en el origen y de radio $1/n$. Tenemos una sucesión estrictamente decreciente de cerrados.

Sea

$$\mathfrak{a}_n = \{f \in C(\mathbb{R}^n) \text{ tales que } f(B_n) = 0\}$$

Probar que $\mathfrak{a}_n$ es una sucesión creciente de ideales que no estaciona.

Generalizar el resultado a espacio topólogicos más generales.

Generalizar el resultado, si es posible, a los anillos $C^\infty(\mathcal{V})$ donde $\mathcal{V}$ es una variedad diferenciable.

19. Módulos sobre anillos principales

En este capítulo clasificaremos los módulos de tipo finito sobre un dominio de ideales principales. Ello equivale a dar condiciones necesarias y suficientes para que dos módulos de tipo finito sean isomorfos. Denotaremos por $\mathcal{C}_A$ la clase de todos los módulos finito generados sobre el anillo A. En el caso en que el anillo esté claro por el contexto, simplemente lo denotaremos por $\mathcal{C}$. En este capítulo sobreentenderemos que todo módulo es de tipo finito y que el anillo es principal.

Definición 19.1 *Un* invariante *del problema de clasificación de A-módulos es un par (φ, X), donde X es un conjunto y $\varphi : \mathcal{C}_A \to X$ una función que cumple:*

Si M, M' son dos elementos de $\mathcal{C}_A$ isomorfos, entonces $\varphi(M) = \varphi(M')$.

Definición 19.2 *Sea $\{\varphi_i, X_i\}_{i\in I}$ una familia de invariantes. Decimos que esta familia es un* sistema completo de invariantes *si*

$$M \sim M' \Longleftrightarrow \varphi_i(M) = \varphi(M') \text{ para todo } i \in I$$

Recordemos algunos resultados básicos sobre anillos principales que utilizaremos en estas notas. Para la demostración de estas afirmaciones puede consultarse [**?**].

Un anillo principal A es un anillo conmutativo, con unidad, íntegro, en el que todo ideal no nulo es principal. Por lo tanto todo ideal $\mathfrak{a}$ de A es de forma $< a >$ donde a es un elemento no nulo. Decimos que el ideal $\mathfrak{a}$ está generado por el elemento a. Si a' genera el mismo ideal que a, entonces existe un elemento invertible $u \in A$ tal que $a' = ua$.

Los elementos irreducibles son aquellos que si descomponen en producto de dos factores, al menos uno de ellos es una unidad. Los elementos irreducibles

de A son precisamente aquellos que generan un ideal máximal. En un anillo principal todos los ideales primos no nulos son maximales. La noción de elemento primo y de elemento maximal coinciden.

Llamamos máximo común divisor de dos elementos $a, b \in A$ a cualquier generador del ideal suma $< a > + < b >$. Lo denotaremos por $MCD(a, b)$. Llamamos mínimo común multiplo de dos elementos $a, b \in A$ a cualquier generador del ideal intersección. Se denotará $mcm(a, b)$.

Lema 19.1 (Bezout) *Si a y b son dos elementos de un anillo principal y d es su máximo común divisor, entonces existen $\lambda, \mu \in A$ tales que*

$$d = \lambda a + \mu b$$

Teorema 19.2 *Un elemento no invertible a del anillo se expresa de modo único, salvo producto por unidades, como producto de elementos primos.*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

Por definición, todo anillo principal es noetheriano.

Por Σ denotaremos el cuerpo de fracciones de A, o lo que lo mismo, la localización de A en el ideal primo nulo.

Ejemplos.

- El anillo $\mathbb{Z}$ es un dominio de ideales principales. Para probarlo se utiliza el conocido algoritmo de la división con resto. Su cuerpo de fracciones es $\mathbb{Q}$. Como los $\mathbb{Z}$-módulos son los grupos abelianos, clasificaremos todos los grupos abelianos de tipo finito.

- Si k es un cuerpo, entonces el anillo de polinomios $k(x)$ es un anillo principal. Si recordamos que dos endomorfismos de un espacio vectorial de dimensión finita sobre un cuerpo k, inducen estructuras de $k(x)$-módulos isomorfas, veremos que como corolario de este capítulo se obtiene la clasificación de endomorfismos.

Recordemos ciertas propiedades de la torsión que utilizaremos en este capítulo.

- La suma directa de módulos de torsión es de torsión.
- Los submódulos y los cocientes de módulos de torsión son asimismo de torsión.
- Un submódulo de un módulo sin torsión no tiene torsión.
- Los módulos libres no tienen torsión (integridad de A).

Definición 19.3 *Llamamos* rango libre *de un módulo M a la dimensión del Σ-espacio M_Σ.*

El rango libre de A^n es precisamente n. Todos los módulos de tipo finito tienen rango libre finito. Los módulos de rango libre cero son precisamente los módulos de torsión (proposición 19.3).

Definición 19.4 *Sea $M' \subset M$ un submódulo. El radical de M' es el conjunto*

$$Rad(M') = \{m \in M \text{ tales que existe } a \neq 0, am \in M'\}$$

De nuevo la integridad nos garantiza que el radical es un submódulo.

Lema 19.3 *La siguiente sucesión es exacta:*

$$0 \to M_\tau \to M \to M_\Sigma$$

Demostración.

Por definición $M_\Sigma = M_0$. Por lo tanto tenemos:
$m/1 = 0 \iff$ existe $a \neq 0$ tal que $am = 0$. $\square$

Proposición 19.4 *Sea M de tipo finito. M es libre si y solo si M no tiene torsión.*

Demostración.

$\Rightarrow$) $a(m_1, \ldots, m_n) = 0 \Longrightarrow am_i = 0$ y como $a \neq 0 \Longrightarrow m_i = 0$ para todo i.

$\Leftarrow$) Procederemos por inducción sobre el rango libre.

Si M no tiene torsión y de rango libre 1 tenemos la sucesión exacta

$$0 \to M \stackrel{\varphi}{\to} \Sigma$$

Sea $(m_1, \ldots, m_k)$ una familia generadora de M. Tenemos que $\varphi(m_i) = s_i/d_i$. Consideramos el elemento de A producto de todos los denominadores:

$$a = d_1 \ldots d_k$$

Si multiplicamos cada $\varphi(m_i)$ por a eliminamos todos los denominadores y por lo tanto podemos considerar que la imagen de φ está en el anillo A. Como A es principal, resulta que M es isomorfo a un ideal.

Sea ahora M de rango libre n. Dado un $m \in M$ no nulo, tenemos que $Rad(m)$ es un submódulo de rango libre 1.

Tenemos la sucesión exacta

$$0 \to Rad(m) \to M \to M/Rad(m) \to 0$$

Ningún módulo tiene torsión y el rango de $M/Rad(m)$ es $n-1$, aplicando la exactitud de la localización. La sucesión escinde por ser el cociente un módulo proyectivo y se concluye puesto que M es la suma de dos módulos libres. $\square$

La condición de finito generado es esencial en este teorema. Por ejemplo $\mathbb{Q}$ es un grupo abeliano sin torsión y sin embargo no es libre.

Teorema 19.5 *Todo módulo de tipo finito descompone de modo único salvo isomorfismos, en suma directa de un módulo libre y de un módulo de torsión de tipo finito.*

Demostración.

La sucesión exacta

$$0 \to M_\tau \to M \to M/M_\tau \to 0$$

escinde por ser libre el cociente. La unicidad es clara.

Corolario 19.6 *Si dos módulos son isomorfos, sus rangos libres coinciden. Tenemos un invariante.*

Corolario 19.7 *Dos módulos son isomorfos si y solo si su rango es el mismo y sus módulos de torsión son isomorfos.*

Esto reduce el problema a clasificar los módulos de torsión finito generados.

De ahora en adelante supondremos que M es finito generado y de torsión.

El anulador de un elemento $m \in M$ es un ideal no nulo. El anulador de M es la intersección de una familia de generadores de M. El anulador de M es la intersección de un número finito de ideales no nulos. Al ser A integro dicho anulador no puede ser nunca nulo. Como A es principal dicho anulador esta generado por un elemento a.

Teorema 19.8 (Primer teorema de descomposición) *Sea $a = p_1^{n_1} \dots p_r^{n_r}$ la descomposición en factores primos de un generador del ideal anulador de M. M descompone, de modo único salvo isomorfismos, en suma directa*

$$M = M_1 \oplus \cdots \oplus M_r$$

donde cada M_i tiene por anulador a $p_i^{n_i}$.

Demostración.

Sea $q_1 = p_1^{n_1}, \quad q_2 = p_2^{n_2} \dots p_r^{n_r}$. Tenemos entonces que $(q_1) + (q_2) = 1$. Aplicando el lema de Bezout (lema 19.1) sabemos que existen elementos que cumplen:

$$\lambda q_1 + \mu q_2 = 1$$

Sea M_1 el submódulo de M formado por los elementos anulados por q_1.

$$M_1 = \{m \text{ tales que } q_1 m = 0\}$$

Denotamos por M' al submódulo de los elementos anulados por q_2.

El anulador de M_1 es precisamente $p_1^{n_1}$.

Tenemos que $m = q_1(\lambda m) + q_2(\mu m)$. Es claro que $q_1(\lambda m)$ pertenece a M' y que $q_2(\mu m)$ pertenece a M_1. Así concluimos que $M = M_1 + M'$. Veremos ahora que estos submódulos están en posición de suma directa.

Si $m \in M_1 \cap M'$ se cumple

$$m = \lambda(q_1 m) + \mu(q_2 m) = 0 + 0 = 0$$

Por inducción se concluye. □

La clasificación de módulos de torsión finito generados queda reducida a clasificar los módulos de torsión finito generados tales que su anulador sea una potencia de un elemento primo o irreducible.

Decimos que un módulo es primario cuando su anulador sea una potencia de un primo. Los módulos cíclicos y primarios son isomorfos a $A/\mathfrak{p}^k$ donde $\mathfrak{p}$ es un ideal primo no nulo.

El segundo teorema de descomposición afirma que todo módulo de torsión de tipo finito y primario se puede expresar como suma directa de módulos cíclicos primarios.

Para demostrar este teorema nos apoyaremos en los siguientes lemas.

Lema 19.9 *Sea M un A-módulo primario de anulador $\mathfrak{p}^k$. Entonces:*

I) *M admite una estructura de B-módulo, donde $B = A/\mathfrak{p}^k$ dada por la fórmula*

$$\pi(a)m = am$$

II) *Existe un vector m no anulado por $\mathfrak{p}^{k-1}$.*

Demostración.

i) Veamos que la definición es independiente del representante tomado Si $\pi(a) = \pi(b) \Longrightarrow a - b$ es múltiplo de $\mathfrak{p}^k$. Entonces $a - b = \lambda\mathfrak{p}^k$. Aplicamos esta igualdad a cualquier vector y obtenemos

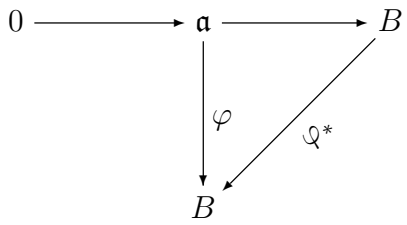
$$(a-b)m = \lambda\mathfrak{p}^k m = 0 \Longrightarrow am = bm$$

ii) Si dicho vector no existiese, todo vector de M estaría anulado por $\mathfrak{p}^{k-1}$, lo que es contradictorio. □

Lema 19.10 *B es un B-módulo inyectivo.*

Demostración.

Utilizaremos el criterio del ideal. Debemos probar que dado un morfismo φ, existe φ_* que cierra el diagrama



Los ideales de B son de la forma $\pi(\mathfrak{p}^r)$ para $r < k$. Si $\mathfrak{q} = \pi(\mathfrak{p}^r)$, entonces el anulador de $\varphi(a)$ es $\pi(\mathfrak{p}^{n-r})$ y por tanto $\varphi(\pi(\mathfrak{p}^r)) = b\pi(\mathfrak{p}^{r+h})$ donde b es un elemento de B y $h > 0$. El morfismo definido por $\varphi_*(1) = b\pi(\mathfrak{p}^h)$ cumple lo pedido. □

Teorema 19.11 (Segundo teorema de descomposición) *Sea M de tipo*
finito, de torsión y de anulador $\mathfrak{p}^k$ con $\mathfrak{p}$ primo. Entonces

$$M \sim \oplus_{i=1}^{k} (A/\mathfrak{p}^i)^{v_i}$$

Demostración.

Veamos primero la unicidad. Recordemos que si $\mathfrak{a}$ es un ideal de un anillo, entonces designamos por $\mathfrak{a}M$ al submódulo

$$\mathfrak{a}M = \{m \in M \text{ tales que existe } a \in \mathfrak{a}, m' \in M \quad am' = m\}$$

Bajo estas hipótesis se cumple:

$$\begin{aligned} l(\mathfrak{p}^{k-1}M) &= v_k \\ l(\mathfrak{p}^{k-2}M) &= 2v_k + v_{k-1} \\ \dots &= \dots \\ l(\mathfrak{p}M) &= (k-1)v_k + (k-2)v_{k-1} + \cdots + v_2 \\ l(M) &= kv_k + (k-1)v_{k-1} + \cdots + v_1 \end{aligned}$$

Así, los números v_i se pueden despejar de las longitudes de los módulos $\mathfrak{p}^i M$ y la descomposición es única.

Veamos ahora la existencia de la descomposición.

Como $\mathfrak{p}^k$ es el anulador de M, existe un vector m no anulado por $\mathfrak{p}^{k-1}$. De este modo el submódulo $< m >$ es isomorfo a $A/\mathfrak{p}^k$ y la siguiente sucesión de A-módulos es exacta

$$0 \to < m >= B \to M \to M/ < m > \to 0$$

Esta sucesión es también una sucesión exacta de B-módulos y como B es inyecto escinde

$$M \sim B \oplus M'$$

M' está de nuevo en la sutuación de M, salvo que ahora su anulador puede ser $\mathfrak{p}^r$ con $r < n$. Inductivamente se construye la descomposición y este proceso termina por ser el módulo de generación finita. $\square$

Sea ahora un módulo de torsión y finito generado. Su anulador no tiene porqué ser una potencia de un primo. Aplicando los dos teoremas de des-

composición tendremos que

$$M \sim \oplus_{i=1}^{k}(\oplus(A/\mathfrak{p}_i^{n_{ij}})^{v_{ij}}$$

Los $\mathfrak{p}_i^{n_{ij}}$ se llaman sf divisores elementales del módulo M. Tenemos el siguiente teorema de clasificación

Teorema 19.12 *Dos módulos M y M' finito generados son isomorfos si y solo si tienen el mismo rango, el mismo anulador y los números $v_{ij}(M)$ y $v_{ij}(M')$ son los mismos para todos los factores invariantes.*

Algunos de estos números pueden ser cero. Ello quiere decir que no entran en la descomposición.

Esta teoría general se aplica a los siguientes casos particulares:

- Clasificación de grupos abelianos finito generados pues como sabemos la noción de grupo abeliano y de $\mathbb{Z}$-módulo coinciden.

- Endomorfismos de un k-espacio de dimensión finita. Decimos que dos endomorfismos φ y φ' son equivalentes si son conjugados respecto a un isomorfismo

  $$\tau\varphi\tau^{-1} = \varphi'$$

  Dado un endomorfismo φ de E, introducimos en E una estructura de $k(x)$-módulo. Este $k(x)$-módulo es de torsión y finito generado puesto que $dim(k(x)) = \infty > dim(\mathrm{End}(E))$.Por lo tanto clasificar endomorfismos equivale a clasificar $k(x)$-módulos de torsión y finito generados.

- Consideremos el grupo proyectivo lineal de dimensión finita. Denotemoslo por $PGL(E)$. Dos proyectividades son equivalentes cuando sean conjugadas. Dos proyectividades $\pi(\varphi)$ y $\pi(\varphi')$ son equivalentes cuando φ sea equivalente a φ' como endomorfismos.

Ya hemos clasificado los módulos de tipo finito en base a unos invariantes llamados divisores elementales. Aquí esbozamos otra clasificación, esta vez

en base a los factores invariantes del módulo. Para las demostraciones nos remitimos a la bibliografía [**?**].

Recordemos que por $\bigwedge^j M$ denotamos la j-ésima potencia exterior del módulo M. M será de torsión.

Definición 19.5 *Llamamos factor invariante j-ésimo de M al anulador de $\bigwedge^j M$ y lo designamos por ϕ_j.*

Es claro que el anulador de $\bigwedge^{j+1} M$ contiene al anulador de $\bigwedge^j M$ y por lo tanto ϕ_{j+1} es múltiplo de ϕ_j. En definitiva, tenemos que los factores invariantes cumplen

$$\phi_1 \mid \phi_2 \mid \cdots \mid \phi_n$$

Sea $M = M_1 \oplus \cdots \oplus M_r$ la descomposición de M dada por el primer teorema de descomposición. Entonces tenemos

$$\bigwedge^j M = \bigwedge^j M_1 \oplus \cdots \oplus \bigwedge^j M_r$$

El anulador de $\bigwedge^j M$ es el producto de los anuladores de $\bigwedge^j M_i$. Utilizando el segundo teorema de descomposción se puede probar que los anuladores de los $\bigwedge_j M_i$ son los divisores elementales del módulo. Así

$$\phi = \mathfrak{p}_1^{n_{1j}} \ldots \mathfrak{p}_r^{r_{rj}}$$

Podemos dar otro teorema de clasificación

Teorema 19.13 *Si M es torsión finito generado y ϕ_j son los factores invariantes*

$$M \sim \oplus_j A/\phi_j$$

Así los factores invariantes, junto con el rango, clasifican los módulos de tipo finito sobre los anillos principales.

Problemas

124 Sea $B \subset A$ un subanillo y M un A-módulo. ¿Son iguales los módulos de torsión, calculados sobre cada uno de los anillos? ¿Existe alguna relación entre

ellos?

125 Probar que un submódulo de un módulo sin torsión tampoco tiene torsión.

Probar que los submódulos y los cocientes de un módulo de torsión son de torsión.

La suma directa de módulos de torsión es de torsión.

126 Si M está generado por n elementos, todo submódulo esta generado por $r \leq n$ elementos.

127 Probar que si M es ciclico y primario, entonces M es isomorfo a $A/\mathfrak{p}^k$ donde $\mathfrak{p}$ es un primo.

128 Sea M de torsión y finitogenerado. Para cada ideal primo $\mathfrak{p}$ del anillo sea $M(\mathfrak{p})$ el conjunto

$$M(\mathfrak{p}) = \{m \in M \text{ tales que existe } j \quad \mathfrak{p}^j m = 0\}$$

- $M(\mathfrak{p})$ es un submódulo.
- $M(\mathfrak{p})$ es no nulo si y solo si $\mathfrak{p}$ es un factor del anulador. Por lo tanto casi todos los $M(\mathfrak{p})$ son cero.
- $M \sim \oplus M(\mathfrak{p})$

129 Calcular la longitud de $A/\mathfrak{p}^k$.

Calcular la longitud de $\mathfrak{p}^r A/p^k$. $(r < k)$

130 Probar

- Si M es de tipo finito, entonces es de rango libre finito.
- El rango libre de A^n es n.
- El rango libre de una suma directa finita es la suma de los rangos libre de cada sumando.
- Rango libre cero equivale a módulo de torsión.

- Los rangos libres de los cocientes y de los submódulos de M son menores que el rango libre de M.
- El rango libre, ¿es una función aditiva?
- El rango libre de $M = M_\tau \oplus L$ es el rango libre de L.

131 Los submódulos de un módulo de tipo finito son de tipo finito.

Los submódulos de un módulo libre de tipo finito, son asimismo libres.

Para módulos de tipo finito sobre anillos principales, libre es equivalente a proyectivo.

132 En el primer teorema de descomposición, demostrar que en efecto el anulador de M_1 es $p_1^{n_1}$.

*** Problema 133** Sea M libre, con rango posiblemente infinito. Si N es un submódulo de M, entonces N es libre. La demostación puede hallarse en [**?**].

Una vez probado esa afirmación demostrar que proyectivo equivale a libre, aunque el módulo no sea finito generado.