Introducción al Análisis Algebraico sobre Extensiones de Ore

Oswaldo Lezama
Carlos Payares
Armando Reyes
César Rodríguez

Seminario de Álgebra Constructiva-SAC^2
Departamento de Matemáticas
Facultad de Ciencias
Universidad Nacional de Colombia
Sede de Bogotá

Julio 2020

Contenido

Prólogo

¿Dónde se aplican las extensiones de Ore y el álgebra homológica? Una posibilidad es en análisis algebraico: el análisis algebraico estudia sistemas lineales funcionales (SLF) de ecuaciones diferenciales ordinarias o parciales, ecuaciones en diferencias, ecuaciones diferenciales con retardo, etc., por medio de técnicas del álgebra homológica, a través de módulos de presentación finita sobre anillos no conmutativos de tipo polinomial, tales como anillos de operadores diferenciales, anillos de polinomios con retardo, anillos de polinomios torcidos iterados, extensiones de Ore, o de manera más general, dominios. Los orígenes del análisis algebraico se remontan a los trabajos de B. Malgrange ([24]), V. Palamodov ([28]), M. Sato ([37]), y más recientemente, a los trabajos de U. Oberst ([26]), M. Fliess ([9], [10]), J. Pommaret, A. Quadrat y D. Robertz ([6], [29], [30], [33], [34]) y M. Kashiwara ([14]).

Una de las principales ideas de los métodos homológicos del análisis algebraico es asociar a un SLF, $Ry = 0$, donde $R \in D^{q\times p}$ es una matriz de tamaño $q \times p$ con entradas en un anillo D, el D-módulo de presentación finita $M := D^{1\times p}/(D^{1\times q}R)$, con $D^{1\times q}R := \{\lambda R | \lambda \in D^{1\times q}\}$ el D-módulo generado por las filas de R. Las propiedades del sistema lineal se estudian entonces a través de propiedades homológicas del módulo M.

Veamos un ejemplo. Consideremos el sistema de ecuaciones de un fluido en un tanque las cuales satisfacen las ecuaciones de Saint-Venant sujetas a un movimiento unidimensional horizontal (modelo linealizado, véanse [6], [7] y [34]):

$$\begin{cases} y_1(t-2h) + y_2(t) - 2\dot{u}(t-h) = 0, \\ y_1(t) + y_2(t-2h) - 2\dot{u}(t-h) = 0. \end{cases}$$

El sistema anterior se puede interpretar algebraicamente como un sistema lineal funcional (SLF):

$$Ry = 0$$

sobre el álgebra de Ore de los operadores diferenciales con retardo con coeficientes en $\mathbb{Q}[t]$, $D_h := \mathbb{Q}[t][\partial_1; \frac{d}{dt}][\partial_2; \sigma_h]$, con

$$R := \begin{bmatrix} \partial_2^2 & 1 & -2\partial_1\partial_2 \\ 1 & \partial_2^2 & -2\partial_1\partial_2 \end{bmatrix} \in D^{2\times 3},\ y := \begin{bmatrix} y_1(t) \\ y_2(t) \\ u(t) \end{bmatrix} \in \mathcal{F}^3,$$

donde $\mathcal{F}$ es un D_h-módulo de funciones en el cual

$$\partial_1 \cdot y(t) := \dot{y}(t),\ \partial_2 \cdot y(t) := y(t-h).$$

D_h es un anillo no conmutativo de tipo polinomial en dos variables ∂_1, ∂_2 con coeficientes en el anillo habitual de polinomios $\mathbb{Q}[t]$, sujeto a las siguientes reglas:

$$\partial_1\partial_2 = \partial_2\partial_1,\ \partial_1 p(t) = p(t)\partial_1 + \dot{p}(t),\ \partial_2 p(t) = p(t-h).$$

La matriz R define un D_h-módulo izquierdo M de presentación finita:

$$D_h^{1\times 2} \xrightarrow{.R} D_h^{1\times 3} \xrightarrow{\pi} M \to 0,$$

con

$$.R(\begin{bmatrix} a & b \end{bmatrix}) := \begin{bmatrix} a & b \end{bmatrix} R \text{ y } M := \operatorname{coker}(.R) = D_h^{1\times 3}/Im(.R).$$

Aplicamos $Hom_{D_h}(\ \ ,\mathcal{F})$ y obtenemos la sucesión exacta de grupos abelianos

$$0 \to Hom_{D_h}(M,\mathcal{F}) \xrightarrow{\pi^*} \mathcal{F}^3 \xrightarrow{R.} \mathcal{F}^2,$$

es decir,

$$Hom_{D_h}(M,\mathcal{F}) \cong \ker(R.) = \{y \in \mathcal{F}^3 | Ry = 0\},$$

(isomorfismo conocido como el *teorema de Malgrange*, véase [24]). El estudio de las propiedades del sistema $Ry = 0$, tales como ser *autónomo*, *controlable*, *parametrizable*, etc. (véase [4]), pueden ser traducidas y estudiadas mediante propiedades homológicas del módulo M y el grupo abeliano $Hom_{D_h}(M,\mathcal{F})$.

Así, las propiedades estructurales de los SLF pueden ser descritas mediante métodos constructivos homológico-matriciales, y su estudio constituye uno de los objetivos centrales de la presente monografía. Para entender estos métodos, se hace necesario conocer algunas propiedades básicas de anillos, módulos y álgebra homológica. Entre estas propiedades se destacan el estudio de la condición de cadena ascendente para ideales, los módulos de presentación finita, los módulos proyectivos e inyectivos, los grupos Ext y la dimensión global. Estas propiedades han sido estudiadas en [12], [25] y [36], y también pueden ser consultadas en [16], [17], [18], [19], [20] y [21]. En esta monografía asumiremos que el lector está familiarizado con fundamentos de anillos y módulos, álgebra homológica y álgebra no conmutativa, pero le sugerimos repasar estos tópicos en las fuentes indicadas anteriormente.

Hemos dividido el contenido en cuatro capítulos: en el primero presentamos y damos suficientes ejemplos de extensiones de Ore ([27]). Además, definimos una clase de anillos estrechamente relacionada y que generaliza una gama muy amplia de extensiones de Ore, las llamadas extensiones de Poincaré-Birkhoff- Witt torcidas (véase [11], [21] y [22]). Estas últimas pueden ser fuente de inspiración para el planteamiento de problemas abiertos y aplicaciones relacionadas con los resultados que presentemos en la monografía. Los temas de este capítulo inicial pueden ser también consultados en [20], [21] y [25]. En el segundo capítulo repasaremos algunos tópicos básicos de álgebra homológica y definiremos los SLF. Haremos una introducción al estudio algebraico de las principales propiedades estructurales de los SLF en las cuales intervienen herramientas homológicas. En particular, probaremos el teorema de Malgrange. El tercer capítulo estudia la descomposición y factorización de los SLF. Veremos la relación entre propiedades homológicas de módulos y descomposiciones triangulares de SLF, y también, la relación entre matrices idempotentes y descomposiciones diagonales en bloques. En el último capítulo presentaremos los principales ingredientes de la teoría no conmutativa de las bases de Gröbner para las extensiones PBW torcidas y su aplicación para realizar algunos de los cálculos involucrados en los resultados de los capítulos 2 y 3. La teoría general no conmutativa de las bases de Gröbner que presentaremos puede ser consultada en [21] (para otros enfoques de la teoría véase también [3], [15] y [23]). En la sección final ilustraremos con ejemplos concretos sobre álgebras de Ore algunos de los resultados haciendo uso de las bases de Gröbner y de herramientas computacionales.

Todos los anillos involucrados en la presente monografía en general no son conmutativos y tienen elemento identidad; consideraremos módulos e ideales tanto a derecha como a izquierda.

Key words and phrases. Anillos y módulos, extensiones de Ore, álgebra homológica constructiva, bases de Gröbner, sistemas lineales funcionales, análisis algebraico.

2010 *Mathematics Subject Classification.* Primary: 16E05. Secondary: 16S36, 16Z05.

Capítulo 1

Extensiones de Ore

En este capítulo el propósito central es presentar y dar suficientes ejemplos de extensiones de Ore. Todos los detalles y pruebas omitidas pueden ser consultadas en [20]. Además, definiremos una clase de anillos estrechamente relacionada con las extensiones de Ore, las llamadas extensiones de Poincaré-Birkhoff- Witt torcidas (véase [11], [21] y [22]).

1.1 Anillos de polinomios torcidos

Una clase importante de anillos no conmutativos de tipo polinomial es la colección de los ***anillos de polinomios torcidos***. Presentamos a continuación una forma de construir tales anillos.

Sea A un anillo, los anillos de polinomios torcidos pueden ser vistos como anillos de polinomios sobre A en una indeterminada x con la propiedad que esta indeterminada no necesariamente conmuta con los elementos de A. Se quiere construir un anillo A' que cumpla las siguientes condiciones:

(c1) $A \hookrightarrow A'$.

(c2) Existe en A' un elemento x tal que A' es un A-módulo libre a izquierda con base $\{x^k\}_{k\geq 0}$, es decir, cada elemento de A' se debe expresar unívocamente como una suma finita $\sum_i a_i x^i$, con $a_i \in A$.

(c3) $xa \in Ax + A$, es decir, $xa = \sigma(a)x + \delta(a)$, para algunos $\sigma(a), \delta(a) \in A$, con $a \in A$.

Puesto que un anillo se debe tener $x(rs) = (xr)s$, entonces

$$\begin{aligned} x(rs) =& \sigma(rs)x + \delta(rs), \\ (xr)s =& \sigma(r)\sigma(s)x + \sigma(r)\delta(s) + \delta(r)s. \end{aligned}$$

De acuerdo con las condiciones anteriores, $\sigma : A \longrightarrow A$ es necesariamente un endomorfismo de anillos, mientras que $\delta : A \longrightarrow A$ debe ser una ***σ-derivación***; es decir, δ debe satisfacer:

$$\begin{aligned}\delta(a+b) =& \delta(a)+\delta(b),\\ \delta(ab) =& \sigma(a)\delta(b)+\delta(a)b.\end{aligned}$$

En particular, $\sigma(1) = 1$ y $\delta(1) = 0$. Así, la condiciones (c1)-(c3) inducen la existencia de un endomorfismo σ y una σ-derivación δ de tal forma que $xa = \sigma(a)x+\delta(a)$ para cada a.

Recíprocamente, dados A un anillo, σ un endomorfismo sobre A y δ una σ-derivación en A, presentaremos enseguida una forma de construir un anillo que satisfaga las condiciones (c1)-(c3).

Sea $B := End_{\mathbb{Z}}(A^{\mathbb{N}})$, donde $A^{\mathbb{N}} := \prod_{i\in\mathbb{N}} A_i$ es el producto de los grupos aditivos $A_i := A$. Así, $A \hookrightarrow B$, identificando cada elemento $a \in A$ con el homomorfismo ϕ_a, donde $\phi_a((a_i)) := (aa_i)$. Definimos:

$$\begin{aligned}x : A^{\mathbb{N}} &\longrightarrow A^{\mathbb{N}}\\ (a_i) &\longmapsto (\sigma(a_{i-1})+\delta(a_i))\end{aligned}$$

con $(a_i) := (a_0, a_1, \dots, a_i, \dots) \in A^{\mathbb{N}}$ y $a_{-1} := 0$.

Denotemos con $A[x; \sigma, \delta]$ el subanillo de B generado por x y A (una copia isomorfa de A). Ahora, si $a \in A$ lo identificamos con el elemento $\phi_a \in B$, tenemos que:

$$xa = \sigma(a)x + \delta(a),$$

de manera que cada $f \in A[x; \sigma, \delta]$ se puede expresar como $f = \sum_{i=0}^{n} a_i x^i$. Nótese además que

$$f(1,0,0,\dots) = \sum_{i=0}^{n} a_i x^i(1,0,0,\dots) = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$$

de modo que la representación de $f \in A[x; \sigma, \delta]$ es única. Así, hemos construido un anillo que satisface las propiedades requeridas. El anillo $A[x; \sigma, \delta]$ también se conoce en la literatura especializada como una ***extensión de Ore de*** A.

Recordamos a continuación algunas propiedades de los anillos de polinomios torcidos (para las pruebas véase [20]).

(i) El grado de un polinomio $f = \sum_{i=1}^{n} a_i x^i$ es definido como n si $a_n \neq 0$, y se denota por $\deg(f)$. Si $a_n \neq 0$, entonces a_n se denomina el ***coeficiente principal*** de f y escribimos $lc(f) = a_n$; $lm(f) := x^n$ es el ***monomio principal*** de f; el ***término principal*** de f, denotado por $lt(f)$, es $a_n x^n$. Ahora, si los coeficientes a_i

de f son todos nulos decimos que f es el ***polinomio nulo*** y escribimos $f = 0$. En este caso definimos $lc(0) := 0$, $lm(0) := 0$ y $lt(0) := 0$. Se tiene entonces que

$$\begin{cases} \deg(f) \geq 0, \\ \deg(f+g) \leq \text{máx}\{\deg(f), \deg(g)\}, \\ \deg(fg) \leq \deg(f) + \deg(g). \end{cases}$$

(ii) A está sumergido en $A[x; \sigma, \delta]$ mediante la aplicación $a \mapsto ax^0$.

(iii) Sea $\langle x\}$ el ideal izquierdo de $A[x; \sigma, \delta]$ generado por x. Entonces se tiene el isomorfismo de A-módulos izquierdos $A[x; \sigma, \delta]/\langle x\} \cong A$. Además, si $\delta = 0$ entonces $\langle x\}$ es un ideal bilátero de $A[x; \sigma]$ y el isomorfismo descrito es entonces un isomorfismo de anillos.

(iv) A partir de la regla de multiplicación establecida en $A[x; \sigma, \delta]$ se puede mostrar que

$$lt(ax^n bx^m) = a\sigma^n(b)x^{n+m},$$

siempre y cuando $a\sigma^n(b) \neq 0$.

(v) ***Propiedad universal***: sea B un anillo y $f : A \to B$ un homomorfismo de anillos tal que existe $y \in B$ que satisface $yf(a) = f(\sigma(a))y + f(\delta(a))$ para cada $a \in A$. Entonces, existe un único homomorfismo de anillos $\overline{f} : A[x; \sigma, \delta] \to B$ tal que $\overline{f}(x) = y$ y el siguiente diagrama es conmutativo:

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[d, "f"'] & A[x; \sigma, \delta] \arrow[dl, dotted, "\overline{f}"] \\ B & \end{tikzcd}$$

donde ι es la inclusión de A en $A[x; \sigma, \delta]$.

El anillo de polinomios torcidos se puede también definir y construir disponiendo los coeficientes de A por el lado derecho, de tal forma que la versión derecha de la propiedad universal anterior también se cumple. Cuando σ es un automorfismo se tiene la siguiente propiedad.

Proposición 1.1.1. *Sea σ un automorfismo y $A[x; \sigma, \delta]$ el anillo de polinomios torcidos por el lado izquierdo. Entonces, el anillo de polinomios torcidos por el lado derecho $A[y; \sigma^{-1}, -\delta\sigma^{-1}]_d$ es isomorfo a $A[x; \sigma, \delta]$.*

Proposición 1.1.2. *Si A es un dominio (es decir, A no tiene divisores de cero) y σ es inyetivo, entonces $A[x; \sigma, \delta]$ es un dominio.*

Corolario 1.1.3. *Bajo las condiciones de la proposición anterior tenemos que*

$$deg(fg) = deg(f) + deg(g),$$

para todo $f, g \in A - \{0\}$.

Proposición 1.1.4. *Sea* A *un anillo de división. Entonces,* $A[x;\sigma,\delta]$ *es un dominio euclidiano a izquierda. Si* σ *es un automorfismo, entonces* $A[x;\sigma,\delta]$ *es también un dominio euclidiano a derecha.*

Corolario 1.1.5. *Sea* A *un anillo de división. Entonces,* $A[x;\sigma,\delta]$ *es un dominio de ideales principales izquierdos. Si* σ *es un automorfismo, entonces* $A[x;\sigma,\delta]$ *es también un dominio de ideales principales derechos.*

Corolario 1.1.6. *Si* A *es un anillo de división, entonces* $A[x;\sigma,\delta]$ *es noetheriano a izquierda. Si* σ *es un automorfismo,* $A[x;\sigma,\delta]$ *es también noetheriano a derecha.*

Teorema 1.1.7 (Teorema de la base de Hilbert)**.** *Si* A *es noetheriano a izquierda (derecha) y* σ *es un automorfismo, entonces* $A[x;\sigma,\delta]$ *es noetheriano a izquierda (derecha).*

Veremos enseguida algunos ejemplos notables de anillos de polinomios torcidos.

Ejemplo 1.1.8. Si $\sigma = i_A$ denotamos a $A[x;\sigma,\delta]$ simplemente como $A[x;\delta]$. Este tipo de anillo se denomina ***anillo de polinomios de tipo derivación***. En este caso,

$$ax^ibx^j = a\sum_{k=0}^{i}\binom{i}{k}\delta^k(b)x^{i+j-k}.$$

Por otra parte, si $\delta = 0$, escribimos $A[x;\sigma]$, de manera que $ax^ibx^j = a\sigma^i(b)x^{i+j}$. Estos anillos se denominan ***anillos de polinomios de tipo endomorfismo***. Cuando $\delta = 0$ y $\sigma = i_A$ tenemos que $A[x;\sigma,\delta] = A[x]$ es el anillo habitual de polinomios.

Ejemplo 1.1.9. ***Polinomios con retardo***. Sea K un cuerpo, $h \in K$ y $A := K[t]$. El anillo de polinomios con retardo, también denominado anillo de ***polinomios con corrimiento***, se define por

$$S_h := K[t][x_h;\sigma_h], \text{ donde } \sigma_h(p(t)) := p(t-h).$$

Notemos que $x_ht = (t-h)x_h$ y para $p(t), q(t) \in K[t]$ se tiene:

$$p(t)x_h^iq(t)x_h^j = p(t)q(t-ih)x_h^{i+j}.$$

Ejemplo 1.1.10. ***Álgebras de Weyl***. Consideremos nuevamente que K es un cuerpo, $A := K[t]$ y $A[x;\sigma,\delta]$, con $\sigma := i_A$ y $\delta := \frac{d}{dt}$, es decir, tenemos la K-álgebra

$$A_1(K) := K[t][x; \tfrac{d}{dt}].$$

Se tiene entonces $xt = tx + 1$, $xp(t) = p(t)x + \frac{d}{dt}p(t)$, y en general,

$$p(t)x^i q(t)x^j = p(t)\sum_{k=0}^{i} \binom{i}{k} \frac{d^k}{dt}(q(t))x^{j+i-k}. \tag{1.1.1}$$

1.2 Extensiones de Ore

Podemos iterar la construcción del anillo de polinomios torcidos y obtener el ***anillo de polinomios torcidos iterado*** $A[x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n]$, con σ_i, δ_i definidas sobre el anillo $A[x_1; \sigma_1, \delta_1] \cdots [x_{i-1}; \sigma_{i-1}, \delta_{i-1}]$, es decir,

$$\sigma_i, \delta_i : A[x_1; \sigma_1, \delta_1] \cdots [x_{i-1}; \sigma_{i-1}, \delta_{i-1}] \to A[x_1; \sigma_1, \delta_1] \cdots [x_{i-1}; \sigma_{i-1}, \delta_{i-1}].$$

Existen anillos y álgebras que pueden ser descritos como un anillo de polinomios torcidos iterado pero en los cuales se cumplen algunas condiciones especiales de conmutatividad.

Definición 1.2.1. *Una **extensión de Ore** de A es un anillo de polinomios torcidos iterado $A[x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n]$ que cumple las siguientes condiciones:*

$$\sigma_i(x_j) = x_j, \ j < i, \tag{1.2.1}$$
$$\delta_i(x_j) = 0, \ j < i, \tag{1.2.2}$$
$$\sigma_i\sigma_1 = \sigma_1\sigma_i, \ 1 \leq i \leq n, \tag{1.2.3}$$
$$\delta_i\delta_1 = \delta_1\delta_i, \ 1 \leq i \leq n, \tag{1.2.4}$$

donde las dos últimas igualdades se entienden que están restringidas al anillo A.

Proposición 1.2.2. *$A[x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n]$ es una extensión de Ore de A si, y sólo si, se cumplen las siguientes condiciones:*

$$x_i x_j = x_j x_i, \ 1 \leq i, j \leq n,$$
$$\sigma_i(A), \delta_i(A) \subseteq A, \ 1 \leq i \leq n.$$

Así, σ_i y δ_i pueden ser asumidas como funciones de A en A, $\sigma_i, \delta_i : A \to A$. Notemos que un anillo de polinomios torcidos de una sola indeterminada es una extensión de Ore trivial.

(1.2.3) y (1.2.4) se cumplen no solo para $j = 1$ sino para cada $j \geq 1$, es decir, en una extensión de Ore se tienen las siguientes identidades:

$$\sigma_i\sigma_j = \sigma_j\sigma_i, \ 1 \leq i, j \leq n, \tag{1.2.5}$$
$$\delta_i\delta_j = \delta_j\delta_i, \ 1 \leq i, j \leq n, \tag{1.2.6}$$
$$\sigma_i\delta_j = \delta_j\sigma_i, \ 1 \leq i \neq j \leq n, \tag{1.2.7}$$

donde estas identidades se entienden que están restringidas al dominio de la función de índice menor (véase [20]).

Presentamos enseguida algunos ejemplos notables de extensiones de Ore.

Ejemplo 1.2.3. ***Álgebras de Ore***. Un álgebra de Ore es una extensión de Ore en la cual el anillo de coeficientes es $A := K[t_1, \dots, t_m]$, $m \geq 0$, donde K un anillo conmutativo, y además para cada $1 \leq i \leq n$, σ_i, δ_i son K-lineales. Observemos que esto es equivalente a que $\sigma_i(k) = k$, $\delta_i(k) = 0$ para cada $k \in K$; además, la extensión de Ore es en efecto una K-álgebra. Así, un álgebra de Ore es una extensión de la forma

$$K[t_1, \dots, t_m][x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n],\ m \geq 0.$$

El álgebra S_h de los polinomios con retardo es un ejemplo de álgebra de Ore con $A = K[t]$ y una sola variable x_h. Notemos que si interpretamos S_h como $K[t; i_K][x_h; \sigma_h]$, entonces S_h es un anillo de polinomios torcidos iterado sobre K pero no es una extensión de Ore de K ya que $tx_h \neq x_h t$.

Ejemplo 1.2.4. ***Álgebras de Weyl de*** n ***variables***. Si $A := K[t_1, \dots, t_n]$ y

$$A_n(K) := A[x_1; \delta_1] \cdots [x_n, \delta_n],$$

con $\delta_j := \frac{\partial}{\partial t_j}$ para $1 \leq j \leq n$, entonces $A_n(K)$ es un álgebra de Ore. Notemos que $x_i t_j = t_j x_i + \delta_{ij}$, $1 \leq i, j \leq n$, donde $\delta_{ij} = 1$ si $i = j$, y 0 en otros casos. En general tenemos que $x_i p = p x_i + \partial p / \partial t_i$, $x_i x_j - x_j x_i = 0$, con $p \in K[t_1, \dots, t_n]$ y $1 \leq i, j \leq n$. Esta álgebra también se conoce como el álgebra de ***operadores diferenciales parciales lineales***. El álgebra de Weyl $A_n(K)$ puede ser ampliada al ***álgebra de Weyl extendida*** $B_n(K) := K(t_1, \dots, t_n)[x_1; \delta_1] \cdots [x_n; \delta_n]$, con $\delta_i = \partial / \partial t_i$, para $1 \leq i \leq n$; ($K(t_1, \dots, t_n)$ es el cuerpo de fracciones de $K[t_1, \dots, t_n]$).

Ejemplo 1.2.5. ***El álgebra mixta o álgebra de operadores diferenciales con retardo***. Sean K un cuerpo y $h \in K$, entonces el álgebra mixta D_h es una álgebra de Ore definida por

$$D_h := K[t][x; \tfrac{d}{dt}][x_h; \sigma_h],$$

donde σ_h es como en el ejemplo 1.1.9.

Ejemplo 1.2.6. ***El álgebra de los sistemas lineales discretos multidimensionales***. Esta álgebra de Ore es definida por

$$D := K[t_1, \dots, t_n][x_1; \sigma_1] \cdots [x_n; \sigma_n],$$

donde K es un cuerpo y

$$\sigma_i(p(t_1, \dots, t_n)) := p(t_1, \dots, t_{i-1}, t_i + 1, t_{i+1}, \dots, t_n),\ 1 \leq i \leq n.$$

1.3 Extensiones PBW torcidas

Introducimos ahora una clase más amplia de anillos de tipo polinomial.

Definición 1.3.1. *Sean R y A dos anillos. Se dice que A es una **extensión** PBW (**Poincaré-Birkhoff-Witt**) de R si se cumplen las siguientes condiciones:*

(i) $R \subseteq A$.

(ii) *Existen en A elementos $x_1, \ldots, x_n$ tales que A es un R-módulo libre a izquierda con base el conjunto $Mon(A)$ de los **monomios estándar**,*

$$Mon(A) := \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}.$$

*En tal caso se dice que A es un **anillo de tipo polinomial** a izquierda sobre R con respecto a $\{x_1, \ldots, x_n\}$.*

(iii) *Para cada $1 \leq i \leq n$ y $r \in R$,*

$$x_i r - r x_i \in R.$$

(iv) *Para cualesquiera $1 \leq i,\, j \leq n$,*

$$x_i x_j - x_j x_i \in R + Rx_1 + \cdots + Rx_n.$$

En tal caso se denota $A := R\langle x_1, \ldots, x_n\rangle$.

Ejemplo 1.3.2. Sea R un anillo y $A := R[x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n]$ una extensión de Ore de R. Decimos que A es una ***extensión de Ore de tipo derivación*** si $\sigma_i = i_R$, para cada $1 \leq i \leq r$. Notemos que estas extensiones son PBW. En efecto, en este caso

$$x_i r - r x_i = \delta_i(r),\ x_i x_j - x_j x_i = 0.$$

En particular, cualquier álgebra de Ore de tipo derivación es una extensión PBW, por ejemplo, las álgebras de Weyl $A_n(K)$ y $B_n(K)$. Notemos también que el anillo habitual de polinomios $R[x_1, \ldots, x_n]$ es una extensión de Ore de tipo derivación. Otro ejemplo notable de extensión PBW es el álgebra envolvente de un álgebra de Lie de dimensión finita. Para su definición y construcción completa véase [20].

Generalizamos a continuación las extensiones PBW de tal forma que clases importantes de extensiones de Ore y otras álgebras queden incluidas (véase [11] y [22]). La idea de presentar estos anillos no conmutativos más generales es que sirvan de motivación para intentar extender los resultados de los próximos capítulos.

Definición 1.3.3. *Sean R y A dos anillos. Se dice que A es una* ***extensión*** PBW ***torcida de*** R *(o una extensión σ-PBW de R) si*

(i) $R \subseteq A$.

(ii) *Existen en A elementos $x_1, \ldots, x_n$ tales que A es un R-módulo libre a izquierda con base el conjunto $Mon(A)$ de los monomios estándar,*

$$Mon(A) := \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}.$$

(iii) *Para cada $1 \leq i \leq n$ y $r \in R - \{0\}$ existe $c_{i,r} \in R - \{0\}$ tal que*

$$x_i r - c_{i,r} x_i \in R. \tag{1.3.1}$$

(iv) *Para cualesquiera $1 \leq i, j \leq n$, existe $c_{i,j} \in R - \{0\}$ tal que*

$$x_j x_i - c_{i,j} x_i x_j \in R + R x_1 + \cdots + R x_n. \tag{1.3.2}$$

En este caso escribimos $A := \sigma(R)\langle x_1, \ldots, x_n\rangle$.

Proposición 1.3.4. *Sea $A = \sigma(R)\langle x_1, \ldots, x_n\rangle$ una extensión PBW torcida de un anillo R. Entonces, dado $i \in \{1, \ldots, n\}$ existe un endomorfismo inyectivo σ_i y una σ_i-derivación δ_i de R tales que para $r \in R$,*

$$x_i r = \sigma_i(r) x_i + \delta_i(r).$$

Dos clases importantes de extensiones PBW torcidas son las siguientes.

Definición 1.3.5. *Sea A una extension PBW torcida de R.*

(a) *A es* ***cuasi-conmutativa*** *si las condiciones (iii) y (iv) de la definición 1.3.3 son reemplazadas por:*

  (*iii'*) *Para cada $1 \leq i \leq n$ y $r \in R - \{0\}$ existe $c_{i,r} \in R - \{0\}$ tal que*

$$x_i r = c_{i,r} x_i. \tag{1.3.3}$$

  (*iv'*) *Para cualesquiera $1 \leq i, j \leq n$, existe $c_{i,j} \in R - \{0\}$ tal que*

$$x_j x_i = c_{i,j} x_i x_j. \tag{1.3.4}$$

(b) *A es* ***biyectiva*** *si σ_i es biyectiva para cada $1 \leq i \leq n$, y además $c_{i,j}$ es invertible para cada $1 \leq i, j \leq n$.*

Los siguientes anillos son ejemplos de extensiones PBW torcidas.

Ejemplo 1.3.6. (i) Cada extensión PBW es una extensión PBW torcida biyectiva ya que en este caso $\sigma_i = i_R$ para cada $1 \leq i \leq n$ y $c_{i,j} = 1$ para cada $1 \leq i, j \leq n$.

(ii) Cada anillo de polinomios torcidos $R[x;\sigma,\delta]$ de ***tipo inyectivo***, es decir, con σ inyectivo, es una extensión PBW torcida. En tal caso tenemos $R[x;\sigma,\delta] = \sigma(R)\langle x\rangle$. Si además $\delta = 0$, entonces la extensión $R[x;\sigma]$ es cuasi-conmutativa.

(iii) Sea $R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$ un ***anillo de polinomios torcidos iterado de tipo inyectivo***, es decir, el cual cumple las siguientes condiciones:

$$\begin{gathered}
\text{para } 1 \leq i \leq n,\ \sigma_i \text{ es inyectivo;}\\
\text{para cada } r \in R \text{ y } 1 \leq i \leq n,\ \sigma_i(r), \delta_i(r) \in R;\\
\text{para } i < j,\ \sigma_j(x_i) = cx_i + d, \text{ donde } c, d \in R \text{ y } c \text{ tiene inverso a izquierda;}\\
\text{para } i < j,\ \delta_j(x_i) \in R + Rx_1 + \cdots + Rx_i.
\end{gathered}$$

Entonces, $R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$ es una extensión PBW torcida. Bajo estas condiciones tenemos que

$$R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n] = \sigma(R)\langle x_1,\ldots,x_n\rangle.$$

En particular, cualquier ***extensión de Ore*** $R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$ ***de tipo inyectivo***, es decir, cuando σ_i es inyectivo para cada $1 \leq i \leq n$, es una extensión PBW torcida. En efecto, en las extensiones de Ore tenemos que para cada $r \in R$ y $1 \leq i \leq n$, $\sigma_i(r), \delta_i(r) \in R$, además para $i < j$, $\sigma_j(x_i) = x_i$ y $\delta_j(x_i) = 0$. Un ejemplo concreto de extensión de Ore de tipo inyectivo son las ***álgebras de Ore de tipo inyectivo***, es decir, cuando $R = K[t_1,\ldots,t_m]$, $m \geq 0$, en tal caso tenemos

$$K[t_1,\ldots,t_m][x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n] = \sigma(K[t_1,\ldots,t_m])\langle x_1,\ldots,x_n\rangle.$$

Algunos ejemplos de álgebras de Ore de tipo inyectivo son los siguientes: el álgebra S_h de polinomios con retardo, el álgebra de operadores diferenciales con retardo D_h y el álgebra D de los sistemas lineales discretos multidimensionales. Estas tres álgebras son pues extensiones PBW torcidas; S_h y D son cuasi-conmutativas y biyectivas, D_h es biyectiva.

(iv) ***Análogo aditivo del álgebra de Weyl***: sea K un cuerpo y consideremos la K-álgebra $A_n(q_1,\ldots,q_n)$ generada por $x_1,\ldots,x_n,y_1,\ldots,y_n$ y sujeta a las siguientes relaciones:

$$\begin{gathered}
x_jx_i = x_ix_j, y_jy_i = y_iy_j,\ 1 \leq i,j \leq n,\\
y_ix_j = x_jy_i,\ i \neq j,\\
y_ix_i = q_ix_iy_i + 1,\ 1 \leq i \leq n,
\end{gathered}$$

donde $q_i \in K - \{0\}$. Notemos que $A_n(q_1,\ldots,q_n)$ es isomorfa al anillos de polinomios torcidos iterados $K[x_1,\ldots,x_n][y_1;\sigma_1,\delta_1]\cdots[y_n;\sigma_n,\delta_n]$, con:

$$\begin{gathered}
\sigma_j(y_i) := y_i, \delta_j(y_i) := 0,\ 1 \leq i < j \leq n,\\
\sigma_i(x_j) := x_j, \delta_i(x_j) := 0,\ i \neq j,\\
\sigma_i(x_i) := q_ix_i, \delta_i(x_i) := 1,\ 1 \leq i \leq n.
\end{gathered}$$

Por lo tanto, $A_n(q_1,\dots,q_n)$ satisface las condiciones de (iii) y es además biyectiva; tenemos entonces que

$$A_n(q_1,\dots,q_n) = \sigma(K[x_1,\dots,x_n])\langle y_1,\dots,y_n\rangle.$$

(v) ***Análogo multiplicativo del álgebra de Weyl***: sea K un cuerpo y consideremos la K-álgebra $\mathcal{O}_n(\lambda_{ji})$ generada por los elementos $x_1,\dots,x_n$ que cumplen las siguientes relaciones:

$$x_jx_i = \lambda_{ji}x_ix_j,\ 1\leq i<j\leq n,$$

con $\lambda_{ji}\in K-\{0\}$. $\mathcal{O}_n(\lambda_{ji})$ es isomorfa al anillo $K[x_1][x_2;\sigma_2]\cdots[x_n;\sigma_n]$, con

$$\sigma_j(x_i) := \lambda_{ji}x_i,\ 1\leq i<j\leq n.$$

Así pues, $\mathcal{O}_n(\lambda_{ji})$ cumple las condiciones de (iii), y por lo tanto

$$\mathcal{O}_n(\lambda_{ji}) = \sigma(K[x_1])\langle x_2,\dots,x_n\rangle.$$

Notemos que $\mathcal{O}_n(\lambda_{ji})$ es cuasi-conmutativa y biyectiva.

(vi) ***El álgebra q-Heisenberg***: sea K un cuerpo, sea $H_n(q)$ la K-álgebra generada por $x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n$ y sujeta a las siguientes relaciones:

$$\begin{gathered}
x_jx_i = x_ix_j, z_jz_i = z_iz_j, y_jy_i = y_iy_j,\ 1\leq i,j\leq n,\\
z_jy_i = y_iz_j, z_jx_i = x_iz_j, y_jx_i = x_iy_j,\ i\neq j,\\
z_iy_i = qy_iz_i, z_ix_i = q^{-1}x_iz_i + y_i, y_ix_i = qx_iy_i,\ 1\leq i\leq n,
\end{gathered}$$

con $q\in K-\{0\}$. Notemos que $H_n(q)$ es una extensión biyectiva de K:

$$h_n(q) = \sigma(K)\langle x_1,\dots,x_n;y_1,\dots,y_n;z_1,\dots,z_n\rangle.$$

Capítulo 2

Sistemas lineales funcionales

El estudio introductorio con enfoque algebraico de los SLF que haremos en el presente capítulo se apoya en los trabajos de Pommaret, Quadrat, Chyzak, Robertz y, en general, del equipo del INRIA (Institut National de Recherche en Informatique et en Automatique) que ha desarrollado una intensa investigación en los últimos años alrededor de los métodos homológicos del análisis algebraico (véanse [2], [4], [5], [6], [29], [30], [31], [32], [33] y [34]).

En el presente capítulo, salvo que se advierta lo contrario, D denotará un anillo arbitrario. En algunas partes se asumirá que D es un dominio, es decir, un anillo sin divisores de cero, y en otras, de forma más precisa, D será un ***dominio de Ore a izquierda***, es decir, cumple la ***condición de Ore a izquierda***: dados $a \in D$ y $s \in D - \{0\}$, existen $u \in D - \{0\}$ y $b \in D$ tales que $ua = bs$. Para el anillo D, $D^{1\times r}$ es el D-módulo libre a izquierda de dimensión $r \geq 1$ conformado por los vectores fila de longitud r con componentes en D, mientras que D^r denota el D-módulo libre a derecha de vectores columnas de longitud r. El conjunto de matrices con componentes en D de tamaño $q \times p$ se denotará por $D^{q\times p}$. Supondremos siempre que D es IBN (***Invariant Basis Number***), es decir, si M es un módulo libre sobre D, todas las bases de M tienen la misma cantidad de elementos. Un D-módulo a izquierda sobre D será denotado por ${}_DM$ y por el lado derecho por M_D. La teoría general de módulos será presentada a izquierda, pero desde luego los resultados son válidos a derecha. Así, el D-módulo ${}_DM$ será denotado por M y diremos simplemente que M es un módulo. Si ${}_DD$ es noetheriano diremos que D es noetheriano, para el caso derecho indicaremos en forma explícita que D_D es noetheriano, y si D es noetheriano por ambos lados diremos que ${}_DD_D$ es noetheriano. Para la representación matricial de homomorfismos entre módulos libres a izquierda usaremos notación por filas y para módulos libres derechos usaremos notación por columnas. La notación de la composición de funciones será la usual.

2.1 Preliminares de álgebra homológica

Esta sección incluye algunas herramientas básicas de álgebra homológica necesarias para estalecer la interpretación de las propiedades más importantes de los SLF.

Definición 2.1.1. *Sea D un anillo.*

(i) *M es **reflexivo** si el D-homomorfismo canónico*

$$\begin{aligned} M &\xrightarrow{\varepsilon} Hom_D(Hom_D(M,D),D) := M^{**} \\ m &\mapsto \varepsilon(m) \end{aligned}$$

es un isomorfismo, donde $\varepsilon(m)(f) := f(m)$ para todo $f \in Hom_D(M,D)$ y cada $m \in M$.

(ii) *M es **establemente libre de rango** $t \geq 0$ si existe un entero $s \geq 0$ tal que $M \oplus D^{1\times s} \cong D^{1\times(s+t)}$.*

(iii) *Sea D un dominio de Ore a izquierda. M es **sin torsión** si el D-módulo*

$$t(M) := \{m \in M | d \cdot m = 0, \text{ para algún } d \in D - \{0\}\}$$

*es nulo. M es **de torsión** si $t(M) = M$. $t(M)$ es llamado el **submódulo de torsión** de M y sus elementos los **elementos de torsión** de M.*

Observación 2.1.2. (i) El rango de un módulo establemente libre está unívocamente determinado. En efecto, sean $t, t', s, s' \geq 0$ tales que $D^{1\times(s+t)} \cong D^{1\times s} \oplus M$ y $D^{1\times(s'+t')} \cong D^{1\times s'} \oplus M$, entonces $D^{1\times s'} \oplus D^{1\times(s+t)} \cong D^{1\times s'} \oplus D^{1\times s} \oplus M$ y $D^{1\times s} \oplus D^{1\times(s'+t')} \cong D^{1\times s} \oplus D^{1\times s'} \oplus M$, pero como D es IBN resulta $s' + s + t = s + s' + t'$, es decir, $t' = t$.

(ii) El hecho que $t(M)$ es un D-submódulo de M es una consecuencia de la condición de Ore a izquierda que tiene D. En efecto, para $m_1, m_2 \in t(M)$ y $d_1, d_2 \in D$ veamos que $d_1 \cdot m_1 + d_2 \cdot m_2 \in t(M)$: existen $p_1, p_2 \in D - \{0\}$ tales que $p_1 \cdot m_1 = 0$ y $p_2 \cdot m_2 = 0$; por la condición de Ore existen $r_1, r_2 \in D$, $s_1, s_2, t_1, t_2 \in D - \{0\}$ tales que $r_1 p_1 = s_1 d_1, r_2 p_2 = s_2 d_2$, $t_1 s_1 = t_2 s_2$, resulta entonces que $t_1 s_1 \cdot (d_1 \cdot m_1 + d_2 \cdot m_2) = t_1(s_1 d_1) \cdot m_1 + t_2(s_2 d_2) \cdot m_2 = t_1 r_1 \cdot (p_1 \cdot m_1) + t_2 r_2 \cdot (p_2 \cdot m_2) = 0$, con $t_1 s_1 \neq 0$.

Proposición 2.1.3. *Sea D un dominio y M un D-módulo f.g. de torsión. Entonces, $M^* := Hom_D(M,D) = 0$.*

Demostración. Dado $m \in M$ existe $d \neq 0$ en D tal que $d \cdot m = 0$; sea $f \in Hom_D(M,D)$, entonces $df(m) = f(d \cdot m) = f(0) = 0$, luego $f(m) = 0$ para cada m, es decir, $f = 0$. □

Veremos más adelante que si ${}_DD_D$ es noetheriano , entonces es cierto el recíproco de la proposición anterior (véase el corolario 2.3.4).

Proposición 2.1.4. *Sea D un dominio y M un D-módulo f.g., entonces*

$$\textit{libre} \Rightarrow \textit{establemente libre} \Rightarrow \textit{proyectivo} \Rightarrow \textit{reflexivo} \Rightarrow \textit{sin torsión.}$$

Demostración. Las tres primeras implicaciones son válidas para cualquier anillo D, además, las dos primeras son evidentes.

Sea M proyectivo; sabemos que $Hom_D(Hom_D(M,D),D) \cong D \otimes_D M \cong M$ (véase [35], lema 3.59; véase también [19]). Finalmente, sea M reflexivo y $m \in t(M)$, entonces existe $d \in D - \{0\}$ tal que $d \cdot m = 0$, y así $df(m) = f(d \cdot m) = f(0) = 0$ para cada $f \in Hom_D(M,D)$, luego $f(m) = 0$. Esto prueba que $\varepsilon(m)(f) = 0$ para todo $f \in Hom_D(M,D)$, por lo tanto, $\varepsilon(m) = 0$, esto es, $m \in \ker(\varepsilon) = 0$ y así $t(M) = 0$. □

Proposición 2.1.5. *Si M es proyectivo f.g., entonces M^* es proyectivo f.g.*

Demostración. Existe $r \geq 0$ y un D-módulo N tal que $D^{1\times r} \cong M \oplus N$, entonces $D^r \cong Hom_D(M \oplus N, D) \cong Hom_D(M,D) \oplus Hom_D(N,D) = M^* \oplus N^*$. □

Proposición 2.1.6. *Si $M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} M_3 \xrightarrow{\alpha_3} M_4$ es un complejo de D-módulos, entonces se tiene la sucesión exacta*

$$0 \to H(M_2) \to \operatorname{coker}(\alpha_1) \to \ker(\alpha_3) \to H(M_3) \to 0,$$

donde $H(M_i) := \ker(\alpha_i)/Im(\alpha_{i-1})$, $i = 2, 3$.

Demostración. Ejercicio para el lector. □

Definición 2.1.7. *Un D-módulo C es un* ***cogenerador*** *para la categoría ${}_DMod$ de los D-módulos a izquierda, si para cada módulo no nulo M y cada elemento $m \in M - \{0\}$ existe $f \in Hom_D(M,C)$ tal que $f(m) \neq 0$.*

Así, C es un cogenerador si, y sólo si, para cada D-módulo izquierdo M se tiene que $Hom_D(M,C) = 0$ si, y sólo si, $M = 0$.

Teorema 2.1.8. *Para cada anillo D, ${}_DMod$ tiene un cogenerador que es inyectivo.*

Demostración. Existe un D-módulo inyectivo C que contiene a $\bigoplus_I D/I$, donde I recorre todos los ideales izquierdos de D (C existe ya que todo módulo se puede sumergir en un módulo inyectivo). Sea M un módulo y sea $m \in M$ no nulo, entonces existe un ideal izquierdo I en D tal que $\langle m\} \cong D/I$. Sea ι la inclusión canónica de $\langle m\}$ en M y sea μ_I la inyección canónica de $\langle m\} \cong D/I$ en C; como C es inyectivo existe un homomorfismo $f : M \to C$ tal que $f\iota = \mu_I$, luego $f(m) \neq 0$. □

Ejemplo 2.1.9. El teorema anterior garantiza la existencia de un cogenerador inyectivo C en la categoría ${}_DMod$, con D un anillo cualquiera. Veamos por ejemplo que $\mathbb{Q}/\mathbb{Z}$ es un cogenerador inyectivo para ${}_{\mathbb{Z}}Mod$. Es claro que $\mathbb{Q}/\mathbb{Z}$ es un módulo ***divisible***, es decir, dados $0 \neq r \in \mathbb{Z}$ y $\overline{x} \in \mathbb{Q}/\mathbb{Z}$ existe $\overline{y} \in \mathbb{Q}/\mathbb{Z}$ tal que $\overline{x} = r\overline{y}$. Recordemos que la divisibilidad de un módulo C sobre un DIP (dominio de ideales principales) D implica que es C inyectivo: en efecto, veamos que para cada ideal I de D, cada homomorfismo $I \xrightarrow{f} C$ se puede extender a todo D. I es de la forma $I = Dd_0$, podemos asumir que $d_0 \neq 0$, existe $c \in C$ tal que $f(d_0) = d_0 \cdot c$; definimos $\widetilde{f} : D \to C$ por $d \mapsto d \cdot c$, notemos que $\widetilde{f}$ es un D-homomorfsimo que extiende f. Así, $\mathbb{Q}/\mathbb{Z}$ es inyectivo. Resta ahora demostrar la condición de cogenerador de $\mathbb{Q}/\mathbb{Z}$. Sea M un $\mathbb{Z}$-módulo no nulo y sea $0 \neq m \in M$; si el orden de m es infinito, definimos $f : \langle m \rangle \to \mathbb{Q}/\mathbb{Z}$ por $m \mapsto \overline{\frac{1}{2}}$, y si m es de orden finito n entonces definimos $m \mapsto \overline{\frac{1}{n}}$. En cada caso f es un $\mathbb{Z}$-homomorfismo y se puede extender a todo M ya que $\mathbb{Q}/\mathbb{Z}$ es inyectivo, además $f(m) \neq \overline{0}$.

Observación 2.1.10. Para un anillo dado D, el cálculo efectivo del módulo C es una tarea interesante y representa utilidad en los métodos homológicos del análisis algebraico ya que en la mayoría de los casos C es el módulo en donde están las soluciones de los SLF.

Ejemplo 2.1.11. Otros ejemplos no triviales de cogeneradores inyectivos son considerados en [4]: (i) Sea Ω un subconjunto convexo abierto de $\mathbb{R}^n$, entonces el espacio $F := C^{\infty}(\Omega)$ de funciones suaves sobre Ω es un cogenerador inyectivo para ${}_DMod$, con $D := A_n(K)$ y $K = \mathbb{R}$ ó $\mathbb{C}$. (ii) Sea $\mathcal{F}$ el conjunto de todas las funciones que son suaves sobre $\mathbb{R}$ excepto en un número finito de puntos; entonces $\mathcal{F}$ es un cogenerador inyectivo para la categoría ${}_DMod$, con $D := B_1(\mathbb{R})$. (iii) Sea D el álgebra de los sistemas discretos multidimensionales del ejemplo 1.2.6 con coeficientes en $K := \mathbb{R}$ ó $\mathbb{C}$; entonces un cogenerador inyectivo para su categoría de módulos es $\mathcal{F} := K^{\mathbb{N}^n}$.

Proposición 2.1.12. *Sean M, N, K, C módulos. Si C es un cogenerador inyectivo, entonces*

$$0 \to N \xrightarrow{g} M \xrightarrow{f} K \to 0$$

es exacta si, y sólo si,

$$0 \to Hom_D(K, C) \xrightarrow{f^*} Hom_D(M, C) \xrightarrow{g^*} Hom_D(N, C) \to 0, \tag{2.1.1}$$

es exacta, con $f^*(\alpha) := \alpha f$, $\alpha \in Hom_D(K, C)$, y g^* se define en forma similar.

Demostración. $\Rightarrow$) Se deduce del hecho que C es un módulo inyectivo.

$\Leftarrow$) Supongamos que (2.1.1) es exacta; probemos primero que f es sobreyectivo. Se tiene la sucesión exacta $0 \to \ker(f) \to M \xrightarrow{f} K \to \operatorname{coker}(f) \to 0$, aplicando $Hom_D(\ \ , C)$ a esta sucesión se obtiene la sucesión exacta

$$0 \to Hom_D(\text{coker}(f), C) \to Hom_D(K, C) \xrightarrow{f^*} Hom_D(M, C) \to Hom_D(\ker(f), C) \to 0,$$

con $\ker(f^*) \cong Hom_D(\text{coker}(f), C)$ y $Hom_D(\ker(f), C) \cong \text{coker}(f^*)$. Como f^* es inyectivo, $Hom_D(\text{coker}(f), C) = 0$, y puesto que C es cogenerador, entonces $\text{coker}(f) = 0$, es decir, $Im(f) = K$, luego f es sobreyectivo.

g es inyectivo: consideremos la sucesión exacta

$$0 \to \ker(g) \to N \xrightarrow{g} M \to \text{coker}(g) \to 0,$$

resulta entonces la sucesión exacta

$$0 \to Hom_D(\text{coker}(g), C) \to Hom_D(M, C) \xrightarrow{g^*} Hom_D(N, C) \to Hom_D(\ker(g), C) \to 0,$$

en particular, $\ker(g^*) \cong Hom_D(\text{coker}(g), C)$ y $Hom_D(\ker(g), C) \cong \text{coker}(g^*) = Hom_D(N, C)/Im(g^*)$. Ya que g^* es sobreyectivo, $Hom_D(\ker(g), C) = 0$, y de nuevo, ya que C es cogenerador, entonces $\ker(g) = 0$, es decir, g es inyectivo.

$\ker(f) \subseteq Im(g)$: supongamos que existe $x \in \ker(f)$ y $x \notin Im(g)$, entonces $\overline{x} \neq \overline{0}$ en $M/Im(g)$, y como C es cogenerador, existe $h \in Hom_(M/Im(g), C)$ tal que $h(\overline{x}) \neq 0$. Consideremos la sucesión exacta corta $0 \to N \xrightarrow{g} M \xrightarrow{j} \text{coker}(g) \to 0$, donde j es el homomorfismo sobreyectivo canónico; aplicando $Hom_D(\quad, C)$ obtenemos la sucesión exacta $0 \to Hom_D(\text{coker}(g), C) \xrightarrow{j^*} Hom_D(M, C) \xrightarrow{g^*} Hom_D(N, C) \to 0$, entonces $g^*j^* = 0$, de donde $(g^*j^*)(h) = 0 = g^*(hj)$, es decir, $hj \in \ker(g^*) = Im(f^*)$, luego $hj = f^*(u)$, con $u \in Hom_D(K, C)$. Resulta, $hj = uf$, de tal manera que $hj(x) = uf(x) = 0$, es decir, $h(\overline{x}) = \overline{0}$, lo cual es contradictorio.

$Im(g) \subseteq \ker(f)$: sea $x \in Im(g)$ y supongamos que $x \notin \ker(f)$, entonces $f(x) \neq 0$ y existe $h \in Hom_D(K, C)$ tal que $h(f(x)) \neq 0$, esto es, $f^*(h)(x) \neq 0$. Existe $z \in N$ tal que $x = g(z)$, así que $f^*(h)(g(z)) \neq 0$, es decir, $(g^*f^*)(h)(z) \neq 0$, pero $(g^*f^*)(h)(z) = 0^*(h)(z) = 0$, resulta así una contradicción. □

Lema 2.1.13. *Sea D un dominio noetheriano y M un D-modulo f.g. Si F es un submódulo libre maximal de M, entonces M/F es de torsión.*

Demostración. Notemos en primer lugar que el conjunto de submódulos libres de M es no vacío y puesto que M es noetheriano, entonces en dicha colección hay elemento maximal F, además, F es de bases finitas. Supongamos que $t(M/F) \neq M/F$, entonces existe $\overline{m} \neq \overline{0}$ en M/F tal que para cada $0 \neq d \in D$, $d \cdot m \notin F$. Por otro lado, F es libre f.g., sea $B := \{f_1, \ldots, f_n\}$ una base de F. Veamos que $B \cup \{m\}$ es una base de $F + Dm$: es claro que B es un sistema de generadores para $F + Dm$; sean $d_0, d_1, \ldots, d_n \in D$ tales que $d_0 \cdot m + d_1 \cdot f_1 + \cdots + d_n \cdot f_n = 0$, entonces $d_0 \cdot m \in F$, con lo cual $d_0 = 0$, y por la independencia lineal de los f_i resulta $d_i = 0$ para cada $1 \leq i \leq n$. Se tiene entonces que $F \subsetneq F + Dm \subseteq M$, lo cual es contradictorio ya que F es maximal. En consecuencia, M/F es de torsión. □

Definición 2.1.14. *Sea M un D-módulo de presentación finita,*

$$F_1 \xrightarrow{d_1} F_0 \to M \to 0.$$

El ***transpuesto*** *de M es el D-módulo derecho definido por $M^T := \mathrm{coker}(d_1^*)$, con*

$$Hom_D(F_0, D) = F_0^* \xrightarrow{d_1^*} F_1^* = Hom_D(F_1, D),\ d_1^*(\alpha) := \alpha d_1.$$

Puesto que F_0^*, F_1^* son D-módulos derechos libres de dimensión finita, entonces M^T es finitamente presentado con presentación

$$F_0^* \xrightarrow{d_1^*} F_1^* \to M^T \to 0.$$

Salvo equivalencia proyectiva, M^T es independiente de la presentación elegida para M. En efecto, se tiene la siguiente propiedad.

Lema 2.1.15. *Sea M un D-módulo con resoluciones proyectivas*

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi_0} M \to 0,$$
$$P_1' \xrightarrow{d_1'} P_0' \xrightarrow{\pi_0'} M \to 0.$$

Entonces, $\mathrm{coker}(d_1^*)$ y $\mathrm{coker}(d_1'^*)$ son proyectivamente equivalentes, es decir, existen D-módulos derechos proyectivos P, P' tales que $\mathrm{coker}(d_1^*) \oplus P \cong \mathrm{coker}(d_1'^*) \oplus P'$.

Demostración. Véase [31], Teorema 2. □

Corolario 2.1.16. *Sea M un D-módulo con presentaciones finitas*

$$F_1 \xrightarrow{d_1} F_0 \xrightarrow{\pi_0} M \to 0,$$
$$F_1' \xrightarrow{d_1'} F_0' \xrightarrow{\pi_0'} M \to 0.$$

Entonces, para cada D-módulo derecho L se tiene que

$$Ext_D^i(N, L) \cong Ext_D^i(N', L),\ i \geq 1,$$

con $N := \mathrm{coker}(d_1^*)$ y $N' := \mathrm{coker}(d_1'^*)$.

Demostración. Por el lema anterior, existen módulos derechos proyectivos P y P' tales que $N \oplus P \cong N' \oplus P'$, y para $i \geq 1$, $Ext_A^i(N \oplus P, L) \cong Ext_A^i(N' \oplus P', L)$, luego $Ext_A^i(N, L) \oplus Ext_A^i(P, L) \cong Ext_A^i(N', L) \oplus Ext_A^i(P', L)$, es decir, $Ext_A^i(N, L) \cong Ext_A^i(N', L)$. □

2.2 Sistemas lineales funcionales

Sea D un anillo arbitrario y consideremos el sistema de ecuaciones lineales

$$\sum_{j=1}^{p} R_{ij}y_j = 0, \quad ,1 \leq i \leq q, \tag{2.2.1}$$

con $R_{ij} \in D$, $p, q \geq 1$. Una solución $y := (y_1, \ldots, y_p)^T$ del sistema (en caso que exista) se asume que está en $\mathcal{F}^p$, donde $\mathcal{F}$ es un D-módulo izquierdo que se elige y se fija (véase la observación 2.1.10). El sistema (2.2.1) se puede escribir matricialmente como

$$Ry = 0, \quad R := [R_{ij}] \in D^{q\times p}. \tag{2.2.2}$$

La ***matriz*** R ***del sistema*** (2.2.1) induce el D-homomorfismo de módulos izquierdos

$$.R : D^{1\times q} \to D^{1\times p}, \quad \lambda \mapsto \lambda R, \tag{2.2.3}$$

donde $\lambda := (\lambda_1, \ldots, \lambda_q) \in D^{1\times q}$. Nótese que $Im(.R) = D^{1\times q}R$ es el D-módulo izquierdo generado por las filas de R. Asociado al sistema (2.2.1) se tiene el D-módulo izquierdo M definido por el conúcleo de $.R$, es decir,

$$M := \operatorname{coker}(.R) = D^{1\times p}/Im(.R) = D^{1\times p}/D^{1\times q}R.$$

Así, asociado al sitema lineal (2.2.1) se tiene un D-módulo finitamente presentado M con presentación

$$D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \to 0, \tag{2.2.4}$$

donde π es el homomorfismo canónico

$$\pi : D^{1\times p} \to M, \quad \beta \mapsto \beta + D^{1\times q}R.$$

M se denomina el ***D-módulo asociado al sistema*** (2.2.1). Recíprocamente, sea M un módulo finitamente presentado con presentación (2.2.4), sean $\{e_j\}_{j=1}^{p}$ la base canónica de $D^{1\times p}$ y $\{f_i\}_{i=1}^{q}$ la base canónica de $D^{1\times q}$; dado $m \in M$ existe $\lambda = (\lambda_1, \ldots, \lambda_p) \in D^{1\times p}$ tal que

$$m = \pi(\lambda) = \sum_{j=1}^{p} \lambda_j \pi(e_j) = \sum_{j=1}^{p} \lambda_j y_j, \text{ con } y_j := \pi(e_j) = e_j + D^{1\times q}R. \tag{2.2.5}$$

Notemos entonces que $\{y_j\}_{j=1}^{p}$ es un sistema de generadores de M; además,

$$f_iR = (R_{i1}, \ldots, R_{ip}) = \sum_{j=1}^{p} R_{ij}e_j \in Im(.R) = \ker(\pi),$$

luego $0 = \pi(f_i R) = \sum_{j=1}^{p} R_{ij} y_j$, es decir, el conjunto $\{y_j\}_{j=1}^{p}$ de generadores de M satisface el sistema lineal (2.2.1).

Sea nuevamente $\mathcal{F}$ un D-módulo izquierdo, aplicando $Hom_D(\quad, \mathcal{F})$ a la presentación (2.2.4) obtenemos la sucesión exacta de grupos abelianos

$$0 \to Hom_D(M, \mathcal{F}) \xrightarrow{\pi^*} Hom_D(D^{1\times p}, \mathcal{F}) \xrightarrow{(.R)^*} Hom_D(D^{1\times q}, \mathcal{F}).$$

$(.R)^*$ es un $\mathbb{Z}$-homomorfismo que podemos reemplazar por $R.$ y definido por el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathcal{F}^p & \xrightarrow{R.} & \mathcal{F}^q \\ \mu \big\downarrow & & \big\downarrow \nu \\ Hom_D(D^{1\times p}, \mathcal{F}) & \xrightarrow{(.R)^*} & Hom_D(D^{1\times q}, \mathcal{F}) \end{array}$$

donde μ, ν son D-isomorfismos definidos por $\mu((\lambda_1, \dots, \lambda_p)^T) := \alpha_\lambda$, $\alpha_\lambda(e_j) := \lambda_j$, $\nu^{-1}(h) := (h(f_1), \dots, h(f_q))^T$, $h \in Hom_D(D^{1\times q}, \mathcal{F})$, $R. := \nu^{-1}(.R)^*\mu$. Se puede verificar fácilmente que

$$R.(\lambda) = R\lambda, \text{ con } \lambda := (\lambda_1, \dots, \lambda_p)^T \in \mathcal{F}^p. \tag{2.2.6}$$

En [24] Malgrange estableció uno de los resultados más importantes del análisis algebraico, el cual constiuye el punto de partida de esta importante área del álgebra homológica aplicada. El resultado de Malgrange (teorema 2.2.1) dice que todas las $\mathcal{F}$-soluciones del sistema lineal (2.2.1) pueden ser estudiadas por medio de los D-módulos $M = D^{1\times p}/D^{1\times q}R$ y $\mathcal{F}$.

Teorema 2.2.1 (**Malgrange**, [24])**.** *Sea D un anillo arbitrario, M un D-módulo finitamente presentado con presentación (2.2.4) y $\mathcal{F}$ un D-módulo. Entonces se tiene el isomorfismo de grupos abelianos*

$$Hom_D(M, \mathcal{F}) \to \ker_{\mathcal{F}}(R.), \ \phi \mapsto \alpha := (\phi(y_1), \dots, \phi(y_p))^T, \tag{2.2.7}$$

donde $R.$ es definido por (2.2.6).

Demostración. Sea $\varphi : \ker_{\mathcal{F}}(R.) \to Hom_D(M, \mathcal{F})$ definido por $\varphi(\alpha) := \phi_\alpha$, con $\phi_\alpha(\pi(\lambda)) := \lambda\alpha$, $\alpha \in \ker_{\mathcal{F}}(R.)$, $\lambda \in D^{1\times p}$. Mostremos en primer lugar que ϕ_α está bien definido: si $\pi(\lambda) = \pi(\lambda')$, entonces $\lambda - \lambda' \in \ker(\pi) = Im(.R)$, luego existe $x \in D^{1\times q}$ tal que $\lambda - \lambda' = xR$, resulta $\phi_\alpha(\pi(\lambda)) = \lambda\alpha = \lambda'\alpha + xR\alpha = \lambda'\alpha = \phi_\alpha(\pi(\lambda'))$. Es claro que ϕ_α es un D-homomorfismo. φ es un $\mathbb{Z}$-homomorfismo; φ es inyectivo puesto que $\phi_\alpha = 0$ si, y sólo si, $\lambda\alpha = 0$ para cada $\lambda \in D^{1\times p}$, y así $\alpha_j = e_j\alpha = 0$, para cada j, es decir, $\alpha = 0$. Además, para todo $\phi \in Hom_D(M, \mathcal{F})$, $\alpha := (\phi(y_1), \dots, \phi(y_p))^T \in \mathcal{F}^p$ satisface $\varphi(\alpha) = \phi$, y para cada $1 \leq i \leq q$, $\sum_{j=1}^{p} R_{ij}\alpha_j = \sum_{j=1}^{p} R_{ij}\phi(y_j) = \phi(\sum_{j=1}^{p} R_{ij}y_j) = \phi(0) = 0$, es decir, $\alpha \in \ker_{\mathcal{F}}(R.)$.

Hemos probado que φ es un $\mathbb{Z}$-isomorfismo y $\varphi^{-1} : Hom_D(M, \mathcal{F}) \to \ker_{\mathcal{F}}(R.)$ viene dado por $\varphi^{-1}(\phi) = \alpha = (\phi(y_1), \dots, \phi(y_p))^T$. $\square$

Definición 2.2.2. *El sistema (2.2.1) se denomina* ***sistema lineal funcional*** *(**SLF**) sobre D. Un D-módulo $\mathcal{F}$ de funciones que contiene las soluciones del SLF (2.2.1) se denomina* ***espacio funcional de soluciones****.*

En los ejemplos descatados de SLF el anillo D es un álgebra de Ore y el D-módulo $\mathcal{F}$ de soluciones es habitualmente el cogenerador inyectivo de la categoría $_{D}Mod$ (observación 2.1.10). Presentamos a continuación algunos ejemplos notables de SLF sobre álgebras de Ore.

Ejemplo 2.2.3. Consideremos el sistema de ecuaciones de un fluido en un tanque las cuales satisfacen las ecuaciones de Saint-Venant sujetas a un movimiento unidimensional horizontal (modelo linealizado, véanse [6], [7] y [34]):

$$\begin{cases} y_1(t-2h) + y_2(t) - 2\dot{u}(t-h) = 0, \\ y_1(t) + y_2(t-2h) - 2\dot{u}(t-h) = 0. \end{cases} \tag{2.2.8}$$

Este es un SLF sobre el álgebra de Ore $D := \mathbb{Q}[t][\partial_1; \frac{d}{dt}][\partial_2; \sigma_h]$ de los operadores diferenciales con retardo con coeficientes en $\mathbb{Q}[t]$ (véase el ejemplo 1.3.6). El sistema anterior se puede escribir matricialmente en la forma $Ry = 0$, con

$$R := \begin{bmatrix} \partial_2^2 & 1 & -2\partial_1\partial_2 \\ 1 & \partial_2^2 & -2\partial_1\partial_2 \end{bmatrix} \in D^{2\times 3}, \ y := \begin{bmatrix} y_1(t) \\ y_2(t) \\ u(t) \end{bmatrix} \in \mathcal{F}^3,$$

donde $\mathcal{F}$ es un D-módulo de funciones tal que

$$\partial_1 \cdot y(t) := \dot{y}(t), \ \partial_2 \cdot y(t) := y(t-h).$$

Ejemplo 2.2.4 ([4])**.** Consideremos el SLF correspondiente a un modelo de túnel de viento definido por las ecuaciones

$$\begin{cases} \dot{x}_1(t) = -ax_1(t) + kax_2(t-h), \\ \dot{x}_2(t) = x_3(t), \\ \dot{x}_3(t) = -w^2x_2(t) - 2\zeta w x_3(t) + w^2u(t), \end{cases} \tag{2.2.9}$$

donde a, k, ζ, w son constantes reales. En este caso el álgebra de Ore subyacente es $D := \mathbb{R}[t][\partial; \frac{d}{dt}][\delta_h; \sigma_h]$ y el sistema se representa matricialmente por $Ry = 0$, con

$$R := \begin{bmatrix} \partial + a & -ka\delta_h & 0 & 0 \\ 0 & \partial & -1 & 0 \\ 0 & w^2 & \partial + 2\zeta w & -w^2 \end{bmatrix} \in D^{3\times 4}, \ y := \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ u(t) \end{bmatrix} \in \mathcal{F}^3, \tag{2.2.10}$$

donde $\mathcal{F}$ es un D-módulo de funciones tal que

$$\partial \cdot y(t) := \dot{y}(t), \ \delta_h \cdot y(t) := y(t-h).$$

Ejemplo 2.2.5. En [4] se presenta un ejemplo de SLF sobre el álgebra de Ore

$$D := \mathbb{Q}[t,s][\partial; \frac{d}{dt}][\delta_h; \sigma_h],$$

con matriz

$$R := \begin{bmatrix} \partial + a_0 & -(a_4\partial + a_0)\delta_h & -a_0 & 0 & -b_0\partial \\ -\delta_h(a_5\partial + a_1) & \partial + a_1 & 0 & a_1 & 0 \\ a_2 & -a_2a_4\delta_h & \partial & 0 & -a_2b_0 \\ a_3a_5\delta_h & -a_3 & 0 & \partial & 0 \end{bmatrix},$$

el cual corresponde a una línea de transmisión eléctrica, donde $a_0, a_1, a_2, a_3, a_4, a_5, b_0$ son constantes racionales. En este caso $\sigma_h(p(t,s)) := p(t, s-h)$.

Ejemplo 2.2.6 ([6])**.** El movimiento de un fluido en rotación con eje de rotación x_3 y velocidad pequeña es definido por las ecuaciones

$$\begin{cases} \rho_0 \dfrac{\partial u_1}{\partial t} - 2\rho_0\Omega_0 u_2 + \dfrac{\partial p}{\partial x_1} = 0, \\ \rho_0 \dfrac{\partial u_2}{\partial t} + 2\rho_0\Omega_0 u_1 + \dfrac{\partial p}{\partial x_2} = 0, \\ \rho_0 \dfrac{\partial u_3}{\partial t} + \dfrac{\partial p}{\partial x_3} = 0, \\ \dfrac{\partial u_1}{\partial x_1} + \dfrac{\partial u_2}{\partial x_2} + \dfrac{\partial u_3}{\partial x_3} = 0, \end{cases} \tag{2.2.11}$$

donde $u := (u_1, u_2, u_3)^T$ denota la rata local de velocidad, p la presión, ρ_0 la densidad constante del fluido y Ω_0 la velocidad angular constante. Las ecuaciones anteriores definen el sistema lineal funcional $Ry = 0$ sobre el álgebra de Ore

$$D := \mathbb{Q}[t, x_1, x_2, x_3][\partial_t; \frac{\partial}{\partial t}][\partial_1; \frac{\partial}{\partial x_1}][\partial_2; \frac{\partial}{\partial x_2}][\partial_3; \frac{\partial}{\partial x_3}]$$

con

$$R := \begin{bmatrix} \rho_0\partial_t & -2\rho_0\Omega_0 & 0 & \partial_1 \\ 2\rho_0\Omega_0 & \rho_0\partial_t & 0 & \partial_2 \\ 0 & 0 & \rho_0\partial_t & \partial_3 \\ \partial_1 & \partial_2 & \partial_3 & 0 \end{bmatrix}, y := \begin{bmatrix} u_1(t, x_1, x_2, x_3) \\ u_2(t, x_1, x_2, x_3) \\ u_3(t, x_1, x_2, x_3) \\ p(t, x_1, x_2, x_3) \end{bmatrix} \in \mathcal{F}^4,$$

donde $\mathcal{F}$ es un D-módulo de funciones tal que

$$\partial_t \cdot y := \frac{\partial y}{\partial t},\ \partial_i \cdot y := \frac{\partial y}{\partial x_i},\ i = 1, 2, 3.$$

Regresemos nuevamente a la teoría general. Sea D noetheriano y M un D-módulo f.g., entonces M tiene una resolución libre en la forma

$$\cdots \xrightarrow{.R_4} D^{1\times r_3} \xrightarrow{.R_3} D^{1\times r_2} \xrightarrow{.R_2} D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \to 0;$$

sea $\mathcal{F}$ un D-módulo arbitrario, aplicando $Hom_D(\ \ ,\mathcal{F})$ a

$$D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \to 0,$$

y también al complejo obtenido al eliminar M de la resolución libre anterior, resulta

$$Hom_D(M,\mathcal{F}) \cong Im(\pi^*) = \ker_{\mathcal{F}}(R_1.)$$

y el complejo de grupos abelianos

$$0 \to \mathcal{F}^{r_0} \xrightarrow{R_1.} \mathcal{F}^{r_1} \xrightarrow{R_2.} \mathcal{F}^{r_2} \xrightarrow{R_3.} \mathcal{F}^{r_3} \xrightarrow{R_4.} \cdots .$$

Los grupos de cohomología del complejo anterior son dados por

$$\begin{cases} Ext^0_D(M,\mathcal{F}) := Hom_D(M,\mathcal{F}) \\ Ext^i_D(M,\mathcal{F}) := \ker_{\mathcal{F}}(R_{i+1}.)/Im_{\mathcal{F}}(R_i.),\ i\geq 1. \end{cases} \tag{2.2.12}$$

Por lo tanto, el grupo abeliano de todas las $\mathcal{F}$-soluciones del sistema $R_1\alpha = 0$ es definido por $Ext^0_D(M,F) = Hom_D(M,\mathcal{F})$, mientras que $Ext^1_D(M,\mathcal{F})$ está relacionado con la solubilidad del sistema no homogéneo $R_1\alpha = \beta$. En efecto, si el sistema lineal $R_1y = \beta$ es soluble, para un $\beta \in \mathcal{F}^{r_1}$ fijo, entonces existe $\varepsilon \in \mathcal{F}^{r_0}$ tal que $R_1\varepsilon = \beta$, luego $\beta \in Im_{\mathcal{F}}(R_1.)$, y de aquí se obtiene la condición necesaria $R_2\beta = 0$ ya que $R_2R_1 = 0$. Recíprocamente, sea $\beta \in \mathcal{F}^{r_1}$ tal que $R_2\beta = 0$, consideremos la clase residual de β en $Ext^1_D(M,\mathcal{F}) = \ker_{\mathcal{F}}(R_2.)/Im(R_1.)$; si esta clase es nula entonces $\beta \in Im(R_1.)$, luego existe $\varepsilon \in \mathcal{F}^{r_0}$ tal que $R_1\varepsilon = \beta$. Notemos además que la solución del sistema no homogéneo no es única ya que si $\varepsilon' \in \ker_{\mathcal{F}}(R_1.)$, entonces $\varepsilon + \varepsilon'$ es también solución. Finalmente, observemos que si $\ker_{\mathcal{F}}(R_2.) = Im(R_1.)$, entonces una condición necesaria y suficiente para la solubilidad del sistema $R_1y = \beta$ es que $R_2\beta = 0$ (véase también [26]).

2.3 Diccionario entre las propiedades estructurales de los SLF y el álgebra homológica

Consideremos el SLF, $Ry = 0$, con R una matriz de tamaño $q\times p$ con entradas en D, de tal forma que sus soluciones se encuentran en un D-módulo $\mathcal{F}$, cogenerador inyectivo. $\mathcal{F}$ juega un papel similar al de las variedades algebraicas de la geometría algebraica, y corresponde al espacio de soluciones, de tal forma que se tiene una cierta dualidad entre análisis funcional y álgebra homológica. En lo que sigue se desarrollará un diccionario entre las propiedades estructurales del sistema lineal $Ry = 0$ y las propiedades homológicas del D-módulo asociado $M := D^{1\times p}/D^{1\times q}R$.

Definición 2.3.1. *Si D es un dominio noetheriano, $R \in D^{q\times p}$, $M := D^{1\times p}/D^{1\times q}R$ y $\mathcal{F}$ es un D-módulo cogenerador inyectivo, entonces*

(i) $\mathcal{B} := \ker_{\mathcal{F}}(R.) = \{\alpha \in \mathcal{F}^p | R\alpha = 0\}$ *se denomina el* ***$\mathcal{F}$-comportamiento*** *o conjunto de* ***$\mathcal{F}$-soluciones*** *del sistema $Ry = 0$.*

(ii) *Un* ***observable*** *del sistema $Ry = 0$ es una función $\psi : \mathcal{B} \to \mathcal{F}$ tal que existen $d_1, \ldots, d_p \in D$ de tal manera que $\psi(\alpha) := d_1\alpha_1 + \cdots + d_p\alpha_p$, para cada $\alpha := (\alpha_1, \ldots, \alpha_p)^T \in \mathcal{B}$.*

(iii) *Un observable ψ es* ***autónomo*** *si existe $d \in D - \{0\}$ tal que $d \cdot \psi(\alpha) = 0$, para cada $\alpha \in \mathcal{B}$. ψ es* ***libre*** *si no es autónomo.*

(iv) *$Ry = 0$ es* ***autónomo*** *si todo observable es autónomo.*

(v) *$Ry = 0$ es* ***controlable*** *si todo observable es libre.*

(vi) *$Ry = 0$ es* ***parametrizable*** *si existe una matriz $Q \in D^{p\times m}$ tal que $\mathcal{B} = Q\mathcal{F}^m$. La matriz Q es llamada una* ***parametrización*** *de $Ry = 0$.*

(vii) *$Ry = 0$ es* ***plano*** *si admite una* ***parametrización inyectiva****, es decir, la matriz de parametrización $Q \in D^{p\times m}$ admite inversa a izquierda $T \in D^{m\times p}$, $TQ = I_m$.*

(viii) *Sea z un elemento no nulo del centro de D y sea $Ry = 0$ un sistema parametrizable con parametrización $Q \in D^{p\times m}$. $Ry = 0$ es* ***z-libre*** *si existen $T \in D^{m\times p}$ y $k \geq 0$ tales que $TQ = z^k I_m$, donde I_m es la matriz idéntica de orden m.*

(ix) *$Ry = 0$ es* ***sin torsión*** *(respectivamente,* ***reflexivo, proyectivo, establemente libre, libre****) si M es sin torsión (respectivamente, reflexivo, proyectivo, establemente libre, libre).*

Teorema 2.3.2. *Sea D un dominio noetheriano. Si $Ry = 0$ es un SLF, con $R \in D^{q\times p}$ y $M := D^{1\times p}/D^{1\times q}R$, y si $\mathcal{F}$ es un D-módulo cogenerador inyectivo y $\mathcal{B}$ es el conjunto de $\mathcal{F}$-soluciones, entonces*

(i) *Los observables están en correspondencia biyectiva con los elementos de M.*

(ii) *Los observables autónomos están en correspondencia biyectiva con los elementos de torsión de M.*

(iii) *$Ry = 0$ es autónomo si, y sólo si, M es de torsión.*

(iv) *$Ry = 0$ es controlable si, y sólo si, M es sin torsión.*

(v) *$Ry = 0$ es parametrizable si, y sólo si, existe $Q \in D^{p\times m}$ tal que $M \cong D^{1\times p}Q$.*

(vi) $Ry = 0$ *es plano si, y sólo si, M es libre.*

(vii) *Sea z un elemento no nulo del centro de D y sea $Ry = 0$ un sistema parametrizable con parametrización $Q \in D^{p\times m}$. $Ry = 0$ es z-libre si, y sólo si, $D_z \otimes_D M$ es libre sobre el anillo $D_z = \{\frac{b}{a} | b \in D, a = z^n, n \geq 0\}$.*

Demostración. (i) Sean $f \in Hom_D(D, M)$ y $m := f(1)$, aplicamos $Hom_D(\ \ , \mathcal{F})$ a $D \xrightarrow{f} M$ y obtenemos el $\mathbb{Z}$-homomorfismo $Hom_D(M, \mathcal{F}) \xrightarrow{f^*} Hom_D(D, \mathcal{F})$, $f^*(\phi) := \phi f$, el cual es equivalente al $\mathbb{Z}$-homomorfismo $\ker_{\mathcal{F}}(R.) \xrightarrow{\psi} \mathcal{F}$ inducido por los isomorfismos $Hom_D(M, \mathcal{F}) \cong \ker_{\mathcal{F}}(R.)$ (teorema 2.2.1) y $Hom_D(D, \mathcal{F}) \cong \mathcal{F}$. Puesto que $M = \langle y_1, \ldots, y_p \}$, con $y_i := \pi(e_i)$, $1 \leq i \leq p$ (véase (2.2.5)), entonces existen $d_1, \ldots, d_p \in D$ tales que $m = \sum_{i=1}^p d_i \cdot y_i$, de donde $(\phi f)(1) = \phi(m) = \sum_{i=1}^p d_i \cdot \phi(y_i) = \sum_{i=1}^p d_i \cdot \alpha_i$, con $\alpha_i := \phi(y_i)$. Por lo tanto, $\ker_{\mathcal{F}}(R.) \xrightarrow{\psi} \mathcal{F}$ definida por $\psi(\alpha) := \sum_{i=1}^p d_i \cdot \alpha_i$ (véase (2.2.7)) es un observable. Veamos ahora que ψ solo depende de m y no de los escalares d_i: sea $m = \sum_{i=1}^p b_i \cdot y_i$, $b_i \in D$, entonces $\nu := (d_1 - b_1, \ldots, d_p - b_p) \in Im(.R) = \ker(.R)$ ya que $\pi(\nu) = \pi((\sum_{i=1}^p (d_i - b_i) \cdot e_i) = \sum_{i=1}^p (d_i - b_i) \cdot y_i = m - m = 0$. Por lo tanto, existe $\lambda \in D^{1\times q}$ tal que $\nu = \lambda R$ de modo que $\sum_{i=1}^p d_i \cdot \alpha_i - \sum_{i=1}^p b_i \cdot \alpha_i = \nu\alpha = (\lambda R)\alpha = \lambda(R\alpha) = 0$. Así, teniendo en cuenta el isomorfismo $Hom_D(D, M) \cong M$ dado por $f \mapsto m := f(1)$, podemos concluir que dado $m \in M$ hemos asignado un único observable ψ.

Recíprocamente, consideremos el observable $\psi : \mathcal{B} \to \mathcal{F}$ definido por $\psi(\alpha) = \sum_{i=1}^p d_i \cdot \alpha_i$ con $\alpha \in \mathcal{B}$ y $d_i \in D$; asociamos entonces a este observable el elemento $m := \sum_{i=1}^p d_i \cdot y_i \in M$. Veamos que esta asignación está bien definida: consideremos dos presentaciones del observable ψ, es decir, $\sum_{i=1}^p d_i \cdot \alpha_i = \sum_{i=1}^p b_i \cdot \alpha_i$, para cada $\alpha \in \mathcal{B}$. Definimos

$$\mathcal{B}^\natural := \{\lambda \in D^{1\times p} | \lambda\alpha = 0 \text{ para cada } \alpha \in \mathcal{B}\}.$$

$\mathcal{B}^\natural \neq \emptyset$ ya que $\nu := (d_1 - b_1, \ldots, d_p - b_p) \in \mathcal{B}^\natural$; si $\lambda \in D^{1\times q}R$, existe $\theta \in D^{1\times q}$ tal que $\lambda = \theta R$, luego $\lambda\alpha = \theta(R\alpha) = 0$ para cada $\alpha \in \mathcal{B}$, por lo tanto, $D^{1\times q}R \subseteq \mathcal{B}^\natural$. Como $D^{1\times p}$ es noetheriano, entonces $\mathcal{B}^\natural$ es un D-módulo f.g., y en consecuencia, existe $R' \in D^{q'\times p}$ tal que $\mathcal{B}^\natural = D^{1\times q'}R'$. Definimos $M' := D^{1\times p}/D^{1\times q'}R'$; según el teorema 2.2.1, $\ker_{\mathcal{F}}(R'.) \cong Hom_D(M', \mathcal{F})$, y puesto que $D^{1\times q}R \subseteq \mathcal{B}^\natural = D^{1\times q'}R'$, se tiene que $\ker_{\mathcal{F}}(R.) \subseteq \ker_{\mathcal{F}}(R'.)$. Aplicamos ahora $Hom_D(\ \ , \mathcal{F})$ a la sucesión exacta

$$0 \to \mathcal{B}^\natural/D^{1\times q}R \to M \to M' \to 0,$$

y puesto que $\mathcal{F}$ es D-inyectivo, resulta el diagrama exacto

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Hom_D(M', \mathcal{F}) & \longrightarrow & Hom_D(M, \mathcal{F}) & \longrightarrow & Hom_D(\mathcal{B}^\natural/D^{1\times q}R, \mathcal{F}) & \longrightarrow & 0 \\
 & & \downarrow \cong & & \downarrow \cong & & \downarrow = & & \\
0 & \longrightarrow & \ker_{\mathcal{F}}(R'.) & \longrightarrow & \ker_{\mathcal{F}}(R.) & \longrightarrow & Hom_D(\mathcal{B}^\natural/D^{1\times q}R, \mathcal{F}) & \longrightarrow & 0
\end{array}$$

en particular, $\ker_{\mathcal{F}}(R'.) \subseteq \ker_{\mathcal{F}}(R.)$, por lo tanto, $\ker_{\mathcal{F}}(R.) = \ker_{\mathcal{F}}(R'.)$, de donde $Hom_D(\mathcal{B}^{\natural}/D^{1\times q}R, \mathcal{F}) = 0$, pero como $\mathcal{F}$ es cogenerador, entonces $\mathcal{B}^{\natural}/D^{1\times q}R = 0$, esto es, $\mathcal{B}^{\natural} = D^{1\times q}R$, luego $\nu \in D^{1\times q}R$ y $\pi(\nu) = 0$, es decir, $m = \sum_{i=1}^{p} d_i \cdot y_i = \sum_{i=1}^{p} b_i \cdot y_i$.

Es claro que las compuestas de las dos asignaciones anteriores dan las idénticas.

(ii) Consecuencia directa de (i).

(iii) y (iv) se obtienen de (ii) ya que D es un dominio Ore a izquierda ([19]).

(v) $Ry = 0$ es parametrizable si, y sólo si, existe una matriz $Q \in D^{p\times m}$ tal que $\mathcal{B} = Q\mathcal{F}^m = Im(Q.)$, esto es, si, y sólo si, la sucesión $\mathcal{F}^m \xrightarrow{Q.} \mathcal{F}^p \xrightarrow{R.} \mathcal{F}^q$ es exacta, pero por la demostración de la proposición 2.1.12, esta sucesión es exacta si, y solo si, $D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.Q} D^{1\times m}$ es exacta, es decir, si, y sólo si, $D^{1\times p}/\ker(.Q) \cong Im(.Q)$; pero $\ker(.Q) = Im(.R) = D^{1\times q}R$ e $Im(.Q) = D^{1\times p}Q$, luego, $Ry = 0$ es parametrizable si, y sólo si, $M = D^{1\times p}/D^{1\times q}R \cong D^{1\times p}Q$.

(vi) $Ry = 0$ es plano si, y sólo si, existen matrices $Q \in D^{p\times m}$ y $T \in D^{m\times p}$ tales que $\mathcal{B} = Q\mathcal{F}^m$ y $TQ = I_m$, si, y sólo si, la sucesión

$$0 \to \mathcal{F}^m \xrightarrow{Q.} \mathcal{F}^p \xrightarrow{R.} R\mathcal{F}^p \to 0$$

es exacta y hendida, es decir, si, y sólo si, la sucesión

$$0 \to D^{1\times q}R \to D^{1\times p} \xrightarrow{.Q} D^{1\times m} \to 0$$

es exacta y hendida, si, y sólo si, $D^{1\times p}/\ker(.Q) \cong D^{1\times p}Q = D^{1\times m}$, si, y sólo si, $M \cong D^{1\times m}$, si, y sólo si, M es libre.

(vii) Sea $Ry = 0$ parametrizable y z-libre, existen matrices $Q \in D^{p\times m}, T \in D^{m\times p}$ tales que $M \cong D^{1\times p}Q$ y $TQ = z^k I_m$, con $k \geq 0$. Sabemos que D_z es D-plano, luego $D_z \otimes_D M \cong D_z \otimes_D Im(.Q) \cong Im((.Q)_z) = D_z^{1\times p}Q_z = D_z^{1\times p}Q \subseteq D_z^{1\times m}$. Además, $(\frac{1}{z^k})T$ es la inversa a izquierda de Q sobre el anillo D_z, y como $D_z^{1\times m}(\frac{1}{z^k})T \subseteq D_z^{1\times p}$, entonces $D_z^{1\times m}(\frac{1}{z^k})TQ \subseteq D_z^{1\times p}Q$, es decir, $D_z^{1\times m} \subseteq D_z^{1\times p}Q$. Resulta entonces que $D_z \otimes_D M \cong D_z^{1\times m}$.

Recíprocamente, supongamos que $D_z \otimes_D M \cong D_z^{1\times n}$ para algún $n \geq 1$; como $Ry = 0$ es parametrizable, según (v) existe $Q \in D^{p\times m}$ tal que $M \cong D^{1\times p}Q$; tenemos entonces que $D_z \otimes_D M \cong D_z \otimes_D D^{1\times p}Q \cong D_z^{1\times p}Q_z = D_z^{1\times p}Q$, luego $D_z^{1\times n} \cong D_z^{1\times p}Q$, y en consecuencia, existe $S \in D_z^{n\times p}$ tal que $SQ = I_n$, pero como Q es de tamaño $p \times m$, entonces necesariamente $n = m$. Tomando un denominador común para S encontramos $k \geq 0$ tal que $TQ = z^k I_m$, con $T := z^k S \in D^{m\times p}$. □

El teorema anterior demuestra como algunas propiedades de los sistemas lineales funcionales son traducidas en propiedades de módulos. Mostraremos enseguida que estas propiedades a su vez pueden ser estudiadas calculando ciertas extensiones de módulos de la forma $Ext_D^i(M^T, D)$, $i \geq 1$. Según el corolario 2.1.16, $Ext_D^i(M^T, D)$ es independiente de la presentación finita de M. En el siguiente teorema, $\mathrm{rgld}(D)$ denota la dimensión global a derecha del anillo D (véase [36] o también [19]).

Teorema 2.3.3. *Sea D un dominio con ${}_DD_D$ noetheriano. Si M es un D-módulo de presentación finita y $N := M^T$, entonces*

(i) $t(M) \cong Ext_D^1(N, D)$.

(ii) *M es sin torsión si, y sólo si, $Ext_D^1(N, D) = 0$.*

(iii) *Se tiene la siguiente sucesión exacta de D-módulos*

$$0 \to Ext_D^1(N, D) \to M \xrightarrow{\varepsilon} M^{**} \to Ext_D^2(N, D) \to 0,$$

donde ε es como en la definición 2.1.1.

(iv) *M es reflexivo si, y sólo si, $Ext_D^i(N, D) = 0$ para $i = 1, 2$.*

(v) *Sea $\mathrm{rgld}(D) < \infty$. M es proyectivo si, y sólo si, $Ext_D^i(N, D) = 0$ para cada $1 \leq i \leq \mathrm{rgld}(D)$.*

Demostración. Sea

$$F_1 \xrightarrow{d_1} F_0 \xrightarrow{\pi} M \to 0. \tag{2.3.1}$$

una presentación finita de M y sea

$$F_0^* \xrightarrow{d_1^*} F_1^* \xrightarrow{\rho} N \to 0. \tag{2.3.2}$$

la correspondiente presentación finita de N (véase la definición 2.1.14). Notemos que además se tiene la sucesión exacta

$$0 \to M^* \to F_0^* \xrightarrow{d_1^*} F_1^* \xrightarrow{\rho} N \to 0, \tag{2.3.3}$$

(i) Sea X un $D-D$-bimódulo; aplicamos $X \otimes_D -$ a la sucesión (2.3.1) y obtenemos la sucesión exacta de D-módulos izquierdos

$$X \otimes_D F_1 \xrightarrow{i_X \otimes d_1} X \otimes_D F_0 \xrightarrow{i_X \otimes \pi} X \otimes_D M \to 0. \tag{2.3.4}$$

De manera similar, aplicando $Hom_D(\ \ , X)$ a (2.3.2) se obtiene la sucesión exacta de D-módulos izquierdos

$$0 \to Hom_D(N, X) \to Hom_D(F_1^*, X) \to Hom_D(F_0^*, X); \tag{2.3.5}$$

pero $Hom_D(F_i^*, X) = Hom_D(Hom_D(F_1, D), X) \cong Hom_D(D, X) \otimes_D F_i \cong X \otimes_D F_i$, $i = 0, 1$ (véase [35], lema 3.59; véase también [19]). Por lo tanto, de (2.3.4) y (2.3.5) resulta la sucesión exacta de D-módulos izquierdos

$$0 \to Hom_D(N, X) \to X \otimes_D F_1 \to X \otimes_D F_0 \to X \otimes_D M \to 0. \tag{2.3.6}$$

De otra parte, como ${}_DD_D$ es un dominio noetheriano, entonces D es un dominio de Ore a izquierda y derecha (véase [19]), luego posee anillo de división a izquierda y derecha $K := Q(D)$ y K es un $D-D$-bimódulo; consideremos la siguiente sucesión exacta de $D-D$-bimódulos

$$0 \to D \xrightarrow{\iota} K \to K/D \to 0, \tag{2.3.7}$$

se obtiene la sucesión exacta larga de D-módulos izquierdos

$$\begin{aligned} &0 \to Hom_D(N, D) \to Hom_D(N, K) \to Hom_D(N, K/D) \to \\ &Ext_D^1(N, D) \to Ext_D^1(N, K) \to Ext_D^1(N, K/D) \to \cdots \end{aligned}$$

pero como K es un D-módulo derecho inyectivo (véase [19]), entonces resulta la sucesión exacta de D-módulos izquierdos

$$0 \to Hom_D(N, D) \to Hom_D(N, K) \to Hom_D(N, K/D) \to Ext_D^1(N, D) \to 0. \tag{2.3.8}$$

Aplicando $- \otimes_D M$ a (2.3.7) obtenemos la sucesión exacta de D-módulos izquierdos

$$D \otimes_D M \xrightarrow{\iota\otimes i_M} K \otimes_D M \to (K/D) \otimes_D M \to 0,$$

y puesto que $\ker(\iota \otimes i_M) = t(M)$, se tiene entonces se tiene la siguiente sucesión exacta de D-módulos izquierdos

$$0 \to t(M) \to M \xrightarrow{\iota\otimes i_M} K \otimes_D M \to (K/D) \otimes_D M \to 0. \tag{2.3.9}$$

Teniendo en cuenta que cada F_i es un D-módulo izquierdo plano, se obtiene de (2.3.7) la sucesión exacta de D-módulos izquierdos

$$0 \to F_i \to K \otimes_D F_i \to (K/D) \otimes_D F_i \to 0, \; i = 0, 1. \tag{2.3.10}$$

Tomando en (2.3.6), $X = D, K, K/D$ y usando (2.3.8), (2.3.9) y (2.3.10), resulta el siguiente diagrama conmutativo exacto de D-módulos izquierdos

$$\begin{tikzcd}
 & & & & 0 \arrow[d] & \\
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & t(M) \arrow[d, "\alpha_1"] & \\
0 \arrow[r] & Hom_D(N,D) \arrow[r, "\beta_3"] \arrow[d, "\alpha_8"'] & F_1 \arrow[r, "\beta_2"] \arrow[d, "\alpha_6"'] & F_0 \arrow[r, "\beta_1"] \arrow[d, "\alpha_4"'] & M \arrow[r] \arrow[d, "\alpha_2"] & 0 \\
0 \arrow[r] & Hom_D(N,K) \arrow[r, "\beta_6"] \arrow[d, "\alpha_9"] & K \otimes_D F_1 \arrow[r, "\beta_5"] \arrow[d, "\alpha_7"] & K \otimes_D F_0 \arrow[r, "\beta_4"] \arrow[d, "\alpha_5"] & K \otimes_D M \arrow[r] \arrow[d, "\alpha_3"] & 0 \\
0 \arrow[r] & Hom_D(N,K/D) \arrow[r, "\beta_9"] \arrow[d, "\alpha_{10}"] & (K/D) \otimes_D F_1 \arrow[r, "\beta_8"] \arrow[d] & (K/D) \otimes_D F_0 \arrow[r, "\beta_7"] \arrow[d] & (K/D) \otimes_D M \arrow[r] \arrow[d] & 0 \\
 & Ext_D^1(N,D) \arrow[d] & 0 & 0 & 0 & \\
 & 0 & & & &
\end{tikzcd}$$

el cual induce una aplicación $\varphi : t(M) \to Ext^1_D(N,D)$ definida de la siguiente manera: sea $x \in t(M)$, entonces $\alpha_1(x) \in M$, luego existe $x_0 \in F_0$ tal que $\alpha_1(x) = \beta_1(x_0)$. Notemos que $\alpha_4(x_0) \in \ker(\beta_4) = Im(\beta_5)$, por lo tanto existe $z \in K \otimes_D F_1$ tal que $\beta_5(z) = \alpha_4(x_0)$. Además, $\alpha_7(z) \in \ker(\beta_8) = Im(\beta_9)$, en consecuencia, existe un único $y \in Hom_D(N, K/D)$ tal que $\alpha_7(z) = \beta_9(y)$. Puesto que $\alpha_{10}(y) \in Ext^1_D(N,D)$, entonces definimos $\varphi(x) := \alpha_{10}(y)$. Se puede demostrar que φ está bien definida y que es un D-isomorfismo. La prueba completa de esta afirmación la dejamos al lector, veamos por ejemplo que φ es sobreyectivo: sea $u \in Ext^1_D(N,D)$, entonces existe $y \in Hom_D(N, K/D)$ tal que $u = \alpha_{10}(y)$; $\beta_9(y) \in (K/D) \otimes_D F_1$, luego existe $z \in K \otimes_D F_1$ tal que $\alpha_7(z) = \beta_9(y)$ y entonces $\beta_8(\alpha_7(z)) = \beta_8(\beta_9(y)) = 0$, es decir, $\alpha_7(z) \in \ker(\beta_8)$; $\alpha_5(\beta_5(z)) = \beta_8(\alpha_7(z)) = 0$, lo cual indica que $\beta_5(z) \in \ker(\alpha_5) = Im(\alpha_4)$, por lo tanto, existe $x_0 \in F_0$ tal que $\beta_5(z) = \alpha_4(x_0)$; se tiene $\alpha_2(\beta_1(x_0)) = \beta_4(\alpha_4(x_0)) = \beta_4(\beta_5(z)) = 0$, luego $\beta_1(x_0) \in \ker(\alpha_2) = Im(\alpha_1)$, de donde $\beta_1(x_0) = \alpha_1(x)$, con $x \in t(M)$. Por lo tanto, $\phi(x) = u$.

(ii) es consecuencia directa de (i).

(iii) En la sucesión exacta (2.3.2), $\ker(d_1^*)$ es f.g. ya que D_D es noetheriano, luego existe un D-módulo derecho libre de dimensión finita F_{-1}^* y un homomorfismo $d_0^* : F_{-1}^* \to F_0^*$; razonando de la misma forma para $\ker(d_0^*)$ y continuando de esta manera obtenemos la sucesión exacta

$$\cdots \to F_{-2}^* \xrightarrow{d_{-1}^*} F_{-1}^* \xrightarrow{d_0^*} F_0^* \xrightarrow{d_1^*} F_1^* \to N \to 0,$$

con F_i^* libre de dimensión finita. Aplicamos $Hom_D(\ \ , D)$ al complejo $\cdots \to F_{-2}^* \xrightarrow{d_{-1}^*} F_{-1}^* \xrightarrow{d_0^*} F_0^* \xrightarrow{d_1^*} F_1^* \to 0$ y se obtiene el complejo de D-módulos izquierdos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Hom_D(F_1^*, D) & \xrightarrow{d_1^{**}} & Hom_D(F_0^*, D) & \xrightarrow{d_0^{**}} & Hom_D(F_{-1}^*, D) & \xrightarrow{d_{-1}^{**}} & Hom_D(F_{-2}^*, D) & \longrightarrow & \cdots \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ 0 & \longrightarrow & F_1 & \xrightarrow{d_1} & F_0 & \xrightarrow{d_0} & F_{-1} & \xrightarrow{d_{-1}} & F_{-2} & \longrightarrow & \cdots \end{array}$$

luego $Ext^1_D(N,D) \cong \ker(d_0)/Im(d_1)$, $Ext^2_D(N,D) \cong \ker(d_{-1})/Im(d_0)$. Aplicamos entonces la proposición 2.1.6 y obtenemos la sucesión exacta

$$0 \to Ext^1_D(N,D) \to \operatorname{coker}(d_1) \to \ker(d_{-1}) \to Ext^2_D(N,D) \to 0.$$

Según (2.3.1), $M \cong \operatorname{coker}(d_1)$; además, de (2.3.3) $\ker(d_1^*) \cong M^*$, se tiene entonces el siguiente diagrama conmutativo exacto

$$\begin{array}{ccccc} F_{-2}^* & \xrightarrow{d_{-1}^*} & F_{-1}^* & \xrightarrow{d_0^*} & \ker(d_1^*) \to 0 \\ \downarrow = & & \downarrow = & & \downarrow\cong \\ F_{-2}^* & \xrightarrow{d_{-1}^*} & F_{-1}^* & \longrightarrow & M^* \to 0 \end{array}$$

Aplicamos $Hom_D(\ \ ,D)$ y resulta la sucesión exacta de D-módulos izquierdos

$$0 \to M^{**} \to F_{-1} \xrightarrow{d_{-1}} F_{-2},$$

de donde $\ker(d_{-1}) \cong M^{**}$, y en consecuencia se tiene la sucesión exacta

$$0 \to Ext_D^1(N,D) \to M \to M^{**} \to Ext_D^2(N,D) \to 0.$$

(iv) se obtiene en forma directa de (iii).

(v) Si M es proyectivo, entonces M es reflexivo (proposición 2.1.4), en consecuencia $Ext_D^i(N,D) = 0$ para $i = 1,2$ (parte (iv)). De (2.3.3) resultan las sucesiones exactas

$$0 \to M^* \to F_0^* \to Im(d_1^*) \to 0, \quad 0 \to \ker(\rho) \to F_1^* \to N \to 0,$$

y a partir de éstas se obtienen las sucesiones exactas largas

$$\cdots \to Ext_D^i(Im(d_1^*),D) \to Ext_D^i(F_0^*,D) \to Ext_D^i(M^*,D) \to Ext_D^{i+1}(Im(d_1^*),D) \to Ext_D^{i+1}(F_0^*,D) \to Ext_D^{i+1}(M^*,D) \to \cdots$$

$$\cdots \to Ext_D^{i+1}(N,D) \to Ext_D^{i+1}(F_1^*,D) \to Ext_D^{i+1}(\ker(\rho),D) \to Ext_D^{i+2}(N,D) \to Ext_D^{i+2}(F_1^*,D) \to Ext_D^{i+2}(\ker(\rho),D) \to \cdots$$

de lo cual se desprenden las sucesiones exactas

$$0 \to Ext_D^i(M^*,D) \to Ext_D^{i+1}(Im(d_1^*),D) \to 0$$

y

$$0 \to Ext_D^{i+1}(\ker(\rho),D) \to Ext_D^{i+2}(N,D) \to 0,$$

pero como $\ker(\rho) = Im(d_1^*)$, entonces $Ext_D^i(M^*,D) \cong Ext_D^{i+2}(N,D)$, para $i \geq 1$. Por la proposición 2.1.5, $Ext_D^i(M^*,D) = 0$, para cada $i \geq 1$, luego para cada $i \geq 1$, $Ext_D^{i+2}(N,D) = 0$. En total, $Ext_D^i(N,D) = 0$, para cada $1 \leq i \leq \operatorname{rgld}(D)$.

Recíprocamente, supongamos que $Ext_D^i(N,D) = 0$ para cada $1 \leq i \leq k$, con $k := \operatorname{rgld}(D)$, consideremos una resolución proyectiva de N de longitud k

$$0 \to P_k \xrightarrow{r_k} P_{k-1} \xrightarrow{r_{k-1}} \cdots \xrightarrow{r_3} P_2 \xrightarrow{r_2} P_1 \xrightarrow{r_1} P_0 \to N \to 0, \tag{2.3.11}$$

con P_i proyectivo f.g.; suprimiendo N y aplicando $Hom_D(\ \ ,D)$ obtenemos el complejo

$$0 \to P_0^* \xrightarrow{r_1^*} P_1^* \xrightarrow{r_2^*} P_2^* \xrightarrow{r_3^*} \cdots \xrightarrow{r_{k-1}^*} P_{k-1}^* \xrightarrow{r_k^*} P_k^* \to 0, \tag{2.3.12}$$

luego $Ext_D^i(N,D) = \ker(r_{i+1}^*)/Im(r_i^*)$, para $i \geq 1$, pero como $Ext_D^i(N,D) = 0$ para cada $1 \leq i \leq k$, entonces la sucesión

$$0 \to N^* \to P_0^* \xrightarrow{r_1^*} P_1^* \xrightarrow{r_2^*} P_2^* \xrightarrow{r_3^*} \cdots \xrightarrow{r_{k-1}^*} P_{k-1}^* \xrightarrow{r_k^*} P_k^* \to 0, \tag{2.3.13}$$

es exacta. Según la proposición 2.1.5, cada P_i^* es proyectivo, en particular, P_k^* es proyectivo, entonces la sucesión anterior es hendida. Por inducción, deducimos que

$Im(r_i^*)$ es un D-módulo izquierdo proyectivo para cada i, de lo cual resulta que la sucesión

$$0 \to N^* \to P_0^* \to Im(r_1^*) \to 0$$

es exacta hendida, luego N^* es sumando directo del proyectivo P_0^*, es decir, N^* es proyectivo. En consecuencia, N^{**} es proyectivo. Aplicando $Hom_D(\ \ , D)$ a (2.3.13) obtenemos la sucesión exacta hendida

$$0 \to P_k \xrightarrow{r_k} P_{k-1} \xrightarrow{r_{k-1}} \cdots \xrightarrow{r_3} P_2 \xrightarrow{r_2} P_1 \xrightarrow{r_1} P_0 \to N^{**} \to 0,$$

luego, junto con la resolución (2.3.11) y el lema de los cinco (véase [19]), concluimos que $N \cong N^{**}$ es proyectivo. Resulta entonces que la sucesión (2.3.3) es exacta hendida, por lo tanto, M^* es proyectivo, y de esta manera, M^{**} es proyectivo. Puesto que $Ext_D^i(N, D) = 0$ para $i = 1, 2$, podemos aplicar el (iv) y obtenemos que $M \cong M^{**}$ es proyectivo. □

Corolario 2.3.4. *Sea D un dominio con ${}_DD_D$ noetheriano y M un D-módulo f.g. Entonces, M es de torsión si, y sólo si, $M^* = 0$.*

Demostración. $\Rightarrow$) Este es el contenido de la proposición 2.1.3.

$\Leftarrow$) Como $M^* = 0$, entonces $M^{**} = 0$; además, como ${}_DD$ es noetheriano, entonces M es de presentación finita, luego por el teorema 2.3.3, $M \cong Ext_D^1(N, D) \cong t(M)$, es decir, M es de torsión. □

Corolario 2.3.5. *Sea D un dominio con ${}_DD_D$ noetheriano, y sea $R \in D^{q\times p}$, $M := D^{1\times p}/D^{1\times q}R$, $\mathcal{F}$ un D-módulo cogenerador inyectivo y $\mathcal{B}$ el conjunto de $\mathcal{F}$-soluciones del sistema $Ry = 0$. Entonces, $Ry = 0$ es parametrizable si, y sólo si, $t(M) = 0$ si, y sólo si, $Ry = 0$ es controlable.*

Demostración. Sea $Ry = 0$ un sistema parametrizable; por el teorema 2.3.2 existe $Q \in D^{p\times m}$ tal que $M \overset{\phi}{\cong} D^{1\times p}Q \subseteq D^{1\times m}$. Sea $z \in t(M)$, existe $d \in D - \{0\}$ tal que $d \cdot z = 0$, luego $0 = \phi(0) = \phi(d \cdot z) = d \cdot \phi(z)$ y entonces $\phi(z) \in t(D^{1\times m}) = 0$, de donde $z = 0$. Esto muestra que $t(M) = 0$. Por el teorema 2.3.2, el sistema $Ry = 0$ es controlable.

Recíprocamente, sea $Ry = 0$ controlable, entonces $t(M) = 0$; sea $N := M^T = \operatorname{coker}(R.) = D^q/RD^p$, entonces N tiene la presentación finita $D^p \xrightarrow{R.} D^q \to N \to 0$. Por el teorema 2.3.3, $Ext_D^1(N, D) = 0$. De otra parte, como D_D es noetheriano, $\ker(R.) \subseteq D^p$ es f.g., luego existe $Q \in D^{p\times m}$ tal que $\ker(R.) = QD^m$, y se tiene la siguiente resolución libre finita de N: $D^m \xrightarrow{Q.} D^p \xrightarrow{R.} D^q \to N \to 0$; aplicamos $Hom_D(\ \ , D)$ al complejo $D^m \xrightarrow{Q.} D^p \xrightarrow{R.} D^q \to 0$ y se obtiene el complejo de D-módulos izquierdos

$$\begin{tikzcd}
0 \arrow[r] & Hom_D(D^q, D) \arrow[r, "(R.)^*"] \arrow[d, "\cong"] & Hom_D(D^p, D) \arrow[r, "(Q.)^*"] \arrow[d, "\cong"] & Hom_D(D^m, D) \arrow[d, "\cong"] \\
0 \arrow[r] & D^{1\times q} \arrow[r, ".R"] & D^{1\times p} \arrow[r, ".Q"] & D^{1\times m}
\end{tikzcd}$$

de modo que $D^{1\times p}/\ker(.Q) \cong D^{1\times p}Q$, pero $0 = Ext^1_D(N, D) = \ker(.Q)/Im(.R)$, luego $\ker(.Q) = Im(.R) = D^{1\times q}R$, con lo cual $M = D^{1\times p}/D^{1\times q}R = D^{1\times p}/\ker(.Q) \cong \mathrm{Im}(.Q) = D^{1\times p}Q$, es decir, el sistema $Ry = 0$ es parametrizable. $\square$

Capítulo 3

Factorización y descomposición de sistemas lineales funcionales

Dados dos SLF, $Ry = 0$ y $R'z = 0$, estudiaremos en este capítulo los elementos del grupo $Hom_D(M, M')$, donde M y M' son los D-módulos de presentación finita asociados a dichos sistemas (véase la sección 2.2). Caracterizaremos matricialmente el núcleo, conúcleo, imagen y coimagen de tales morfismos, y veremos que cuando $M = M'$, es decir, para un mismo sistema, la existencia de un endomorfismo no inyectivo es equivalente a la factorización no trivial de la matriz R, $R = R_1R_2$. Veremos también, que bajo ciertas condiciones, un sistema $Ry = 0$ es triangulable en bloques, es decir, equivalente a un sistema $\overline{R}z = 0$, donde $\overline{R}$ es una matriz triangular en bloques del mismo tamaño de R. De igual manera, bajo ciertas condiciones, la existencia de idempotentes no triviales en $End_D(M)$ induce un sistema equivalente $\overline{R}z = 0$, donde $\overline{R}$ es una matriz diagonal en bloques del mismo tamaño de R. Además, tales idempotentes permiten describir las $\mathcal{F}$-soluciones del sistema (teorema 3.5.3).

Salvo que se advierta lo contrario, D es un anillo noetheriano, es decir, ${}_DD$ es noetheriano. Todo lo que presentaremos ha sido tomado y adaptado de [6].

3.1 Morfismos de sistemas lineales funcionales

En esta sección estudiamos desde un enfoque matricial-constructivo los elementos del grupo $Hom_D(M, M')$, donde M y M' son los D-módulos de presentación finita asociados a dos sistemas lineales funcionales. En [6] se muestra que si D es conmutativo, entonces es posible calcular de manera explícita un conjunto de generadores para el D-módulo $Hom_D(M, M')$. Cuando D no es necesariamente conmutativo, en [21] se ha también calculado un sistema de generadores para $Hom_D(M, M')$ asumiendo que M' es un $D - D$-bimódulo centralizante.

Iniciamos con el siguiente resultado que será ampliamente usado a lo largo de todo el capítulo.

Proposición 3.1.1. *Sean M y M' dos D-módulos de presentación finita:*

$$D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \to 0$$

$$D^{1\times q'} \xrightarrow{.R'} D^{1\times p'} \xrightarrow{\pi'} M' \to 0.$$

Entonces,

1. *La existencia de un D-homomorfismo $f : M \to M'$ es equivalente a la existencia de dos matrices $P \in D^{p\times p'}, Q \in D^{q\times q'}$ tales que*

$$RP = QR'. \tag{3.1.1}$$

De esta forma, el siguiente diagrama es conmutativo

$$\begin{tikzcd} D^{1\times q} \arrow[r, ".R"] \arrow[d, ".Q"] & D^{1\times p} \arrow[r, "\pi"] \arrow[d, ".P"] & M \arrow[r] \arrow[d, "f"] & 0 \\ D^{1\times q'} \arrow[r, ".R'"] & D^{1\times p'} \arrow[r, "\pi'"] & M' \arrow[r] & 0 \end{tikzcd} \tag{3.1.2}$$

donde $f \in Hom_D(M, M')$ es definido por

$$f(\pi(\lambda)) := \pi'(\lambda P),\ \lambda \in D^{1\times p}. \tag{3.1.3}$$

2. *Sea $R_2' \in D^{q_2'\times q'}$ tal que $\ker(.R') = D^{1\times q_2'}R_2'$, y sean $P \in D^{p\times p'}$ y $Q \in D^{q\times q'}$ tales que $RP = QR'$. Entonces, para cualesquiera $Z_1 \in D^{p\times q'}$ y $Z_2 \in D^{q\times q_2'}$, las matrices definidas por*

$$\overline{P} := P + Z_1R', \qquad \overline{Q} := Q + RZ_1 + Z_2R_2',$$

satisfacen $R\overline{P} = \overline{Q}R'$, y además, $f(\pi(\lambda)) = \pi'(\lambda\overline{P}),\ \lambda \in D^{1\times p}$.

Demostración. 1. Puesto que $D^{1\times p}$ es un D-modulo proyectivo, entonces existe un D-homomorfismo $p : D^{1\times p} \to D^{1\times p'}$ tal que $\pi' p = f\pi$. Sea P la matriz del homomorfismo p en las bases canónicas de $D^{1\times p}$ y $D^{1\times p'}$. Es claro que p coincide con el D-homomorfismo $.P$ inducido por la matriz P. Ahora notemos que $\pi'.P.R = 0$, es decir, $Im(.P.R) \subseteq \ker(\pi') = Im(.R')$, luego como $D^{1\times q}$ es proyectivo, existe un D-homomorfismo $q : D^{1\times q} \to D^{1\times q'}$ tal que $.R'q = .P.R$. Si Q es la matriz de q en las bases canónicas, entonces (3.1.1)-(3.1.3) se cumplen.

Recíprocamente, supongamos que (3.1.1) se cumple. Entonces, f como en (3.1.3) es un D-homomorfismo bien definido: en efecto, sean $\lambda, \lambda' \in D^{1\times p}$ tales que $\pi(\lambda) = \pi(\lambda')$, entonces $\lambda - \lambda' \in \ker(\pi) = Im(.R)$, de donde existe $\alpha \in D^{1\times q}$ tal que $\lambda - \lambda' = \alpha R$. Resulta, $\pi'((\lambda - \lambda')P) = \pi'(\alpha RP) = \pi'(\alpha QR') = (\pi'.R'.Q)(\alpha) = 0$. Es claro que f es un D-homomorfismo que hace el diagrama (3.1.2) conmutativo.

2. Esta parte de la proposición se prueba por cálculo directo. $\square$

Sean M y M' de presentación finita y $f \in Hom_D(M, M')$, queremos ahora caracterizar matricialmente los D-módulos $\ker(f)$, $Im(f)$, $\operatorname{coker}(f)$ y $Coim(f)$. Recordemos que si $R \in D^{q\times p}$, entonces $\ker(.R) := \{\lambda \in D^{1\times q} \mid \lambda R = 0\}$, es decir, $\ker(.R)$ es el módulo de sicigias del módulo generado por las filas de R (véase [21], capítulo 9).

Proposición 3.1.2. *Sean $R \in D^{q\times p}, R' \in D^{q'\times p'}, M := D^{1\times p}/(D^{1\times q}R)$, y $M' := D^{1\times p'}/(D^{1\times q'}R')$. Sea $f : M \to M'$ un D-homomorfismo definido por medio de dos matrices $P \in D^{p\times p'}, Q \in D^{q\times q'}$, las cuales satisfacen la relación (3.1.1). Entonces,*

1. *Existen matrices $S \in D^{r\times p}$ y $T \in D^{r\times q'}$ tales que*

$$\ker\left(.\begin{bmatrix} P \\ R' \end{bmatrix}\right) = D^{1\times r}[S \quad -T]. \tag{3.1.4}$$

2. $\ker(f) \cong (D^{1\times r}S)/(D^{1\times q}R)$.

3. $Coim(f) \cong D^{1\times p}/(D^{1\times r}S)$.

4. $Im(f) \cong \left(D^{1\times(p+q')}\begin{bmatrix} P \\ R' \end{bmatrix}\right)\Big/(D^{1\times q'}R')$.

5. $\operatorname{coker}(f) \cong D^{1\times p'}\Big/\left(D^{1\times(p+q')}\begin{bmatrix} P \\ R' \end{bmatrix}\right)$.

Demostración. 1. Puesto que ${}_DD$ es noetheriano, el núcleo del D-homomorfismo matricial en (3.1.4) es f.g. y entonces existe $r \geq 1$ y matrices $S \in D^{r\times p}$ y $T \in D^{r\times q'}$ tales que (3.1.4) se tiene.

2. Sea $m = \pi(\lambda) \in \ker(f)$ con $\lambda \in D^{1\times p}$ (véase el diagrama (3.1.2)). Entonces, $0 = f(m) = \pi'(\lambda P)$ implica que $\lambda P \in (D^{1\times q'}R')$, es decir, existe $\mu \in D^{1\times q'}$ tal que $\lambda P = \mu R'$. Por lo tanto,

$$[\lambda \quad -\mu] \in \ker\left(.\begin{bmatrix} P \\ R' \end{bmatrix}\right).$$

Recíprocamente, si $[\lambda \quad -\mu]$ está en el núcleo del homomorfismo matricial de (3.1.4), entonces $m := \pi(\lambda) \in \ker(f)$.

Puesto que $RP = QR'$, entonces

$$(D^{1\times q}[R \quad -Q]) \subseteq \ker\left(. \begin{bmatrix} P \\ R' \end{bmatrix}\right) = D^{1\times r}[S \quad -T],$$

y así, existe una matriz $L \in D^{q\times r}$ la cual satisface

$$R = LS, \qquad Q = LT.$$

En particular, $Im(.R) \subseteq Im(.S)$, es decir, $D^{1\times q}R \subseteq D^{1\times r}S$. Entonces definimos

$$\begin{aligned} \ker(f) &\xrightarrow{k} (D^{1\times r}S)/(D^{1\times q}R) \\ m = \pi(\lambda) &\mapsto \overline{\lambda} \end{aligned}$$

k está bien definida ya que si $\lambda' \in D^{1\times p}$ es tal que $m = \pi(\lambda')$, entonces $\lambda - \lambda' \in \ker(\pi) = Im(.R) = (D^{1\times q}R)$. Es claro que k es un D-homomorfismo. Si $m = \pi(\lambda) \in \ker(f)$ es tal que $k(\pi(\lambda)) = \overline{0}$, entonces $\lambda \in Im(.R) = \ker(\pi)$, es decir, $m = 0$ y así k es inyectivo. Para concluir veamos que k es sobreyectivo: sea λ una de las filas de S y sea μ la correspondiente fila de T, entonces $[\lambda \quad -\mu]$ está en el núcleo del homomorfismo de (3.1.4), y como vimos, $m := \pi(\lambda) \in \ker(f)$ y $k(m) = \overline{\lambda}$.

3. A partir de la sucesión exacta corta $0 \to \ker(f) \xrightarrow{i} M \xrightarrow{\rho} Coim(f) \to 0$, donde i denota la inclusión y ρ el homomorfismo canónico, y ya que $M = D^{1\times p}/(D^{1\times q}R)$, junto con el hecho que $\ker(f) = (D^{1\times r}S)/(D^{1\times q}R)$, se obtiene la sucesión exacta

$$0 \to (D^{1\times r}S)/(D^{1\times q}R) \xrightarrow{i} D^{1\times p}/(D^{1\times q}R) \xrightarrow{\rho} Coim(f) \to 0,$$

lo cual muestra que $Coim(f) \cong D^{1\times p}/(D^{1\times r}S)$.

4. Según (3.1.3), para todo $\lambda \in D^{1\times p}$, $f(\pi(\lambda)) = \pi'(\lambda P)$, luego definimos

$$\begin{aligned} Im(f) &\xrightarrow{h} \left(D^{1\times(p+q')} \begin{bmatrix} P \\ R' \end{bmatrix}\right) \Big/ (D^{1\times q'}R') \\ f(\pi(\lambda)) &\mapsto \overline{\lambda P} \end{aligned}$$

h está bien definida ya que si $\lambda' \in D^{1\times p}$ es tal que $f(\pi(\lambda)) = f(\pi(\lambda'))$, entonces $\pi'(\lambda P) = \pi'(\lambda' P)$, de donde $\lambda P - \lambda' P \in \ker(\pi') = Im(.R')$. Claramente h es un D-homomorfismo; sea $f(\pi(\lambda)) \in \ker(h)$, entonces existe $\mu \in D^{1\times q'}$ tal que $\lambda P = \mu R'$, con lo cual $f(\pi(\lambda)) = (\pi'.P)(\lambda) = \pi'(\lambda P) = \pi'(\mu R') = (\pi'.R')(\mu) = 0$. Esto muestra que h es inyectivo. Veamos que h es sobreyectivo: sea $\alpha \in D^{1\times p'}$ una de las filas de $\begin{bmatrix} P \\ R' \end{bmatrix}$; si α es la i-ésima fila de P, $1 \leq i \leq p$, entonces $\overline{\alpha} = \overline{e_i P} = f(\pi(e_i))$ ya que $(\pi'.P)(e_i) = \pi'(e_i P) = \pi'(\alpha)$, donde e_i es el i-ésimo vector canónico de $D^{1\times p}$. Sea α una de las filas de R', entonces $\overline{\alpha} = \overline{0}$ y la preimagen de $\overline{\alpha}$ es cero. Hemos demostrado de h es un isomorfismo.

5. Utilizando la sucesión exacta corta

$$0 \to Im(f) \xrightarrow{j} M' \xrightarrow{\sigma} \operatorname{coker}(f) \to 0,$$

donde j denota la inclusión, σ el homomorfismo canónico, y puesto que $M' = D^{1\times p'}/(D^{1\times q'}R')$ e $Im(f)$ es como en el punto anterior, obtenemos la sucesión exacta

$$0 \to \left(D^{1\times(p+q')}\begin{bmatrix} P \\ R' \end{bmatrix}\right)\Big/(D^{1\times q'}R') \xrightarrow{j} D^{1\times p'}/(D^{1\times q'}R') \xrightarrow{\sigma} \operatorname{coker}(f) \to 0,$$

luego el resultado se obtiene por el segundo teorema de isomorfismo para módulos.

□

3.2 Factorización de sistemas lineales funcionales

A continuación precisamos la factorización de sistemas lineales funcionales que vimos en la demostración de la proposición 3.1.2. Véase [6], teorema 3.1.

Teorema 3.2.1. *Sean $R \in D^{q\times p}$ y $R' \in D^{q'\times p'}$ matrices, $M := D^{1\times p}/(D^{1\times q}R)$ y $M' := D^{1\times p'}/(D^{1\times q'}R')$. Sea $f : M \to M'$ un D-homomorfismo definido por medio de dos matrices $P \in D^{p\times p'}$ y $Q \in D^{q\times q'}$, las cuales satisfacen la relación (3.1.1). Entonces se obtiene una factorización de R en la forma $R = LS$, con $L \in D^{q\times r}$ y $S \in D^{r\times p}$, tal que $Coim(f) = D^{1\times p}/(D^{1\times r}S)$.*

Demostración. Tal como vimos en la demostración de la proposición 3.1.2, a partir de (3.1.4) y la condición $RP = QR'$, obtenemos

$$(D^{1\times q}[R \quad -Q]) \subseteq \ker\left(. \begin{bmatrix} P \\ R' \end{bmatrix}\right) = D^{1\times r}[S \quad -T],$$

y así, existe una matriz $L \in D^{q\times r}$ la cual satisface

$$R = LS, \qquad Q = LT. \tag{3.2.1}$$

Según la proposición 3.1.2, $Coim(f) = D^{1\times p}/(D^{1\times r}S)$. Notemos adicionalmente que se tiene el siguiente diagrama conmutativo:

$$
\begin{tikzcd}
 & & 0 \arrow[d] & \\
 & 0 \arrow[d] & \ker(f) \arrow[d, "i"] & \\
D^{1\times q} \arrow[r, ".R"] \arrow[d, ".L"] & D^{1\times p} \arrow[r, "\pi"] \arrow[d, "="] & M \arrow[r] \arrow[d, "\rho"] & 0 \\
D^{1\times r} \arrow[r, ".S"] & D^{1\times p} \arrow[r, "\kappa"] \arrow[d] & Coim(f) \arrow[r] \arrow[d] & 0, \\
 & 0 & 0 &
\end{tikzcd}
\tag{3.2.2}
$$

donde i es la inclusión y π, ρ, κ son los homomorfismos canónicos. $\square$

El siguiente lema será útil para la caracterización matricial de homomorfismos nulos, inyectivos y sobreyectivos que presentaremos en el teorema 3.2.4.

Lema 3.2.2. *Sean $R \in D^{q\times p}, R' \in D^{q'\times p}$ y $R'' \in D^{q\times q'}$ tres matrices tales que $R = R''R'$. Sea $T' \in D^{r'\times q'}$ tal que $\ker(.R') = D^{1\times r'}T'$. Sean $M_1 := (D^{1\times q'}R')/(D^{1\times q}R)$ y $M_2 := D^{1\times q'}/(D^{1\times q}R'' + D^{1\times r'}T')$. Sean π_1 y π_2 los homomorfismos canónicos:*

$$
\begin{aligned}
\pi_1 &: D^{1\times q'}R' \to (D^{1\times q'}R')/(D^{1\times q}R),\\
\pi_2 &: D^{1\times q'} \to D^{1\times q'}/(D^{1\times q}R'' + D^{1\times r'}T').
\end{aligned}
$$

Entonces, el D-homomorfismo ψ definido por

$$\psi : M_2 \to M_1, \quad m_2 = \pi_2(\lambda) \mapsto \psi(m_2) := \pi_1(\lambda R'),\ \lambda \in D^{1\times q'}$$

es un isomorfismo y su inverso está dado por

$$\phi : M_1 \to M_2, \quad m_1 = \pi_1(\lambda R') \mapsto \phi(m_1) := \pi_2(\lambda),\ \lambda \in D^{1\times q'}.$$

En otras palabras, se tiene el isomorfismo de D-módulos

$$(D^{1\times q'}R')/(D^{1\times q}R) \cong D^{1\times q'}/(D^{1\times q}R'' + D^{1\times r'}T'). \tag{3.2.3}$$

Demostración. Veamos que la función ψ está bien definida. Supongamos que $m_2 = \pi_2(\lambda) = \pi_2(\lambda')$, donde $\lambda, \lambda' \in D^{1\times q'}$. Entonces, $\pi_2(\lambda - \lambda') = 0$, es decir, $\lambda - \lambda' \in$

$(D^{1\times q}R''+D^{1\times r'}T')$, luego existen $\mu \in D^{1\times q}, \nu \in D^{1\times r'}$ tales que $\lambda-\lambda' = \mu R''+\nu T'$. Tenemos entonces

$$(\lambda-\lambda')R' = (\mu R''+\nu T')R' = \mu R \Rightarrow \pi_1((\lambda-\lambda')R') = \pi_1(\mu R) = 0, \qquad (3.2.4)$$

lo cual implica que $\pi_1(\lambda' R') = \pi_1(\lambda R') = \psi(m_2)$. Mostremos ahora que ϕ está bien definida. Consideremos $m_1 = \pi_1(\lambda R') = \pi_1(\lambda' R')$, donde $\lambda, \lambda' \in D^{1\times q'}$. Obtenemos $\pi_1((\lambda-\lambda')R') = 0$, es decir, $(\lambda-\lambda')R' \in (D^{1\times q}R)$, y así, existe $\mu \in D^{1\times q}$ tal que $(\lambda-\lambda')R' = \mu R$. Ahora, usando la factorización $R = R''R'$, se obtiene que $(\lambda-\lambda'-\mu R'')R' = 0$, así que $\lambda-\lambda'-\mu R'' \in \ker(.R') = D^{1\times r'}T'$. Por lo tanto, existe $\nu \in D^{1\times r'}$ tal que $\lambda-\lambda' = \mu R''+\nu T'$, y así

$$\pi_2(\lambda)-\pi_2(\lambda') = \pi_2(\lambda-\lambda') = \pi_2(\mu R''+\nu T') = 0.$$

Finalmente, para todo $m_1 = \pi_1(\lambda R') \in M_1$ y todo $m_2 = \pi_2(\lambda) \in M_2$, con $\lambda \in D^{1\times q'}$, tenemos

$$\begin{aligned}(\psi\circ\phi)(m_1) &= \psi(\pi_2(\lambda)) = \pi_1(\lambda R') = m_1,\\ (\phi\circ\psi)(m_2) &= \phi(\pi_1(\lambda R')) = \pi_2(\lambda) = m_2,\end{aligned}$$

lo cual muestra que $\psi\circ\phi = \mathrm{id}_{M_1}, \phi\circ\psi = \mathrm{id}_{M_2}$, y así obtenemos (3.2.3). □

De la proposición 3.1.2 y el lema 3.2.2 obtenemos los siguientes resultados.

Corolario 3.2.3. *Sean $R \in D^{q\times p}$ y $R' \in D^{q'\times p'}$ matrices y sean $M := D^{1\times p}/(D^{1\times q}R)$, $M' := D^{1\times p'}/(D^{1\times q'}R')$. Sea $f : M \to M'$ un D-homomorfismo definido por medio de dos matrices $P \in D^{p\times p'}$ y $Q \in D^{q\times q'}$, las cuales satisfacen la relación (3.1.1). Sean $L \in D^{q\times r}$ y $S \in D^{r\times p}$ tales que $R = LS$ y sea $\ker(.S) = D^{1\times r_2}S_2, S_2 \in D^{r_2\times r}$. Entonces,*

$$\ker(f) \cong D^{1\times r} \Big/ \left(D^{1\times(q+r_2)}\begin{bmatrix} L \\ S_2\end{bmatrix}\right).$$

Demostración. De la proposición 3.1.2 sabemos que

$$\ker(f) \cong (D^{1\times r}S)/(D^{1\times q}R),$$

luego $\ker(f) \cong (D^{1\times r}S)/(D^{1\times q}LS)$, aplicamos entonces (3.2.3) y obtenemos

$$\begin{gathered}\ker(f) \cong (D^{1\times r}S)/(D^{1\times q}LS) \cong D^{1\times r}/(D^{1\times q}L + D^{1\times r_2}S_2) = \\ D^{1\times r} \Big/ \left(D^{1\times(q+r_2)}\begin{bmatrix} L \\ S_2\end{bmatrix}\right).\end{gathered}$$

□

Teorema 3.2.4. *Sean $R \in D^{q\times p}$ y $R' \in D^{q'\times p'}$ matrices y sean $M := D^{1\times p}/(D^{1\times q}R)$, $M' := D^{1\times p'}/(D^{1\times q'}R')$. Sea $f : M \to M'$ un D-homomorfismo definido por medio de dos matrices $P \in D^{p\times p'}$ y $Q \in D^{q\times q'}$, las cuales satisfacen la relación (3.1.1). Sean $L \in D^{q\times r}$ y $S \in D^{r\times p}$ tales que $R = LS$ y sea $\ker(.S) = D^{1\times r_2}S_2, S_2 \in D^{r_2\times r}$. Entonces, para un homomorfismo $f \in Hom_D(M, M')$ se tiene que:*

1. *f es nulo si, y sólo si, se cumple alguna de las siguientes condiciones:*
   (a) *Existe una matriz $Z \in D^{p\times q'}$ tal que $P = ZR'$. En tal caso, existe $Z' \in D^{q\times q'_2}$ tal que $Q = RZ + Z'R'_2$, donde la matriz $R'_2 \in D^{q'_2\times q'}$ satisface $\ker(.R') = D^{1\times q'_2}R'_2$.*
   (b) *S tiene inversa a izquierda.*
2. *f es inyectivo si, y sólo si, se cumple alguna de las siguientes condiciones:*
   (a) *Existe una matriz $F \in D^{r\times q}$ tal que $S = FR$.*
   (b) *La matriz $[L^T \quad S_2^T]^T$ tiene inversa a izquierda.*
3. *f es sobreyectivo si, y sólo si, la matriz $[P^T \quad R'^T]^T$ tiene inversa a izquierda.*
4. *f es un isomorfismo si, y sólo si, las matrices $[L^T \quad S_2^T]^T$ y $[P^T \quad R'^T]^T$ admiten inversa a izquierda.*

Demostración. 1. Por la parte 4 de la proposición 3.1.2, tenemos que $Im(f) = 0$ si, y sólo si, $D^{1\times p}P + D^{1\times q'}R' = D^{1\times q'}R'$, esto es, si, y sólo si, $(D^{1\times p}P) \subseteq (D^{1\times q'}R')$, lo cual es equivalente a la existencia de una matriz $Z \in D^{p\times q'}$ tal que $P = ZR'$. Así, reemplazando $P = ZR'$ en la condición (3.1.1), obtenemos

$$RZR' = QR' \Leftrightarrow (Q - RZ)R' = 0.$$

Por lo tanto, existe $Z' \in D^{q\times q'_2}$ tal que $Q - RZ = Z'R'_2$, lo cual prueba (a).

Veamos la prueba de (b). A partir del isomorfismo canónico $Coim(f) \to Im(f)$ obtenemos de la parte 3 de la proposición 3.1.2 que $\mathrm{Im} f = 0$ si, y sólo si,

$$Coim(f) = D^{1\times p}/(D^{1\times r}S) = 0 \Leftrightarrow D^{1\times r}S = D^{1\times p},$$

es decir, si, y sólo si, S admite inversa a izquierda.

2. De la parte 2 de la proposición 3.1.2, tenemos que $\ker(f) = 0$ si, y sólo si, $D^{1\times r}S = D^{1\times q}R$, es decir, si, y sólo si, existe $F \in D^{r\times q}$ tal que $S = FR$. Además, por el corolario 3.2.3, $\ker(f) = 0$ si, y sólo si, $D^{1\times q}L + D^{1\times r_2}S_2 = D^{1\times r}$, lo cual es equivalente a que la matriz $[L^T \quad S_2^T]^T$ admita inversa a izquierda.

3. f es un epimorfismo si, y sólo si, $\mathrm{coker}(f) = 0$, lo cual es equivalente a que $D^{1\times p}P + D^{1\times q'}R' = D^{1\times p'}$ (parte 5 de la proposición 3.1.2). Esto último es es equivalente a que la matriz $[P^T \quad R'^T]^T$ admita inversa a izquierda.

4. La afirmación se sigue de 2(b) y 3. □

3.3 Descomposiciones triangulares de SLF

En esta sección estudiaremos la descomposición triangular de sistemas lineales funcionales. Para esto utilizaremos el ***grupo lineal general*** sobre D denotado por $GL_p(D)$, esto es,

$$GL_p(D) := \{U \in D^{p\times p} \mid \exists V \in D^{p\times p} : UV = VU = I_p\},$$

donde I_p denota la matriz idéntica de tamaño $p \times p$. Llamaremos a un elemento de $GL_p(D)$ una ***matriz unimodular***.

Proposición 3.3.1. *Sea $P \in D^{p\times p}$. Las siguientes afirmaciones son equivalentes:*

1. *Los D-módulos* $\ker(.P)$ *y $Coim(.P)$ son libres de rangos m y $p-m$, respectivamente, con $1 \leq m \leq p$*

2. *Existen matrices $U \in GL_p(D)$ y $J \in D^{p\times p}$ tales que*

$$UP = JU, \tag{3.3.1}$$

donde J es de la forma

$$J = \begin{bmatrix} 0 & 0 \\ J_1 & J_2 \end{bmatrix}, \quad J_1 \in D^{(p-m)\times m}, \quad J_2 \in D^{(p-m)\times(p-m)},$$

y $[J_1 \quad J_2]$ tiene rango de filas completo, es decir, $\ker(.[J_1 \quad J_2]) = 0$.

Además, U tiene la forma

$$U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} \tag{3.3.2}$$

y satisface las siguientes condiciones:

(a) *$U_1 \in D^{m\times p}$ define una base para* $\ker(.P)$, *es decir,*

$$\ker(.U_1) = 0 \text{ y } \ker(.P) = D^{1\times m}U_1.$$

(b) *$U_2 \in D^{(p-m)\times p}$ define una base para $Coim(.P) = D^{1\times p}/(D^{1\times m}U_1)$, esto es,*

$$\ker(.U_2) = 0 \text{ y } Coim(.P) = D^{1\times(p-m)}U_2.$$

(c) *Existen matrices matrices $W_1 \in D^{p\times m}$ y $W_2 \in D^{p\times(p-m)}$ tales que las siguientes sucesiones son exactas hendidas:*

$$0 \to D^{1\times m} \xrightarrow{.U_1} D^{1\times p} \xrightarrow{.W_2} D^{1\times(p-m)} \to 0,$$

$$0 \to D^{1\times(p-m)} \xrightarrow{.U_2} D^{1\times p} \xrightarrow{.W_1} D^{1\times m} \to 0.$$

(d) *Se tienen las relaciones*

$$U_1 P = 0, \quad U_2 P = J_1 U_1 + J_2 U_2.$$

Demostración. $1 \Rightarrow 2$: supongamos que $\ker(.P)$ y $Coim(.P)$ son libres de rangos m y $p-m$, respectivamente. Ya que D es noetheriano, sea $U_1 \in D^{m\times p}$ una base para $\ker(.P)$, esto es, $\ker(.U_1) = 0$ y $\ker(.P) = D^{1\times m}U_1$. Se tiene entonces la sucesión exacta

$$0 \to D^{1\times m} \xrightarrow{.U_1} D^{1\times p} \xrightarrow{\kappa} Coim(.P) \to 0,$$

donde κ es el homomorfismo canónico. Puesto que $Coim(.P)$ es libre de rango $p-m$ se tiene un D-isomorfismo $\phi : Coim(.P) \to D^{1\times(p-m)}$, y de aquí, el D-homomorfismo $\phi \circ \kappa : D^{1\times p} \to D^{1\times(p-m)}$ con matriz $W_2 \in D^{p\times(p-m)}$ en las bases canónicas. Resulta entonces la sucesión exacta

$$0 \to D^{1\times m} \xrightarrow{.U_1} D^{1\times p} \xrightarrow{.W_2} D^{1\times(p-m)} \to 0.$$

Dado que $D^{1\times(p-m)}$ es un D-módulo libre, entonces es proyectivo, y así la sucesión anterior es hendida, lo cual significa que existen matrices $W_1 \in D^{p\times m}, U_2 \in D^{(p-m)\times p}$ tales que cumplen las identidades de Bézout:

$$\begin{bmatrix} U_1 \\ U_2 \end{bmatrix} [W_1 \quad W_2] = I_p, \quad [W_1 \quad W_2] \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} = I_p.$$

Esto hace que la segunda sucesión en (c) también sea exacta hendida. Sea U definido como en (3.3.2), entonces $U^{-1} = [W_1 \quad W_2] \in D^{p\times p}$ y

$$UP = \begin{bmatrix} U_1 P \\ U_2 P \end{bmatrix} = \begin{bmatrix} 0 \\ (U_2 P U^{-1})U \end{bmatrix} = \begin{bmatrix} 0 \\ U_2 P U^{-1} \end{bmatrix} U.$$

Podemos partir $U_2 P U^{-1}$ en dos bloques y denotar

$$[J_1 \quad J_2] := U_2 P U^{-1}, \quad J := \begin{bmatrix} 0 \\ U_2 P U^{-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ J_1 & J_2 \end{bmatrix} \in D^{p\times p}.$$

Con esta notación,

$$U_2 P = U_2 P U^{-1} U = [J_1 \quad J_2] \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} = J_1 U_1 + J_2 U_2.$$

Finalmente, si $\lambda \in \ker(.(U_2 P U^{-1}))$, entonces

$$\begin{aligned} \lambda[U_2 P U^{-1}] = 0 \Leftrightarrow (\lambda U_2)P = 0 \Leftrightarrow \lambda U_2 \in \ker(.P) = D^{1\times m}U_1 \\ \Leftrightarrow \exists \mu \in D^{1\times m} : \lambda U_2 = \mu U_1 \\ \Leftrightarrow [-\mu \quad \lambda] \in \ker(.U) = 0, \end{aligned}$$

con lo cual $\lambda = 0$ ya que U es unimodular.

$2 \Rightarrow 1$: utilizando la relación (3.3.1), y el hecho que U es una matriz unimodular, tenemos el diagrama conmutativo

$$\begin{tikzcd} D^{1\times p} \arrow[r, ".P"] & D^{1\times p} \\ D^{1\times p} \arrow[u, ".U"] \arrow[r, ".J"] & D^{1\times p} \arrow[u, ".U"'] \end{tikzcd}$$

el cual prueba que $\ker(.P) \cong \ker(.J)$. Calculemos $\ker(.J)$: consideremos $[\lambda_1 \quad \lambda_2] \in \ker(.J)$, entonces $\lambda_2[J_1 \quad J_2] = 0$, y dado que $[J_1 \quad J_2]$ tiene rango de filas completo, se sigue que $\lambda_2 = 0$ y λ_1 es un elemento arbitrario de $D^{1\times m}$, por lo tanto $\ker(.J) = D^{1\times m}$ y así $\ker(.P)$ es un D-módulo libre de rango m.

Similarmente, $Im(.P) \cong Im(.J) = D^{1\times(p-m)}[J_1 \quad J_2]$, pero $[J_1 \quad J_2]$ tiene rango de filas completo, entonces $D^{1\times(p-m)}[J_1 \quad J_2] \cong D^{1\times(p-m)}$. Por lo tanto, $Coim(.P) \cong Im(.P)$ es un D-módulo libre de rango $p-m$, lo cual finaliza la demostración. $\square$

Los siguientes dos lemas son necesarios para la prueba del teorema 3.3.4 sobre triangulación de sistemas lineales funcionales.

Lema 3.3.2. *Sean $R \in D^{q\times p}, P \in D^{p\times p}$ y $Q \in D^{q\times q}$ matrices tales que $RP = QR$. Sean $U \in GL_p(D)$ y $V \in GL_q(D)$ las cuales satisfacen*

$$\begin{cases} UP = J_P U, \\ VQ = J_Q V, \end{cases} \tag{3.3.3}$$

para ciertas matrices $J_P \in D^{p\times p}$ y $J_Q \in D^{q\times q}$. Entonces,

$$[VRU^{-1}]J_P = J_Q[VRU^{-1}]. \tag{3.3.4}$$

Demostración. Véase [6], Lema 3.2. $\square$

Lema 3.3.3. *Sean*

$$\begin{cases} J_P = \begin{bmatrix} 0 & 0 \\ J_1 & J_2 \end{bmatrix}, \\ J_Q = \begin{bmatrix} 0 & 0 \\ J_3 & J_4 \end{bmatrix}, \end{cases} \tag{3.3.5}$$

matrices de tamaño $p \times p$ y $q \times q$, respectivamente, con

$$J_1 \in D^{(p-m)\times m},\ J_2 \in D^{(p-m)\times(p-m)},\ J_3 \in D^{(q-l)\times l},\ J_4 \in D^{(q-l)\times(q-l)},$$

y $1 \leq m \leq p, 1 \leq l \leq q$. Además, sea $\overline{R} \in D^{q\times p}$ una matriz tal que

$$\overline{R} J_P = J_Q \overline{R}.$$

Si $[J_1 \ \ J_2]$ tiene rango de filas completo, entonces existen tres matrices $\overline{R_1} \in D^{l\times m}, \overline{R_2} \in D^{(q-l)\times m}, \overline{R_3} \in D^{(q-l)\times(p-m)}$ tales que

$$\overline{R} = \begin{bmatrix} \overline{R_1} & 0 \\ \overline{R_2} & \overline{R_3} \end{bmatrix}. \tag{3.3.6}$$

Demostración. Véase [6], Lema 3.3. □

Teorema 3.3.4. *Sea $R \in D^{q\times p}$, $M := D^{1\times p}/(D^{1\times q}R)$ y $f : M \to M$ un D-endomorfismo definido por las matrices $P \in D^{p\times p}$ y $Q \in D^{q\times q}$ tales que $RP = QR$. Si $\ker(.P)$, $Coim(.P)$, $\ker(.Q)$ y $Coim(.Q)$ son libres de rangos $m, p-m, l$ y $q-l$, respectivamente, con $1 \leq m \leq p$ y $1 \leq l \leq q$, entonces se tienen las siguientes afirmaciones:*

1. *Existen matrices $U \in GL_p(D)$ y $V \in GL_q(D)$ tales que*

$$\begin{cases} P = U^{-1} J_P U, \\ Q = V^{-1} J_Q V, \end{cases}$$

donde J_P y J_Q son las matrices definidas por la relación (3.3.5). Las matrices U y V están definidas por

$$\begin{cases} U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}, \quad U_1 \in D^{m\times p}, \quad U_2 \in D^{(p-m)\times p}, \\ V = \begin{bmatrix} V_1 \\ V_2 \end{bmatrix}, \quad V_1 \in D^{l\times q}, \quad V_2 \in D^{(q-l)\times q}, \end{cases}$$

donde las matrices de rango completo U_1 y V_1, respectivamente, definen bases para $\ker(.P)$ y $\ker(.Q)$, es decir,

$$\begin{cases} \ker(.P) = D^{1\times m} U_1, \\ \ker(.Q) = D^{1\times l} V_1, \end{cases}$$

y las matrices de rango completo U_2 y V_2, respectivamente, definen bases para

$$Coim(.P) = D^{1\times p}/(D^{1\times m} U_1), \quad Coim(.Q) = D^{1\times q}/(D^{1\times l} V_1).$$

2. *La matriz R es equivalente a la matriz $\overline{R} := VRU^{-1} \in D^{q\times p}$.*

3. *Si denotamos por $U^{-1} := [W_1 \;\; W_2]$, con $W_1 \in D^{p\times m}, W_2 \in D^{p\times(p-m)}$, entonces*

$$\overline{R} = \begin{bmatrix} V_1RW_1 & 0 \\ V_2RW_1 & V_2RW_2 \end{bmatrix}.$$

Demostración. 1. El resultado se sigue de la afirmación 2 de la proposición 3.3.1.

2. Puesto que U y V son matrices unimodulares, entonces $R = V^{-1}\overline{R}U$.

3. Por el lema 3.3.2, la matriz $\overline{R} = VRU^{-1}$ satisface la condición (3.3.4). Así, aplicando el lema 3.3.3 a la matriz $\overline{R}$, obtenemos que $\overline{R}$ tiene la forma triangular (3.3.6), donde $\overline{R_1} \in D^{l\times m}, \overline{R_2} \in D^{(q-l)\times m}$ y $\overline{R_3} \in D^{(q-l)\times(p-m)}$. Por último, tenemos que

$$\overline{R} = VRU^{-1} = \begin{bmatrix} V_1RW_1 & V_1RW_2 \\ V_2RW_1 & V_2RW_2 \end{bmatrix}$$

con $V_1RW_1 \in D^{l\times m}, V_2RW_1 \in D^{(p-l)\times m}, V_1RW_2 \in D^{(q-l)\times m}, V_2RW_2 \in D^{(p-l)\times(p-m)}$. Notemos que necesariamente $V_1RW_2 = 0$. □

3.4 Idempotentes y descomposiciones diagonales

Veremos en esta sección la descomposición diagonal de sistemas lineales funcionales. Iniciamos con dos lemas relativos a endomorfismos y matrices idempotentes.

Lema 3.4.1. *Sea M un D-módulo con sucesión exacta*

$$D^{1\times q_2} \xrightarrow{.R_2} D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \to 0,$$

y sea $f : M \to M \in End_D(M)$ definido por las matrices $P \in D^{p\times p}$ y $Q \in D^{q\times q}$ tales que $RP = QR$. Entonces, f es un idempotente si, y sólo si, existe una matriz $Z \in D^{p\times q}$ que satisface la igualdad

$$P^2 = P + ZR. \tag{3.4.1}$$

En tal caso, existe una matriz $Z' \in D^{q\times q_2}$ tal que

$$Q^2 = Q + RZ + Z'R_2. \tag{3.4.2}$$

En particular, si R es de rango de filas completo, es decir, $R_2 = 0$, entonces

$$Q^2 = Q + RZ. \tag{3.4.3}$$

Demostración. A partir de la igualdad $RP = QR$ obtenemos $RP^2 = QRP$, y de aquí, $RP^2 = Q^2R$, lo cual muestra que $f^2 : M \to M$ puede ser definido por las matrices P^2 y Q^2. Por la parte 1 del teorema 3.2.4, el homomorfismo $f^2 - f$ es nulo si, y sólo si, existen dos matrices $Z \in D^{p\times q}$ y $Z' \in D^{q\times q_2}$, las cuales satisfacen las condiciones (3.4.1) y (3.4.2). Esto finaliza la demostración. □

Lema 3.4.2. *Sea $P \in D^{p\times p}$ una matriz idempotente. Entonces las siguientes condiciones son equivalentes:*

1. $\ker(.P)$ *e* $Im(.P)$ *son libres de rangos m y $p - m$, respectivamente, donde* $1 \le m \le p$.

2. *Existe $U \in GL_p(D)$ tale que*

$$P = U^{-1}J_P U,$$

donde J_P tiene la forma

$$J_P = \begin{bmatrix} 0 & 0 \\ 0 & I_{p-m} \end{bmatrix}.$$

Además, U satisface

$$U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}, \quad U_1 \in D^{m\times p}, \quad U_2 \in D^{(p-m)\times p}$$

donde las matrices de rango de fila completo U_1, U_2 son las bases de los D-módulos libres $\ker(.P), Im(.P)$*, respectivamente, es decir,*

$$\ker(.P) = D^{1\times m}U_1, Im(.P) = D^{1\times(p-m)}U_2.$$

Demostración. Véase [6], Proposición 4.3. □

Podemos ya probar el resultado principal de la presente sección.

Teorema 3.4.3. *Sea $R \in D^{q\times p}, M := D^{1\times p}/(D^{1\times q}R)$, y $f : M \to M$ un D-endomorfismo idempotente definido por las matrices $P \in D^{p\times p}, Q \in D^{q\times q}$, las cuales satisfacen (3.1.1) y además son idempotentes. Si* $\ker(.P), Im(.P), \ker(.Q), Im(.Q)$ *son libres de rangos $m, p - m, l$, $q - l$, respectivamente, con $1 \le m \le p, 1 \le l \le q$, entonces:*

1. *Existen matrices $U \in GL_p(D)$ y $V \in GL_q(D)$ tales que*

$$\begin{cases} P = U^{-1}J_P U, \\ Q = V^{-1}J_Q V, \end{cases}$$

donde J_P *y* J_Q *son las matrices*

$$\begin{cases} J_P = \begin{bmatrix} 0 & 0 \\ 0 & I_{p-m} \end{bmatrix} \in D^{p\times p}, \\ J_Q = \begin{bmatrix} 0 & 0 \\ 0 & I_{q-l} \end{bmatrix} \in D^{q\times q}. \end{cases}$$

Además, las matrices U *y* V *satisfacen*

$$\begin{cases} U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}, \quad U_1 \in D^{m\times p}, \quad U_2 \in D^{(p-m)\times p} \\ V = \begin{bmatrix} V_1 \\ V_2 \end{bmatrix}, \quad V_1 \in D^{l\times q}, \quad V_2 \in D^{(q-l)\times q} \end{cases}$$

donde las matrices de rango de fila completo U_1, U_2, V_1, V_2 *son las bases de los* D*-módulos libres* $\ker(.P), Im(.P), \ker(.Q), Im(.Q)$*, respectivamente, es decir,*

$$\begin{cases} \ker(.P) = D^{1\times m}U_1, Im(.P) = D^{1\times(p-m)}U_2, \\ \ker(.Q) = D^{1\times l}V_1, Im(.Q) = D^{1\times(q-l)}V_2. \end{cases}$$

2. *La matriz* R *es equivalente a la matriz* $\overline{R} := VRU^{-1}$*.*

3. *Si denotamos* $U^{-1} = [W_1 \;\; W_2]$*, con* $W_1 \in D^{p\times m}, W_2 \in D^{p\times(p-m)}$*, entonces*

$$\overline{R} = \begin{bmatrix} V_1RW_1 & 0 \\ 0 & V_2RW_2 \end{bmatrix}. \tag{3.4.4}$$

Demostración. 1. El resultado se obtiene directamente del lema 3.4.2.

2. Evidente.

3. Según 1, podemos aplicar el lema 3.3.2 y obtener que $\overline{R}J_P = J_Q\overline{R}$. La matriz $\overline{R}$ se puede escribir en la forma

$$\overline{R} = \begin{bmatrix} \overline{R}_{11} & \overline{R}_{12} \\ \overline{R}_{21} & \overline{R}_{22} \end{bmatrix},$$

con $\overline{R}_{11} \in D^{l\times m}, \overline{R}_{12} \in D^{l\times(p-m)}, \overline{R}_{21} \in D^{(q-l)\times m}, \overline{R}_{22} \in D^{(q-l)\times(p-m)}$, luego

$$\overline{R}J_P = \begin{bmatrix} 0 & \overline{R}_{12} \\ 0 & \overline{R}_{22} \end{bmatrix} \text{ y } J_Q\overline{R} = \begin{bmatrix} 0 & 0 \\ \overline{R}_{21} & \overline{R}_{22} \end{bmatrix},$$

con lo cual $\overline{R}_{12} = 0$ y $\overline{R}_{21} = 0$. Ya que $V_1RW_1 \in D^{l\times m}, V_2RW_1 \in D^{(q-l)\times m}, V_1RW_2 \in D^{l\times(p-m)}, V_2RW_2 \in D^{(q-l)\times(p-m)}$, entonces

$$\overline{R} = \begin{bmatrix} \overline{R}_{11} & 0 \\ 0 & \overline{R}_{22} \end{bmatrix} = VRU^{-1} = \begin{bmatrix} V_1RW_1 & V_1RW_2 \\ V_2RW_1 & V_2RW_2 \end{bmatrix} = \begin{bmatrix} V_1RW_1 & 0 \\ 0 & V_2RW_2 \end{bmatrix}.$$

□

3.5 Descripción del espacio de soluciones

Concluimos este capítulo con un teorema relativo a la descripción del módulo de $\mathcal{F}$-soluciones de un sistema lineal funcional, en el caso en que el módulo asociado disponga de un endomorfismo idempotente no trivial.

Para el teorema central necesitamos dos resultados preliminares.

Lema 3.5.1. *Sean $R \in D^{q\times p}$, $M = D^{1\times p}/(D^{1\times q}R)$ y $f : M \to M$ un D-endomorfismo definido por las matrices $P \in D^{p\times p}$ y $Q \in D^{q\times q}$ tales que $RP = QR$. Entonces, las siguientes afirmaciones son equivalentes:*

1. *f es un idempotente.*

2. *Existe $X \in D^{p\times r}$ tal que*
$$P = I_p - XS, \tag{3.5.1}$$
donde $S \in D^{r\times p}$ es la matriz definida en la proposición 3.1.2.

En tal caso, el siguiente diagrama es conmutativo, exacto y la tercera columna es hendida:

$$\begin{tikzcd}
 & & 0 \arrow[d] & \\
D^{1\times r} \arrow[r, ".S"] \arrow[d, ".T"] & D^{1\times p} \arrow[r, "\kappa"] \arrow[d, ".P"] & Coim(f) \arrow[r] \arrow[d, "f^{\#}"] & 0 \\
D^{1\times q} \arrow[r, ".R"] & D^{1\times p} \arrow[r, "\pi"] & M \arrow[r] \arrow[d, "id_M - f"] & 0 \\
 & & \ker(f) \arrow[d] & \\
 & & 0 &
\end{tikzcd}$$

con κ como en (3.2.2), T como en (3.2.1) y $f^{\#}$ es definido mediante la sucesión exacta corta hendida
$$0 \to \ker(f) \xrightarrow{i} M \xrightarrow{\rho} Coim(f) \to 0, \tag{3.5.2}$$
$$f^{\#}(\rho(m)) := f(m),\ m \in M.$$

Demostración. Véase [6], Proposición 4.1. □

Proposición 3.5.2. *Sean $R \in D^{q\times p}$ y $S \in D^{r\times p}$ matrices tales que $(D^{1\times q}R) \subseteq (D^{1\times r}S)$. Entonces, $M' := D^{1\times p}/(D^{1\times r}S)$ es isomorfo a un sumando directo de $M := D^{1\times p}/(D^{1\times q}R)$, esto es,*

$$M \cong M' \oplus \ker(\rho), \tag{3.5.3}$$

si, y sólo si, existen dos matrices $X \in D^{p\times r}, T \in D^{r\times q}$ tales que

$$S - SXS = TR, \tag{3.5.4}$$

con $\rho : M \to M'$ definido por $\rho(\pi(\lambda)) := \kappa(\lambda)$, $\lambda \in D^{1\times p}$, y $\pi : D^{1\times p} \to M$, $\kappa : D^{1\times p} \to M'$ los homomorfismos canónicos.

Demostración. Véase [6], Proposición 4.2. □

Probaremos entonces el teorema central sobre factorización de sistemas lineales funcionales y el cálculo de las $\mathcal{F}$-soluciones dado por $\ker_{\mathcal{F}}(R.)$.

Teorema 3.5.3. *Sean $R \in D^{q\times p}$, $M := D^{1\times p}/(D^{1\times q}R)$ y $f \in End_D(M)$ un idempotente no trivial definido por matrices $P \in D^{p\times p}$ y $Q \in D^{q\times q}$ tales que $RP = QR$. Además, sean $S \in D^{r\times p}, L \in D^{q\times r}, X \in D^{p\times r}$ y $S_2 \in D^{r_2\times r}$ matrices tales que*

$$\begin{cases} Coim(f) = D^{1\times p}/(D^{1\times r}S), \\ R = LS, \\ I_p - P = XS, \\ \ker(.S) = D^{1\times r_2}S_2. \end{cases}$$

Si $\mathcal{F}$ es un D-módulo inyectivo, entonces cualquier solución $\eta \in \mathcal{F}^p$ de $R\eta = 0$ tiene la forma $\eta = \zeta + X\tau$, donde $\zeta \in \mathcal{F}^p$ es una solución de $S\zeta = 0$ y $\tau \in \mathcal{F}^r$ es una solución del sistema

$$\begin{cases} L\tau = 0, \\ S_2\tau = 0. \end{cases} \tag{3.5.5}$$

La integración del sistema $R\eta = 0$ es equivalente a la integración de los dos sistemas independientes $S\zeta = 0$ y (3.5.5).

Demostración. Para comenzar observemos primero que las condiciones impuestas a S fueron dadas en el lema 3.5.1, la proposición 3.1.2 y el corolario 3.2.3.

Aplicando el funtor $Hom_D(\ ,\mathcal{F})$ al diagrama conmutativo exacto (3.2.2), del teorema de Malgrange (teorema 2.2.1), y dado que $\mathcal{F}$ es un D-módulo inyectivo, obtenemos el siguiente diagrama conmutativo exacto:

$$\begin{tikzcd}
0 \arrow[r] & \ker_{\mathcal{F}}(R.) \arrow[r] & \mathcal{F}^p \arrow[r, "R."] & \mathcal{F}^q & \\
0 \arrow[r] & \ker_{\mathcal{F}}(S.) \arrow[r] \arrow[u, "\rho^*"'] & \mathcal{F}^p \arrow[r, "S."] \arrow[u, "="'] & \mathcal{F}^r \arrow[r, "S_2."] \arrow[u, "L."'] & \mathcal{F}^{r_2}
\end{tikzcd}$$

Veamos primero que cualquier elemento de la forma $\eta = \zeta + X\tau$, donde $\zeta \in \mathcal{F}^p$ satisface $S\zeta = 0$ y $\tau \in F^r$ satisface (3.5.5), es una solución de $R\eta = 0$: dado que $R = LS$ y $S\zeta = 0$, tenemos que

$$R\eta = R\zeta + R(X\tau) = L(S\zeta) + R(X\tau) = R(X\tau).$$

Puesto que τ satisface la segunda ecuación de (3.5.5), y considerando la exactitud de la última sucesión horizontal en el diagrama anterior, entonces existe $\overline{\eta} \in \mathcal{F}^p$ tal que $\tau = S\overline{\eta}$. Sustituyendo esta relación en la primera igualdad de (3.5.5), obtenemos

$$0 = L\tau = L(S\overline{\eta}) = R\overline{\eta}.$$

Así, por (3.5.1) y la relación $RP = QR$, tenemos

$$\overline{\eta} - P\overline{\eta} = XS\overline{\eta} = X\tau \Rightarrow R\overline{\eta} - RP\overline{\eta} = R(X\tau) \Rightarrow R(X\tau) = R\overline{\eta} - QR\overline{\eta} = 0.$$

Este último resultado prueba que $R\eta = R(X\tau) = 0$, es decir, que $\zeta + X\tau$ es una solución del sistema $R\eta = 0$.

Veamos ahora que cualquier solución $\eta \in \mathcal{F}^p$ de $R\eta = 0$ tiene la forma $\eta = \zeta + X\tau$, donde $\zeta \in \mathcal{F}^P$ satisface $S\zeta = 0$ y $\tau \in \mathcal{F}^r$ satisface (3.5.5). Consideremos $\eta \in \mathcal{F}^p$ tal que $R\eta = 0$, esto es, $(LS)\eta = 0$. Por el diagrama conmutativo anterior, tenemos que el elemento $\tau \in \mathcal{F}^r$ definido por $\tau := S\eta$, satisface (3.5.5). Por tanto, de (3.5.4) obtenemos que el elemento $\zeta := \eta - X\tau$ cumple

$$S\zeta = S\eta - S(X(S\eta)) = T(R\eta) = 0.$$

□

Capítulo 4

Bases de Gröbner y aplicaciones

Los cálculos efectivos involucrados en los resultados presentados en los capítulos 2 y 3 requieren del uso de bases de Gröbner o de librerías y paquetes de cómputo que utilizan dichas bases. En este último capítulo vamos a presentar los principales ingredientes de la teoría no conmutativa de las bases de Gröbner para las extensiones PBW torcidas y su aplicación para realizar algunos de los cálculos mencionados anteriormente. La teoría completa puede ser consultada en [21] y ha sido implementada para `MAPLE` mediante librerías en [8]. Para otros cálculos de los capítulos 2 y 3 también se usará la teoría particular de bases de Gröbner para álgebras de Ore que ha sido desarrollada en [6] e implementada para `MAPLE` en [5]. La teoría no conmutativa de la bases de Gröbner también puede ser consultada en [3], [15] y [23] y las implementaciones para `SINGULAR` en [13]. En la última sección del capítulo ilustraremos con ejemplos concretos sobre álgebras de Ore algunos de los resultados haciendo uso de estas herramientas computacionales.

4.1 Inventario de matrices y objetos a calcular

En esta primera sección haremos un inventario de las matrices y demás objetos algebraicos que deben ser efectivamente calculados para que los resultados presentados en los capítulos anteriores sean no solo teóricamente interesantes sino también puedan ser implementados y aplicados.

1. Establecer de manera efectiva si un SLF es autónomo, controlable, parametrizable, mediante el cálculo de la torsión $t(M)$ de su módulo asociado M. Para esto, calcular $Ext_D^1(M^T, D)$ y el dual M^*. Véase las definiciones 2.1.14 - 2.3.1, los teoremas 2.3.2 - 2.3.3 y los corolarios 2.3.4 - 2.3.5.

2. Cálculo de la matriz Q de parametrización de un SLF parametrizable. Véase la definición 2.3.1.

3. Cálculo de la inversa a izquierda de la matriz Q, cuando la parametrización del sistema es inyectiva, definición 2.3.1. También la inversas a izquierda de la matrices del teorema 3.2.4. De manera más general, esta tarea induce el cálculo de la inversa a izquierda de una matriz.

4. Cálculo de las matrices P y Q de (3.1.1) en la proposición 3.1.1.

5. Cálculo de $Hom_D(M, M')$ cuando M y M' son módulos de presentación finita. Véase la proposición 3.1.1.

6. Dada una matriz $R \in D^{q\times p}$, cálculo de $\ker(.R)$. De forma más general, cálculo del módulo de sicigias de un submódulo finitamente generado de $D^{1\times q}$. Véase la proposición 3.1.2.

7. Cálculo de las matrices S y T en la proposición 3.1.2

8. Dadas las matrices R y S, cálculo de la matriz L para la factorización $R = LS$ en los teoremas 3.2.1 y 3.2.4.

9. Cálculo de las matrices Z y F en el teorema 3.2.4. Este cálculo se puede abordar de manera más general como un problema de membresía mediante el algoritmo de división.

10. Para dos módulos de presentación finita M y M' y $f \in Hom_D(M, M')$, determinar mediante el punto anterior, si f es inyectivo, sobreyectivo, biyectivo.

11. Calculo de las matrices U y V de la proposición 3.3.1 y el teorema 3.3.4, y así, calcular la forma triangular $\overline{R}$ en el teorema 3.3.4.

12. Calculo de las matrices U y V del teorema 3.4.3, y con esto, calcular la forma diagonal $\overline{R}$ en dicho teorema.

13. Cálculo de espacio de soluciones $\ker_{\mathcal{F}}(.R)$. Para este propósito, calcular las matrices X y S_2 en el lema 3.5.1 y el teorema 3.5.3.

4.2 Bases de Gröbner

Los resultados constructivo-matriciales presentados en los capítulos 2 y 3 fueron probados en general para dominios noetherianos tanto a izquierda como a derecha (véase por ejemplo los teoremas 2.3.2 - 2.3.3 y la introducción al capítulo 3). Sin embargo, para realizar los cálculos requeridos en la sección anterior es necesario asumir que D sea un anillo de tipo polinomial y así poder utilizar como herramienta la teoría de bases Gröbner. Esta teoría computacional ha sido suficientemente estudiada y desarrollada de manera general para anillos no conmutativos de tipo polinomial (véase por ejemplo [3], [11], [15], [21], [23]).

A pesar de que la mayor parte de los ejemplos concretos de SLF son sobre extensiones de Ore (véase la sección 4.5 más adelante) y las teoría de Gröbner para este caso particular es bien conocida, la teoría de bases de Gröbner que presentaremos de manera muy resumida en la presente sección será para extensiones PBW torcidas biyectivas. La razón para hacerlo de esta manera general es pensando en el problema 4.5.5 y también considerando que estas extensiones generalizan las de Ore de tipo biyectivo, y además cubren los ejemplos notables de SLF.

Incluir de manera completa en la presente monografía la teoría de las bases de Gröbner para las extensiones PBW torcidas ocuparía demasiado espacio (véase la parte III del libro [21]). Nosotros presentaremos solo los *ingredientes principales* y remitimos al lector a [21] para las pruebas y todos los detalles.

En esta sección $A = \sigma(R)\langle x_1, \dots, x_n\rangle$ denotará una extensión PBW torcida biyectiva de un anillo R. No debe presentar confusión el anillo R de coeficientes de la extensión A con la notación que usamos en los capítulos 2 y 3 para la matriz de un sistema lineal funcional. $Mon(A)$ denotará el conjunto de monomios estándar de A (véase la definición 1.3.3). En adelante usaremos también la siguiente notación.

Definición 4.2.1. *Sea σ_i como en la proposición 1.3.4, $1 \leq i \leq n$.*

(i) *Para $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, denotamos $\sigma^\alpha := \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n}$, $|\alpha| := \alpha_1 + \cdots + \alpha_n$. Si $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, entonces $\alpha + \beta := (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$.*

(ii) *Para $X = x^\alpha \in Mon(A)$, $\exp(X) := \alpha$ y $\deg(X) := |\alpha|$.*

(iii) *Sea $0 \neq f \in A$, $t(f)$ es el conjunto finito de términos que conforman f, es decir, si $f = c_1X_1 + \cdots + c_tX_t$, con $X_i \in Mon(A)$ y $c_i \in R - \{0\}$, entonces $t(f) := \{c_1X_1, \dots, c_tX_t\}$.*

(iv) *Sea f como en (iii), entonces $\deg(f) := \max\{\deg(X_i)\}_{i=1}^t$.*

Usaremos la siguiente caracterización de las extensiones PBW torcidas.

Teorema 4.2.2. *Sea A un anillo polinomial a izquierda sobre R con respecto a $\{x_1, \dots, x_n\}$. Entonces, A es una extensión PBW torcida de R si, y sólo si, se cumplen las siguientes condiciones:*

(a) *Para cada $x^\alpha \in Mon(A)$ y cada $0 \neq r \in R$ existen elementos únicos $r_\alpha := \sigma^\alpha(r) \in R - \{0\}$ y $p_{\alpha,r} \in A$ tales que:*

$$x^\alpha r = r_\alpha x^\alpha + p_{\alpha,r}, \tag{4.2.1}$$

donde $p_{\alpha,r} = 0$ ó $\deg(p_{\alpha,r}) < |\alpha|$ si $p_{\alpha,r} \neq 0$. Además, si r es invertible a izquierda, entonces r_α es invertible a izquierda.

(b) *Dados* $x^\alpha, x^\beta \in Mon(A)$ *existen* $c_{\alpha,\beta} \in R$ *y* $p_{\alpha,\beta} \in A$ *únicos tales que*

$$x^\alpha x^\beta = c_{\alpha,\beta} x^{\alpha+\beta} + p_{\alpha,\beta}, \tag{4.2.2}$$

donde $c_{\alpha,\beta}$ *es invertible a izquierda,* $p_{\alpha,\beta} = 0$ *ó* $\deg(p_{\alpha,\beta}) < |\alpha+\beta|$ *si* $p_{\alpha,\beta} \neq 0$.

A continuación presentamos en forma muy resumida los principales ingredientes de la teoría de las bases de Gröbner.

1. Órdenes monomiales en $Mon(A)$.

   Sea $\succeq$ un orden total definido en $Mon(A)$. Si $x^\alpha \succeq x^\beta$ pero $x^\alpha \neq x^\beta$ se escribe $x^\alpha \succ x^\beta$. $x^\beta \preceq x^\alpha$ siginifica que $x^\alpha \succeq x^\beta$. Sea $f \neq 0$ un polinomio de A, si $f = c_1 X_1 + \cdots + c_t X_t$, con $c_i \in R - \{0\}$ y $X_1 \succ \cdots \succ X_t$ los monomios de f, entonces $lm(f) := X_1$ es el ***monomio principal*** de f, $lc(f) := c_1$ es el ***coeficiente principal*** de f y $lt(f) := c_1 X_1$ es el ***término principal*** de f. Si $f = 0$, se define $lm(0) := 0, lc(0) := 0, lt(0) := 0$, y $X \succ 0$ para cada $X \in Mon(A)$.

   Definición 4.2.3. *Sea* $\succeq$ *un orden total en* $Mon(A)$*, se dice que* $\succeq$ *es un* ***orden monomial*** *sobre* $Mon(A)$ *si se cumplen las siguientes condiciones:*

   (i) *Para cualesqueira* $x^\beta, x^\alpha, x^\gamma, x^\lambda \in Mon(A)$

   $$x^\beta \succeq x^\alpha \Rightarrow lm(x^\gamma x^\beta x^\lambda) \succeq lm(x^\gamma x^\alpha x^\lambda).$$

   (ii) $x^\alpha \succeq 1$*, para cada* $x^\alpha \in Mon(A)$.

   (iii) $\succeq$ *compatible, es decir,* $|\beta| \geq |\alpha| \Rightarrow x^\beta \succeq x^\alpha$.

   Los órdenes monomiales se conocen también como ***órdenes admisibles***.

   Proposición 4.2.4. *Cada orden monomial sobre* $Mon(A)$ *es un buen orden.*

   En adelante asumiremos que $Mon(A)$ está dotado con un orden monomial.

   Definición 4.2.5. *Sea* $x^\alpha, x^\beta \in Mon(A)$*, se dice que* x^α ***divide*** *a* x^β*,* $x^\alpha \mid x^\beta$*, si existen* $x^\gamma, x^\lambda \in Mon(A)$ *tales que* $x^\beta = lm(x^\gamma x^\alpha x^\lambda)$*. Cada monomio de* $Mon(A)$ *divide al polinomio nulo.*

   Observación 4.2.6. (i) Se puede probar que $x^\alpha \mid x^\beta$ si, y sólo si, existe $\alpha' \in \mathbb{N}^n$ tal que $\beta = \alpha' + \alpha$.

   (ii) En $Mon(A)$ cada par de elementos tiene ***mínimo común múltiplo***: en efecto, si $x^\alpha, x^\beta \in Mon(A)$, entonces

   $$lcm(x^\alpha, x^\beta) = x^\gamma, \text{ con } \gamma := (\gamma_1, \ldots, \gamma_n),\ \gamma_i := \max\{\alpha_i, \beta_i\},\ 1 \leq i \leq n.$$

2. Reducción en A.

Definición 4.2.7. *Sea F un conjunto finito de elementos no nulos de A, y sean $f, h \in A$. Se dice que f se* ***reduce*** *a h mediante F en un paso, lo cual se denota por $f \xrightarrow{F} h$, si existen $f_1, \ldots, f_t \in F$ y $r_1, \ldots, r_t \in R$ tales que:*

(i) *$lm(f_i) \mid lm(f)$, $1 \leq i \leq t$, es decir, existe $x^{\alpha_i} \in Mon(A)$ tal que $\alpha_i + \exp(lm(f_i)) = \exp(lm(f))$.*

(ii) *$lc(f) = r_1\sigma^{\alpha_1}(lc(f_1))c_{\alpha_1,f_1} + \cdots + r_t\sigma^{\alpha_t}(lc(f_t))c_{\alpha_t,f_t}$, donde c_{α_i,f_i} son como en el teorema 4.2.2, es decir, $c_{\alpha_i,f_i} := c_{\alpha_i,\exp(lm(f_i))}$.*

(iii) *$h = f - \sum_{i=1}^{t} r_i x^{\alpha_i} f_i$.*

Se dice que f se reduce a h mediante F, lo cual se denota por $f \xrightarrow{F}_+ h$, si existen $h_1, \ldots, h_{t-1} \in A$ tales que

$$f \xrightarrow{F} h_1 \xrightarrow{F} h_2 \xrightarrow{F} \cdots \xrightarrow{F} h_{t-1} \xrightarrow{F} h.$$

f es ***reducido*** *(también llamado* ***minimal****) con respecto a F si $f = 0$ o alguna de las condiciones (i) o (ii) no se cumple. En caso contrario se dice que f es* ***reducible*** *con respecto a F. Si $f \xrightarrow{F}_+ h$ y h es reducido, entonces se dice que h es un* ***residuo*** *para f con respecto a F. Por definición, $0 \xrightarrow{F} 0$.*

En cualquier versión de la teoría de bases de Gröbner es clave el ingrediente de reducción. En nuestra definición resulta necesario imponer condiciones computationales al anillo R de coeficientes para poder resolver ecuaciones lineales en R, tal como se observó en la condición (ii) de la definición 4.2.7.

Definición 4.2.8. *Un anillo R es* ***Gröbner soluble a izquierda*** *(LGS) si se cumplen las siguientes condiciones:*

(i) *R es noetheriano a izquierda.*

(ii) *Dados $a, r_1, \ldots, r_m \in R$ existe un algoritmo que permita decidir si a pertenece al ideal izquierdo $Rr_1 + \cdots + Rr_m$, y en caso afirmativo, calcular $b_1, \ldots, b_m \in R$ tales que $a = b_1r_1 + \cdots + b_mr_m$.*

(iii) *Dados $r_1, \ldots, r_m \in R$ existe un algoritmo que permita encontrar un conjunto finito de generadores para el R-módulo izquierdo*

$$Syz_R[r_1 \ \cdots \ r_m] := \{(b_1, \ldots, b_m) \in R^m \mid b_1r_1 + \cdots + b_mr_m = 0\}.$$

Observación 4.2.9. En adelante asumiremos que A es una extension PBW torcida biyectiva de R (véase las definiciones 1.3.3 y 1.3.5), donde R satisface las siguientes condiciones: (a) R es un dominio (b) R es LGS. (c) R es noetheriano a derecha. Bajo estas hipótesis, es conocido que A es también un dominio noetheriano a ambos lados (véase [21] para las propiedades de anillos y módulos y las propiedades homológicas de las extensiones PBW torcidas).

3. Algoritmo de la división.

Teorema 4.2.10. *Sea $F = \{f_1, \ldots, f_t\}$ un conjunto finito de polinomios no nulos de A y sea $f \in A$. Entonces, el siguiente* ***algoritmo de división*** *produce polinomios $q_1, \ldots, q_t, h \in A$, con h reducido respecto de F, tales que $f \xrightarrow{F}_+ h$ y*

$$f = q_1 f_1 + \cdots + q_t f_t + h,$$

con

$$lm(f) = \max\{lm(lm(q_1)lm(f_1)), \ldots, lm(lm(q_t)lm(f_t)), lm(h)\}.$$

Division algorithm in A

INPUT: $f, f_1, \ldots, f_t \in A$ *with* $f_j \neq 0\,(1 \leq j \leq t)$

OUTPUT: $q_1, \ldots, q_t, h \in A$ *with* $f = q_1 f_1 + \cdots + q_t f_t + h$, h *reduced w.r.t.* $\{f_1, \ldots, f_t\}$ *and* $lm(f) = \max\{lm(lm(q_1)lm(f_1)), \ldots, lm(lm(q_t)lm(f_t)), lm(h)\}$

INITIALIZATION: $q_1 := 0, q_2 := 0, \ldots, q_t := 0, h := f$

WHILE $h \neq 0$ *and there exists* j *such that* $lm(f_j)$ *divides* $lm(h)$ **DO**

  Calculate $J := \{j \mid lm(f_j) \text{ divides } lm(h)\}$

  FOR $j \in J$ **DO**

    Calculate $\alpha_j \in \mathbb{N}^n$ *such that* $\alpha_j + \exp(lm(f_j)) = \exp(lm(h))$

  IF *the equation* $lc(h) = \sum_{j\in J} r_j \sigma^{\alpha_j}(lc(f_j))c_{\alpha_j, f_j}$ *is soluble, where* c_{α_j, f_j} *are defined as in Theorem 4.2.2* **THEN**

    Calculate one solution $(r_j)_{j\in J}$

    $h := h - \sum_{j\in J} r_j x^{\alpha_j} f_j$

    FOR $j \in J$ **DO**

      $q_j := q_j + r_j x^{\alpha_j}$

  ELSE

    Stop

Ejemplos concretos de ilustración del algoritmo han sido realizados a mano en [21]. El algoritmo por supuesto puede ser aplicado para álgebras y extensiones de Ore de tipo biyectivo. En la sección 4.4 veremos que este algoritmo ha sido implementado para `MAPLE` en [8].

4. Bases de Gröbner de ideales izquierdos.

   Definiremos ahora las bases de Gröbner para los ideales izquierdos de las extensiones PBW torcidas.

   Definición 4.2.11. *Sea $I \neq 0$ un ideal izquierdo de A y sea G un conjunto finito no vacío de polinomios no nulos de I. Se dice que G es una* ***base de Gröbner*** *de I si cada elemento $0 \neq f \in I$ es reducible respecto de G. $\{0\}$ es una base de Gröbner para $I = 0$.*

   Teorema 4.2.12. *Sea $I \neq 0$ un ideal izquierdo de A y sea G un conjunto finito no vacío de polinomios no nulos de I. Entonces las siguientes condiciones son equivalentes:*

   (i) *G es una base de Gröbner de I.*

   (ii) *Para cada polinomio $f \in A$,*

   $$f \in I \text{ si, y sólo si, } f \xrightarrow{G}_{+} 0.$$

   Corolario 4.2.13. *Sea $I \neq 0$ un ideal izquierdo de A.*

   (i) *Si G es una base de Gröbner de I, entonces $I = \langle G\}$ (ideal izquierdo de A generado por G).*

   (ii) *Sea G una base de Gröbner de I, si $f \in I$ y $f \xrightarrow{G}_{+} h$, con h reducido, entonces $h = 0$.*

5. Algoritmo de Buchberger.

   Veremos a continuación que cada ideal izquierdo de A tiene bases de Gröbner y mostraremos un algoritmo para calcularlas.

   Definición 4.2.14. *Sea $F := \{g_1, \dots, g_s\} \subseteq A$, X_F el mínimo común múltiplo de $\{lm(g_1), \dots, lm(g_s)\}$, $\theta \in \mathbb{N}^n$, $\beta_i := \exp(lm(g_i))$ y $\gamma_i \in \mathbb{N}^n$ de tal forma que $\gamma_i + \beta_i = \exp(X_F)$, $1 \leq i \leq s$. Sea $B_{F,\theta}$ un conjunto finito de generadores en R^s de*

   $$S_{F,\theta} := Syz_R[\sigma^{\gamma_1+\theta}(lc(g_1))c_{\gamma_1+\theta,\beta_1} \ \cdots \ \sigma^{\gamma_s+\theta}(lc(g_s))c_{\gamma_s+\theta,\beta_s})].$$

   Para $\theta = \mathbf{0} := (0, \dots, 0)$, $S_{F,\theta}$ será denotado por S_F y $B_{F,\theta}$ por B_F.

Teorema 4.2.15. *Sea $F = \{f_1, \dots, f_s\}$ un conjunto finito de polinomios no nulos de A. El siguiente algoritmo produce una base de Gröbner para el ideal izquierdo $\langle F\}$ de A ($P(X)$ denota la colección de subconjuntos de X):*

Buchberger's algorithm for
bijective skew PBW extensions

INPUT: $F := \{f_1, \dots, f_s\} \subseteq A,\ f_i \neq 0,\ 1 \leq i \leq s$

OUTPUT: $G = \{g_1, \dots, g_t\}$ *a Gröbner basis for* $\langle F\}$

INITIALIZATION: $G := \emptyset, G' := F$

WHILE $G' \neq G$ **DO**

$D := P(G') - P(G)$

$G := G'$

FOR *each* $S := \{g_{i_1}, \dots, g_{i_k}\} \in D$ **DO**

Compute B_S

FOR *each* $\boldsymbol{b} = (b_1, \dots, b_k) \in B_S$ **DO**

Reduce $\sum_{j=1}^k b_j x^{\gamma_j} g_{i_j} \xrightarrow{G'}_+ r$, *with r reduced with respect to G' and γ_j defined as in Definition 4.2.14*

IF $r \neq 0$ **THEN** $G' := G' \cup \{r\}$

Corolario 4.2.16. *Cada ideal izquierdo de A tiene una base de Gröbner.*

Ejemplos concretos de ilustración del algoritmo de Buchberger han sido realizados a mano en [21] para álgebras que son extensiones PBW torcidas y que incluyen como caso particular las extensiones y álgebras de Ore de tipo biyectivo. En la sección 4.4 veremos que este algoritmo también ha sido implementado para `MAPLE` en [8].

6. Bases de Gröbner de submódulos de $A^{1\times q}$, $q \geq 1$.

   La teoría de bases de Gröbner que presentamos en los numerales anteriores puede ser generalizada a los submódulos del A-módulo izquierdo libre $A^{1\times q}$, $q \geq 1$. Notemos que para $q = 1$ obtenemos los ideales izquierdos de A. Invitamos a los lectores a consultar en [21] la construcción completa ya que la teoría de Gröbner de submódulos es la que se aplica principalmente en los cálculos matriciales de la sección 4.1 y que realizaremos en la próxima sección.

7. Extensiones PBW torcidas a derecha y bases de Gröbner a derecha.

   A pesar que la teoría constructiva que estudiamos en los capítulo 2 y 3 y que la mayoría de los cálculos matriciales que señalamos en la sección 4.1 corresponden a módulos a izquierda, algunas construcciones involucran módulos a derecha, por ejemplo, el módulo dual M^* es un D-módulo derecho, lo mismo que M^T (véase el numeral 1 de la sección 4.1). Es conveniente por lo tanto anotar que existe la teoría de bases de Gröbner para módulos a derecha y la noción de extensiones PBW torcidas a derecha, es decir, disponiendo los coeficientes de la extensión A por el lado derecho (véase [21]). Puesto que estamos asumiendo que las extensiones son biyectivas, entonces en [21] se establece que toda extensión a izquierda se puede interpretar también como una extensión a derecha; si además asumimos que el anillo R de coeficientes es también Gröbner soluble a derecha, entonces para una extensión A podemos contar con todos los resultados de la teoría de bases de Gröbner para módulos derechos sobre A. Se debe señalar que en todos los ejemplos notables de extensiones PBW torcidas el anillo de coeficientes es un dominio Gröbner soluble a ambos lados (por ejemplo, un cuerpo, un anillo de polinomios con coeficientes en un cuerpo, etc), véase el capítulo 2 de [21].

Observación 4.2.17. Teniendo en cuenta que el anillo habitual de polinomios y las extensiones de Ore de tipo biyectivo son ejemplos de extensiones PBW torcidas biyectivas, entonces la teoría de bases de Gröbner que hemos presentado puede ser aplicada a esos dos casos particulares. Así, la teoría clásica de bases de Gröbner de los anillos de polinomios conmutativos con coeficientes en cuerpos queda cubierta con lo que hemos presentado.

4.3 Cálculos matriciales usando bases de Gröbner

Con las herramientas de bases de Gröbner presentadas en la sección anterior es posible realizar los cálculos señalados en la sección 4.1. Nos disponemos ahora a mostrar algunos de esos cálculos mediante procedimientos y algoritmos los cuales incluyen el uso de las bases Gröbner. Asumiremos que $D := A = \sigma(R)\langle x_1, \ldots, x_n\rangle$ es una extensión PBW torcida biyectiva de un dominio R el cual es Gröbner soluble a ambos lados (véase la observación 4.2.9 y el numeral 7 al final de la sección anterior).

A. El problema de la membresía.

   Sea $F := \{f_1, \ldots, f_s\} \subset A$ e $I := \langle F\rangle$ el ideal izquierdo de A generado por F. El problema de la membresía consiste en determinar si se puede de manera efectiva decidir si un elemento f de A pertenece a I. La teoría de bases de Gröbner proporciona una forma fácil de responder a esta pregunta. En efecto, sea G una base de Gröbner de I (véase el corolario 4.2.16); haciendo uso del algoritmo de la división (teorema 4.2.10) es posible obtener polinomios $h_1, \dots, h_t, h \in A$, con h reducido respecto de G, tal que $f \xrightarrow{G}_+ h$ y $f = q_1 f_1 + \cdots + q_t f_t + h$, pero según el corolario 4.2.13, si $h \neq 0$, entonces $f \notin I$, y si $h = 0$, entonces $f \in I$.

El problema de la membresía puede ser extendido a submódulos de $A^{1\times q}$: sea $F := \{\boldsymbol{f}_1, \dots, \boldsymbol{f}_s\}$ un conjunto finito de vectores no nulos de $A^{1\times q}$ y $M := \langle \boldsymbol{f}_1, \dots, \boldsymbol{f}_s \rangle$ el A-submódulo de $A^{1\times q}$ generado por $\boldsymbol{f}_1, \dots, \boldsymbol{f}_s$; sea $G = \{\boldsymbol{g}_1, \dots, \boldsymbol{g}_t\}$ una base de Gröbner para M y $\boldsymbol{f} \in A^{1\times q}$; con el algoritmo de la división encontramos $l_1, \dots, l_t \in A$ y $\boldsymbol{h} \in A^{1\times q}$ reducido respecto de F tal que $\boldsymbol{f} = l_1 \boldsymbol{g}_1 + \cdots + l_t \boldsymbol{g}_t + \boldsymbol{h}$; luego, $\boldsymbol{f} \in M$ si, y sólo si, $\boldsymbol{h} = \boldsymbol{0}$.

El siguiente teorema complementa lo anterior y permite expresar $\boldsymbol{f}$ como A-combinación lineal de $\boldsymbol{f}_1, \dots, \boldsymbol{f}_s$ cuando $\boldsymbol{f} \in M$. La prueba consiste en aplicar el algoritmo de Buchberger para módulos (véase [21], capítulo 15).

Teorema 4.3.1. *Sea $F = \{\boldsymbol{f}_1, \dots, \boldsymbol{f}_s\}$ un subconjunto finito de vectores no nulos de $A^{1\times q}$ y $G = \{\boldsymbol{g}_1, \dots, \boldsymbol{g}_t\}$ una base de Gröbner de $M := \langle F \rangle$. Entonces, existen matrices $H \in A^{t\times s}$ y $Q \in A^{s\times t}$ tales que*

$$G = HF \text{ and } F = QG, \tag{4.3.1}$$

donde $G := (\boldsymbol{g}_1, \dots, \boldsymbol{g}_t)^T \in A^{t\times q}$ y $F := (\boldsymbol{f}_1, \dots, \boldsymbol{f}_s)^T \in A^{s\times q}$.

Observación 4.3.2. El problema de membresía y el teorema 4.3.1 permiten realizar el cálculo 9 de la sección 4.1. En efecto, dadas las matrices $P \in A^{p\times p'}$ y $R' \in A^{q'\times p'}$ se debe calcular $Z \in A^{p\times q'}$ de tal forma que $P = ZR'$, pero esto es equivalente a probar que $(D^{1\times p}P) \subseteq (D^{1\times q'}R')$, es decir, que cada fila de P pertenece al A-módulo generado por las filas de R'. Para esto calculamos una base de Gröbner G' para el módulo generado por las filas de R', tenemos entonces que $\langle G' \rangle = \langle R' \rangle$ y

$$\langle P \rangle \subseteq \langle R' \rangle \Leftrightarrow \langle P \rangle \subseteq \langle G' \rangle.$$

Tomamos cada fila de P y aplicamos el algoritmo de la división con los elementos de G', si algún residuo es no nulo, entonces tal matriz Z no existe. Si cada residuo es nulo, entonces existe una matriz L conformada por los polinomios cociente que resultan en el agoritmo de división tal que $P = LG'$, aplicamos el teorema 4.3.1 y encontramos una matriz H tal que $G' = HR'$, por lo tanto, la matriz Z existe y es dada por $Z := LH$. De otra parte, para el cálculo de la matriz F en el teorema 3.2.4, dada la matriz S, F satisface $S = FR$ si, y sólo si, el módulo generado por las filas de S está incluido en el módulo generado por las filas de R. Procedemos entonces como vimos para el cálculo de Z.

Otra eventual aplicación del procedimiento de membresía es realizar el cálculo 2 de la sección 4.1 ya que $\mathcal{B}$ y $\mathcal{F}^m$ son módulos y la matriz Q de parametrización satisface $\mathcal{B} = Q\mathcal{F}^m$.

B. Cálculo de sicigias.

Sea $M := \langle \boldsymbol{f}_1, \ldots, \boldsymbol{f}_s \rangle$ un submódulo finitamente generado de $A^{1\times q}$. Recordemos que el ***módulo de sicigias*** de M, denotado $Syz(M)$, está conformado por los vectores $\boldsymbol{h} = (h_1, \ldots, h_s) \in A^{1\times s}$ tales que

$$h_1\boldsymbol{f}_1 + \cdots + h_s\boldsymbol{f}_s = \mathbf{0}.$$

Si denotamos por F la matriz $F := (\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s)^T \in A^{s\times q}$, entonces

$$Syz(M) := \{\boldsymbol{h} \in A^{1\times s} \mid \boldsymbol{h}F = \mathbf{0}\} = \ker(.F),$$

con $.F$ definido por $.F : A^{1\times s} \to A^{1\times q}$, $\boldsymbol{e}_i \mapsto \boldsymbol{e}_i F = \boldsymbol{f}_i$, donde $\{\boldsymbol{e}_i\}_{i=1}^s$ es la base canónica de $A^{1\times s}$. También escribiremos

$$Syz(F) := Syz(M) = Syz(\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}). \tag{4.3.2}$$

Puesto que $A^{1\times s}$ es un A-módulo noetheriano y $Syz(M)$ es un submódulo de $A^{1\times s}$, entonces $Syz(M)$ es finitamente generado y determina una matriz cuyas filas son sus generadores.

El cálculo de $Syz(M)$ se realiza en dos pasos (para todos los detalles véase [21], capítulo 15): primero calculamos una base de Gröbner $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t\}$ para M y también calculamos $Syz(G) := Syz(\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t\}) \leq A^{1\times t}$, luego, como segundo paso, construimos un sistema de generadores para $Syz(M)$ a partir de un sistema $\{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l\}$ de generadores de $Syz(G)$.

Con la notación del teorema 4.3.1, sean $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_s$ las filas de $I_s - QH$, entonces se tiene el siguiente resultado.

Teorema 4.3.3. *Con la notación anterior,*

$$Syz(F) = Syz(M) = Syz(\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}) = \langle \boldsymbol{s}_1 H, \ldots, \boldsymbol{s}_l H, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_s \rangle.$$

Observación 4.3.4. Es claro que los cálculos 6 y 7 de la sección 4.1 corresponden a calcular módulos de sicigias. Para 8, una vez se tenga la matriz S mediante el cálculo en 7, la matriz L se calcula por membresía. Lo mismo ocurre para el cálculo de X en 13. El cálculo de la matriz S_2 es por sicigias.

C. Matriz de presentación de un módulo.

Dado un sistema lineal funcional, sabemos que el módulo asociado es finitamente generado y tiene una presentación finita, véase (2.2.4). Veamos ahora que si $M := \langle \boldsymbol{f}_1, \ldots, \boldsymbol{f}_s \rangle$ es un submódulo finitamente generado de $A^{1\times q}$, entonces podemos asociar a M una presentación finita con su respectiva matriz de presentación: en efecto, se tiene el A-homomorfismo sobreyectivo $\pi : A^{1\times s} \to M$, $\boldsymbol{e}_i \mapsto \boldsymbol{f}_i$, $1 \le i \le s$, calculamos la matriz Π de sicigias de M y obtenemos la presentación finita $A^{1\times l} \xrightarrow{\Pi} A^{1\times s} \xrightarrow{\pi} M \longrightarrow 0$, $M \cong A^{1\times s}/A^{1\times l}\Pi$.

D. Cálculo de la inversa a izquierda de una matriz.

Vamos ahora a presentar un algoritmo que determina si una matriz rectangular dada con entradas en A tiene inversa a izquierda, y en caso positivo, calcular una inversa. Un algoritmo similar se puede construir para inversas a derecha (véase [21], capítulo 17). El algoritmo está soportado en el siguiente hecho teórico válido sobre cualquier anillo.

Proposición 4.3.5. *Sea F una matriz rectangular sobre A de tamaño $r \times s$. Si F tiene inversa a izquierda, entonces $r \ge s$. Además, F tiene inversa a izquierda si, y sólo si, el módulo generado por las filas de F coincide con $A^{1\times s}$.*

Corolario 4.3.6. *Sea $F \in A^{r\times s}$ una matriz rectangular. El siguiente algoritmo determina si F tiene inversa a izquierda, y en caso positivo, calcula una inversa a izquierda de F:*

Algorithm for the left inverse of a matrix

INPUT: A rectangular matrix $F \in A^{r \times s}$

OUTPUT: A matrix $L \in A^{s \times r}$ satisfying $LF = I_s$ if it exists, and 0 in other case

INITIALIZATION:

IF $r < s$

RETURN 0

IF $r \geq s$, let $G := \{\boldsymbol{g}_1, \dots, \boldsymbol{g}_t\}$ be a Gröbner basis for the left submodule generated by rows of F and $\{\boldsymbol{e}_i\}_{i=1}^{s}$ be the canonical basis of $A^{1\times s}$. Use the division algorithm to verify if $\boldsymbol{e}_i \in \langle G \rangle$ for each $\leq i \leq s$.

IF there exists some $\boldsymbol{e}_i$ such that $\boldsymbol{e}_i \notin \langle G \rangle$,

RETURN 0

IF $\langle G \rangle = A^{1\times s}$, let $H \in A^{t\times r}$ with the property $G = HF$, and consider $K := [k_{ij}] \in A^{s\times t}$, where the k_{ij}'s are such that

$$\boldsymbol{e}_i = k_{i1}\boldsymbol{g}_1 + k_{i2}\boldsymbol{g}_2 + \cdots + k_{it}\boldsymbol{g}_t \text{ for } 1 \leq i \leq s.$$

Thus, $I_s = KG$

RETURN $L := KH$

Observación 4.3.7. Es claro que el algoritmo anterior permite realizar el calculo 3 de la sección 4.1.

E. Cálculo de bases de módulos libres.

Dado un módulo establemente libre (definición 2.1.1) con una presentación minimal, vamos a determinar si dicho módulo es libre, y en caso afirmativo, calcular una base. La siguiente definición y resultados se pueden enunciar para anillos arbitrarios, pero seguiremos asumiendo que A es una extensión PBW torcida con las hipótesis que hemos fijado (véase la observación 4.2.9).

Definición 4.3.8. *Sea M un A-módulo con presentación finita*

$$A^{1\times s} \xrightarrow{f_1} A^{1\times r} \xrightarrow{f_0} M \to 0.$$

*Se dice que la presentación es **minimal** si f_1 tiene inversa a izquierda.*

En tal caso se tiene la siguiente sucesión exacta

$$0 \to A^{1\times s} \xrightarrow{f_1} A^{1\times r} \xrightarrow{f_0} M \to 0. \tag{4.3.3}$$

Proposición 4.3.9. *Sea M un A-módulo. M es establemente libre si, y sólo si, M tiene una presentación minimal.*

Teorema 4.3.10. *Sea M un A-módulo establemente libre con presentación minimal (4.3.3). Sea $g_1 : A^{1\times r} \to A^{1\times s}$ tal que $g_1 f_1 = i_{A^{1\times s}}$. Las siguientes condiciones son equivalentes:*

(i) *M es libre de dimensión $r - s$.*

(ii) *Existe una matriz $U \in GL_r(A)$ tal que $UG_1 = \begin{bmatrix} I_s \\ 0 \end{bmatrix}$, donde G_1 es la matriz de g_1 en las bases canónicas. En tal caso, las últimas $r - s$ filas de U conforman una base para M. Además, las primeras s filas de U constituyen $F_1 := m(f_1)$, la matriz de f_1 en las bases canónicas.*

Nuestro siguiente algoritmo calcula la matriz U del teorema 4.3.10, si existe, y en tal caso, una base para el módulo M. Recordemos que U es invertible si, y sólo si, las filas de U conforman una base de $A^{1\times r}$. Ya que f_1 es inyectiva, $Syz(F_1) = 0$, por lo tanto, para construir U debemos encontrar vectores $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{r-s} \in Syz(G_1)$ tales que $\{F_{1(1)}, \ldots, F_{1(s)}, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{r-s}\}$ sean una base para $A^{1\times r}$, donde $G_1 := m(g_1)$ es la matriz de g_1 en las bases canónicas y $F_{1(i)}$ denota la i-ésima fila of F_1, $1 \leq i \leq s$.

Algorithm for computing bases

INPUT: A nonzero stably free module M given by the minimal presentation (4.3.3).

OUTPUT: A matrix $U \in GL_r(S)$ satisfying $UG_1 = \begin{bmatrix} I_s \\ 0 \end{bmatrix}$, where $G_1 = m(g_1)$, and such that the last $r-s$ rows of U conform a basis for M and the first s rows of U conform the matrix $F_1 = m(f_1)$, if U exists. Otherwise, return 0.

INITIALIZATION: Compute a finite set of generators $X = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_l\}$ for $Syz(G_1)$.

IF $l < r-s$

RETURN 0

IF $l \geq r-s$, for each subset $\{\boldsymbol{g}^j_{i_1}, \ldots, \boldsymbol{g}^j_{i_{r-s}}\}$ of X verify if $U_j := \begin{bmatrix} F & \boldsymbol{g}^j_{i_1} & \ldots & \boldsymbol{g}^j_{i_{r-s}} \end{bmatrix}^T$ has a left inverse using the Corollary 4.3.6.

IF none of these matrices U_j has a left inverse

RETURN 0

IF the matrices $U_{j_1}, \ldots, U_{j_t}$ have left inverse, compute $Syz(U_{j_k})$ for $1 \leq k \leq t$.

IF $Syz(U_{j_k}) \neq 0$ for all $1 \leq k \leq t$

RETURN 0

IF there exists U_j is such that $Syz(U_j) = 0$

RETURN $U := U_j$.

Observación 4.3.11. Para realizar el cálculo de las matrices U, V y $\overline{R}$ de los numerales 11 y 12 de la sección 4.1 se puede proceder de la siguiente manera: usar sicigias para calcular $U_1 = \ker(.P)$; aplicar el algoritmo anterior para calcular U_2 ya que U_2 corresponde a una base de $Coim(.P) = D^{1\times p}/(D^{1\times m}U_1)$ el cual es un módulo con presentación finita minimal:

$$0 \to D^{1\times m} \xrightarrow{.U_1} D^{1\times p} \xrightarrow{\kappa} Coim(.P) \to 0.$$

Esto completa el cálculo de U según (3.3.2). Lo mismo se tiene para V. Según los teoremas 3.3.4 y 3.4.3, para obtener las matrices W_1, W_2 y $\overline{R}$ calculamos U^{-1}, pero como A es noetheriano, basta calcular la inversa a izquierda de U mediante el algoritmo del corolario 4.3.6.

F. Para realizar los cálculos 1, 4, 5 y 10 de la sección 4.1 es necesario disponer de procedimientos que permitan calcular $Hom_D(M, M')$, M^*, $Ext^1_D(M, M')$, $Ext^1_D(M^T, D)$ y $t(M)$. En [6] se han usado las librerías `OREMODULES`, `MORPHISMS`, `QUOTIENT`, implementadas en `MAPLE` en [5]), para realizar algunos de los cálculos anteriores, asumiendo que D es una álgebra de Ore sujeta a ciertas restricciones. Por ejemplo, si D es un anillo conmutativo, entonces $Hom_D(M, M')$ es un D-módulo y en [6] se ha diseñado un algoritmo para calcular un conjunto de generadores de $Hom_D(M, M')$, así como las matrices P y Q de (3.1.1). En los ejemplos que presentaremos en la última sección de la monografía, los cuales han sido tomados de [6], los autores en [6] usaron las librerías anteriores para realizar todas las cuentas.

Observación 4.3.12. Para el caso general en que D sea una extensión PBW torcida, en [21] también se han construido procedimientos y algoritmos que permiten realizar todos cálculos señalados arriba, pero su implementación en `MAPLE` aún no se ha completado.

4.4 Implementación

En esta sección presentamos la librería `SPBWE.lib` implementada para `MAPLE` en [8], la cual permite trabajar computacionalmente con las extensiones PBW torcidas, en particular, permite hacer efectivos los cálculos, procedimientos y algoritmos de las secciones anteriores. `SPBWE.lib` consta de los siguientes paquetes:

`RingTools`, `SPBWETools`, `SPBWEGrobner` y `SPBWERings`.

- `RingTools`: define la estructura del anillo R de coeficientes de una extensión PBW torcida A.
- `SPBWETools`: esta es una colección de funciones inherentes a las extensiones las cuales permiten definir la estructura misma de A. Estas funciones son en general muy útiles para trabajar en anillos no conmutatiovs de tipo polinomial.
- `SPBWEGrobner`: esta es una colección de funciones cuya principal rutina es el algoritmo de Buchberger para calcular las bases de Gröbner.
- `SPBWERings`: este paquete consta de ejemplos concretos predefinidos de extensiones PBW torcidas dentro de la librería.

A continuación presentamos algunos ejemplos de cálculos con `SPBWE.lib` incluyendo en cada caso la instrucción correspondiente.

Ejemplo 4.4.1. Implementaión de las extensiones. Una extensión PBW torcida $A := \sigma(R)\langle x_1 \ldots, x_n\rangle$ se define con la siguiente instrucción y parámetros:

$$\texttt{SetSkewPBWExtension(}L_1\texttt{,}L_1\texttt{,}L_3\texttt{,}L_4\texttt{,}C\texttt{)}$$

$L_1 :=$	lista de las variables $x_1, \dots, x_n$, con $x_1 \succ \cdots \succ x_n$.
$L_2 :=$	lista de las relaciones entre las variables x_i, $1 \leq i \leq n$.
$L_3 :=$	lista de los automorfismos σ_i, $1 \leq i \leq n$.
$L_4 :=$	lista de las σ-derivaciones, δ_i, $1 \leq i \leq n$.
$C :=$	anillo R de coeficientes.

El parámetro C puede ser omitido cuando el anillo de coeficientes es un subanillo del cuerpo de fracciones $\mathbb{C}(t_1, \dots, t_m)$, donde $t_i \notin \{x_1, \dots, x_n\}$, $1 \leq i \leq m$. Más exactamente, el anillo C por defecto puede ser alguno de los siguientes anillos:

$$S, \; S[t_1, \dots, t_m], \; S(t_1, \dots, t_m), \text{ donde } S \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}. \tag{4.4.1}$$

Veamos un par de ejemplos.

(a) Consideremos el análogo multiplicativo del álgebra de Weyl $\mathcal{O}_3(\lambda_{ji})$, con $n = 3$, $\lambda_{31} = 2$, $\lambda_{32} = 2$ y $\lambda_{21} = -1$ (véase el ejemplo 1.3.6). $\mathcal{O}_3(\lambda_{ji})$ es una extensión PBW torcida de $\mathbb{Q}[x_3]$. En efecto, $A := \mathcal{O}_3(\lambda_{ji}) = \sigma(\mathbb{Q}[x_3])\langle x_1, x_2\rangle$ está sujeta a la relación (`rel`): $x_2x_1 = -x_1x_2$, y en este caso las σ_i's y δ_i's satisfacen

$$\sigma_1(x_3) = \tfrac{1}{2}x_3, \quad \sigma_2(x_3) = \tfrac{1}{2}x_3, \quad \delta_1 = \delta_2 = 0.$$

La implementación es entonces

$$A := \texttt{SetSkewPBWExtension([}x_1, x_2\texttt{],rel,[}\sigma_1, \sigma_2\texttt{],[}0, 0\texttt{])}$$

(b) Veamos ahora el álgebra de difusión $A = \sigma(\mathbb{Q}[x_1, x_2, x_3])\langle D_1, D_2, D_3\rangle$, con relaciones (`rels`):

$$\begin{aligned} D_2D_1 =& D_1D_2 + x_2D_1 - x_1D_2, \\ D_3D_1 =& D_1D_3 + x_3D_1 - x_1D_3, \\ D_3D_2 =& D_2D_3 + x_3D_2 - x_2D_3. \end{aligned}$$

La implementación de A es

$$A{:=}\texttt{SetSkewPBWExtension([}D_1, D_2, D_3\texttt{],rels,[}id, id, id\texttt{],[}0, 0, 0\texttt{])}$$

El paquete permite hacer la siguiente cuenta sencilla: sea

$$z_1 := x_1x_2D_1D_2 + x_3D_1D_3 \text{ y } z_2 := D_2^2D_3^2,$$

entonces

$$z_1 \cdot z_2 = x_1x_2D_1D_2^3D_3^2 + x_3D_1D_2^2D_3^3 + 2x_3^2D_1D_2^2D_3^2 - 2x_2x_3D_1D_2D_3^3 - x_2x_3^2D_1D_2D_3^2 + x_2^2x_3D_1D_3^3.$$

Ejemplo 4.4.2. Algoritmo de la división.

`DivisionAlgorithm(`f`,[`$f_1,\ldots,f_n$`],order over `A`,skew `PBW` extension `A`)`

Para el álgebra de difusión $A := \sigma(\mathbb{Q}[x_1,x_2])\langle D_1,D_2\rangle$ sujeta a la relación (`rel`)

$$D_2D_1 = 2D_1D_2 + x_2D_1 - x_1D_2,$$

consideremos como ejemplo ilustrativo

$$f := x_1x_2^2D_1^2D_2 + x_1^2x_2D_2,\ f_1 := x_1x_2D_1D_2,\ f_2 := x_2D_1,\ f_3 := x_1D_2.$$

Mediante

`DivisionAlgorithm(`f`,[`f_1,f_2,f_3`],lex,`A`)`

el software produce

$$q_1 := x_2D_1,\ q_2 := 0,\ q_3 := x_1x_2 \text{ y } h = 0.$$

Por lo tanto,

$$f = q_1f_1 + q_2f_2 + q_3f_3.$$

Ejemplo 4.4.3. Algoritmo de Buchberger.

`BuchbergerAlgSkewPoly(`$L,\mathrm{ord},\ \mathrm{ORD},A$`)`

`L` := lista de los generadores del submódulo.
`ord` := orden monomial sobre A.
`ORD` := orden sobre A^m.

Para el análogo multiplicativo del álgebra de Weyl,

$$A := \mathcal{O}_3(2,\tfrac{1}{2},3) = \sigma(\mathbb{Q})\langle x_1,x_2,x_3\rangle,$$

definida por las relaciones

$$x_2x_1 = 2x_1x_2,\quad x_3x_1 = \tfrac{1}{2}x_1x_3,\quad x_3x_2 = 3x_2x_3,$$

sea $M := \langle \boldsymbol{f}_1,\boldsymbol{f}_2\rangle$, con $\boldsymbol{f}_1 := x_1^2x_2^2\boldsymbol{e}_1 + x_2x_3\boldsymbol{e}_2$ y $\boldsymbol{f}_2 := 2x_1x_2x_3\boldsymbol{e}_1 + x_2\boldsymbol{e}_2$. Aplicamos

`BuchbergerAlgSkewPoly([f`$_1$`,f`$_2$`],gradlex,TOPREV,`A`)`

y obtenemos la base de Gröbner $G = \{\boldsymbol{g}_1,\boldsymbol{g}_2,\boldsymbol{g}_3\}$, donde

$$\boldsymbol{g}_1 = x_1^2x_2^2\boldsymbol{e}_1 + x_2x_3\boldsymbol{e}_2,\quad \boldsymbol{g}_2 = 2x_1x_2x_3\boldsymbol{e}_1 + x_2\boldsymbol{e}_2,\quad \boldsymbol{g}_3 = 48x_2x_3^2\boldsymbol{e}_2 - 9x_1x_2^2\boldsymbol{e}_2.$$

Ejemplo 4.4.4. Cálculo de sicigias. Sea $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}$ un conjunto finito de vectores no nulos de $A^{1\times q}$, la sintáxis para el cálculo del módulo de sicigias es la siguiente:

$$\texttt{SyzModule(}M, \text{ord}, \ \text{ORD}, A\texttt{)},$$

donde M es una matriz cuyas filas son $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s$. Con esta instrucción el software arroja una matriz cuyas filas son los generadores del módulo de sicigias. Observemos que si $q = 1$, el algoritmo calcula el módulo de sicigias de un ideal izquierdo de A.

Veamos un ejemplo, consideremos el álgebra de Witten $A := \sigma(\mathbb{Q})\langle x, y, z\rangle$ sujeta a las siguientes relaciones (véase [21], capítulo 2):

$$zx = xz - x, \quad zy = yz + 2y \quad yx = -xy,$$

y calculemos $Syz(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3)$, donde $\boldsymbol{f}_1 = \boldsymbol{e}_1 + (x+y)\boldsymbol{e}_2$, $\boldsymbol{f}_2 = z\boldsymbol{e}_2$, $\boldsymbol{f}_3 = y\boldsymbol{e}_1 + z\boldsymbol{e}_2$. Sea $M := [\boldsymbol{f}_1 \ \ \boldsymbol{f}_2 \ \ \boldsymbol{f}_3]^T$, aplicamos

$$\texttt{SyzModule(}M\texttt{, gradlex, TOPREV, }A\texttt{)}$$

y el paquete produce

$$Syz(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3) = \langle \boldsymbol{u}_1, \boldsymbol{u}_2\rangle, \text{ con } \boldsymbol{u}_i = L_{i1}\boldsymbol{e}_1 + L_{i2}\boldsymbol{e}_2 + L_{i3}\boldsymbol{e}_3 \text{ para } i = 1, 2,$$

donde

$$\begin{aligned}
&L_{11} = -yz^2 + yz + 2y,\\
&L_{12} = -xyz + y^2z + 3xy + 3y^2 - z^2 + 5z - 4,\\
&L_{13} = z^2 - 5z + 4,\\
&L_{21} = xyz + y^2z + xy - 2y^2,\\
&L_{22} = x^2y - 2xy^2 - y^3 + xz + yz - x - 4y,\\
&L_{23} = -xz - yz + x + 4y.
\end{aligned}$$

Ejemplo 4.4.5. Inversa a izquierda de una matriz.

La siguiente instrucción calcula la inversa a izquierda de una matriz M:

$$\texttt{LeftInverseMatrix(}M, \text{ord}, \ \text{ORD}, A\texttt{)}.$$

Como ilustración, sea $A := \sigma(\mathbb{K})\langle x, y\rangle$, $yx = -xy + 1$, y consideremos tres casos.

Caso ($\mathbb{K} := \mathbb{Q}$). Para la matriz

$$M := \begin{bmatrix} 1 & 1\\ y & 0\\ x^2 & 0\\ 1 & y\end{bmatrix},$$

la instrucción

$$\texttt{LeftInverseMatrix(}M, \text{gradlex}, \text{TOPREV}, A\texttt{)}$$

produce como inversa a izquierda la matriz

$$\begin{bmatrix} -y & 1 & 0 & 1 \\ y+1 & -1 & 0 & -1 \end{bmatrix}.$$

Caso ($\mathbb{K} := \mathbb{Q}$). Para las matrices

$$M^{(1)} := \begin{bmatrix} 1 & 1 \\ xy & 0 \\ x^2 & 0 \\ 1 & y \end{bmatrix}, \ M^{(2)} := \begin{bmatrix} 1 & 1 \\ xy & 1 \\ y^2 & x \\ x & 2 \\ xy^2 & y \end{bmatrix},$$

la instrucción

$$\texttt{LeftInverseMatrix(}M^{(k)}, \text{gradlex}, \text{TOPREV}, A\texttt{)}$$

con $k = 1, 2$, produce las inversas a izquierda:

$$\texttt{left inverse of } M^{(1)} = \begin{bmatrix} xy^2 - y & y+1 & 0 & -xy+1 \\ -xy^2 + y + 1 & -y-1 & 0 & xy-1 \end{bmatrix},$$
$$\texttt{left inverse of } M^{(2)} = \begin{bmatrix} \frac{1}{4}x^2 + \frac{1}{2}x + \frac{1}{4}y + 1 & -\frac{1}{4}y & -\frac{1}{4}x & -\frac{1}{4}x - \frac{1}{2} & 0 \\ -\frac{1}{4}x^2 - \frac{1}{2}x - \frac{1}{4}y & \frac{1}{4}y & \frac{1}{4}x & \frac{1}{4}x + \frac{1}{2} & 0 \end{bmatrix}.$$

Caso ($\mathbb{K} := \mathbb{Z}_2$). Para

$$M^{(3)} := \begin{bmatrix} x & y & 0 \\ y & y^2 & -x \\ x^2 & -xy & 1 \\ x+y & 1 & -y \end{bmatrix}, \ M^{(4)} := \begin{bmatrix} 1 & x & y \\ x+1 & 0 & 0 \\ -xy & 1 & -y \\ xy^2 & y & 1 \\ y^2 & 1 & x+y \end{bmatrix}.$$

las inversas son:

$$\texttt{left inverse of } M^{(3)} = \begin{bmatrix} m_{11}^{(3)} & m_{12}^{(3)} & m_{13}^{(3)} & m_{14}^{(3)} \\ m_{21}^{(3)} & m_{22}^{(3)} & m_{23}^{(3)} & m_{24}^{(3)} \\ m_{31}^{(3)} & m_{32}^{(3)} & m_{33}^{(3)} & m_{34}^{(3)} \end{bmatrix},$$
$$\texttt{left inverse of } M^{(4)} = \begin{bmatrix} m_{11}^{(4)} & m_{12}^{(4)} & m_{13}^{(4)} & m_{14}^{(4)} & m_{15}^{(4)} \\ m_{21}^{(4)} & m_{22}^{(4)} & m_{23}^{(4)} & m_{24}^{(4)} & m_{25}^{(4)} \\ m_{31}^{(4)} & m_{32}^{(4)} & m_{33}^{(4)} & m_{34}^{(4)} & m_{35}^{(4)} \end{bmatrix},$$

donde

$$m_{11}^{(3)} = x^2y^4 + x^3y^2 + xy^4 + x^2y^2 + y^4 + x^3 + y^3 + y,$$
$$m_{12}^{(3)} = xy^2 + y^3 + y^2 + x,$$
$$m_{13}^{(3)} = xy^4 + x^2y^2 + y^4 + xy^2 + y^3 + x^2 + y^2,$$
$$m_{14}^{(3)} = xy^3 + xy^2 + y^3 + y^2,$$
$$m_{21}^{(3)} = x^2y^4 + x^3y^2 + x^2y^3 + xy^4 + x^3y + xy^3 + y^4 + xy^2 + x^2 + xy + y^2 + y,$$
$$m_{22}^{(3)} = xy^2 + y^3 + xy + 1,$$
$$m_{23}^{(3)} = xy^4 + x^2y^2 + xy^3 + y^4 + x^2y + y,$$
$$m_{24}^{(3)} = xy^3 + y^3 + y + 1,$$
$$m_{31}^{(3)} = x,$$
$$m_{32}^{(3)} = 0,$$
$$m_{33}^{(3)} = 1,$$
$$m_{34}^{(3)} = 0,$$

y

$$m_{11}^{(4)} = xy^2 + xy + y^2 + y,$$
$$m_{12}^{(4)} = x^2y^3 + x^2y^2 + xy^2 + y^3 + y,$$
$$m_{13}^{(4)} = xy^2 + y^2,$$
$$m_{14}^{(4)} = x^2y + x^2 + y + 1,$$
$$m_{15}^{(4)} = xy + x + y + 1,$$
$$m_{21}^{(4)} = xy^2 + xy + x + y,$$
$$m_{22}^{(4)} = x^2y^3 + x^2y^2 + xy^3 + x^2y + y^3 + xy + y^2 + x + y + 1,$$
$$m_{23}^{(4)} = xy^2 + x^2 + xy,$$
$$m_{24}^{(4)} = x^2y + x^2 + xy + 1,$$
$$m_{25}^{(4)} = x + y,$$
$$m_{31}^{(4)} = x,$$
$$m_{32}^{(4)} = x^2y + xy^2 + y^3 + xy + x + y + 1,$$
$$m_{33}^{(4)} = x^2 + xy + y + 1,$$
$$m_{34}^{(4)} = 0,$$
$$m_{35}^{(4)} = xy + y + 1.$$

4.5 Ejemplos

En los ejemplos que presentaremos en esta última sección, los cuales hemos tomado de [6], los autores en [6] usaron para lo cálculos las librerías `OREMODULES`, `MORPHISMS`, `QUOTIENT`, implementadas para `MAPLE` en [4] y [5].

Ejemplo 4.5.1. En este primer ejemplo verificaremos si el sistema del ejemplo 2.2.4 es controlable y parametrizable. Por la parte (iv) del teorema 2.3.2 tenemos que (2.2.9) es controlable si, y sólo si, el D-módulo $M = D^{1\times 4}/(D^{1\times 3}R)$ es sin torsión, con R definido por (2.2.10). Por la parte (ii) del teorema 2.3.3 esto es equivalente a $Ext_D^1(N, D) = 0$, donde $N = D^{1\times 3}/(D^{1\times 4}R^T)$. Con el fin de calcular el D-módulo $Ext_D^1(N, D)$, notemos que una resolución libre de N está dada por

$$0 \to D \xrightarrow{.Q^T} D^{1\times 4} \xrightarrow{.R^T} D^{1\times 3} \to N \to 0, \tag{4.5.1}$$

donde Q^T es tal que $\ker(.R^T) = DQ^T$. El cálculo de $\ker(.R^T)$ ha sido realizado en [6] mediante las librerías señaladas antes y se encontró que:

$$Q^T = (\omega^2 ka\delta_h, \omega^2\partial + \omega^2 a, \omega^2\partial^2 + \omega^2 a\partial, \partial^3 + (2\zeta\omega + a)\partial^2 + (\omega^2 + 2a\zeta w)\partial + a\omega^2).$$

Tenemos entonces el complejo

$$0 \to D^{1\times 3} \xrightarrow{.R} D^{1\times 4} \xrightarrow{.Q} D \to 0, \tag{4.5.2}$$

de donde

$$Ext_D^1(N, D) = \ker(.Q)/(D^{1\times 3}R).$$

En [6] se ha calculado $\ker(.Q)$, es decir, se ha calculado el módulo L de sicigias del módulo $D^{1\times 4}Q$ generado por las filas de Q:

$$L = \begin{bmatrix} \partial + a & -ka\delta_h & 0 & 0 \\ 0 & \omega^2 & \partial + 2\zeta\omega & -\omega^2 \\ 0 & \partial & -1 & 0 \end{bmatrix} \in D^{3\times 4}.$$

Por lo tanto, $Ext^1(N, D) = (D^{1\times 3}L)/(D^{1\times 3}R)$. Para verificar si se tiene la igualdad $Ext_D^1(N, D) = 0$ se puede aplicar el algoritmo `QUOTIENT`(L, R) de [4] y encontrar que $(D^{1\times 3}L)/(D^{1\times 3}R) = 0$. Otra forma es probar que $D^{1\times 3}L = D^{1\times 3}R$ mediante bases de Gröbner y el problema de membresía, mostrando que cada fila de L pertenece al D-modulo generado por las filas de R (véase el literal A de la sección 4.3). Hemos demostrado que el sistema (2.2.9) es controlable, y así, de la prueba del corolario 2.3.5 obtenemos que una parametrización para este sistema está dada por Q.

Ejemplo 4.5.2. Consideremos dos sistemas de ecuaciones diferenciales parciales los cuales surgen en la teoría de la elasticidad: el *operador de Killing* y el *operador de Spencer* del operador de Killing (véase [6] y [29]):

$$\begin{cases} \partial_1\xi_1 = 0, \\ \frac{1}{2}(\partial_2\xi_1 + \partial_1\xi_2) = 0, \\ \partial_2\xi_2 = 0, \end{cases} \quad \text{y} \quad \begin{cases} \partial_1 z_1 = 0, \\ \partial_2 z_1 - z_2 = 0, \\ \partial_1 z_2 = 0, \\ \partial_1 z_3 + z_2 = 0, \\ \partial_2 z_3 = 0, \\ \partial_2 z_2 = 0. \end{cases}$$

Sea $D := \mathbb{Q}[x_1, x_2][\partial_1; \mathrm{id}, \frac{\partial}{\partial x_1}][\partial_2; \mathrm{id}, \frac{\partial}{\partial x_2}]$ el anillo de operadores diferenciales con coeficientes en $\mathbb{Q}[x_1, x_2]$. Las matrices asociadas a estos dos SLF son:

$$R = \begin{bmatrix} \partial_1 & 0 \\ \frac{1}{2}\partial_2 & \frac{1}{2}\partial_1 \\ 0 & \partial_2 \end{bmatrix} \in D^{3\times 2}, \qquad R' = \begin{bmatrix} \partial_1 & \partial_2 & 0 & 0 & 0 & 0 \\ 0 & -1 & \partial_1 & 1 & 0 & \partial_2 \\ 0 & 0 & 0 & \partial_1 & \partial_1 & 0 \end{bmatrix}^T \in D^{6\times 3},$$

a las cuales asociamos los correspondientes D-módulos finitamente presentados $M := D^{1\times 2}/(D^{1\times 3}R)$ y $M' := D^{1\times 3}/(D^{1\times 6}R')$. El algoritmo 2.1 de [6] permite calcular las matrices

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad Q = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \end{bmatrix},$$

las cuales satisfacen la relación (3.1.1), por lo tanto, definen un homomorfismo $f : M \to M'$ dado por $f(\xi_1) = z_1$ y $f(\xi_2) = z_3$. Según vimos en la observación 4.3.4, la matriz S de la proposición 3.1.2 es calculable con las herramientas computacionales que hemos presentado, y también con las herramientas particulares de [6] implementadas para álgebras de Ore. Así, en [6] se muestra que

$$S = \begin{bmatrix} \partial_2 & \partial_1 & \partial_2^2 & 0 \\ \partial_1 & 0 & 0 & \partial_2 \end{bmatrix}^T.$$

Según el teorema 3.2.4, f es inyectivo si, y sólo si, existe una matriz F tal que $S = FR$, pero según la observación 4.3.2 esto se resuelve mediante el procedimiento de membresía. En [6] se calculó

$$F = \begin{bmatrix} 0 & 2 & 0 \\ 1 & 0 & 0 \\ 0 & 2\partial_2 & -\partial_1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Además, que f sea un epimorfismo, es equivalente a que la matriz $[P^T \;\; R'^T]^T$ admita inversa a izquierda, y esa inversa es (véase [6] o también el ejemplo 4.4.5):

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\partial_1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Lo anterior muestra que f es un D-isomorfismo, por lo tanto, $M \cong M'$.

Ejemplo 4.5.3. Consideremos el álgebra de Weyl $D := A_1(\mathbb{Q})$, la matriz

$$R := \begin{bmatrix} \partial & -t & t & \partial \\ \partial & t\partial - t & \partial & -1 \\ \partial & -t & \partial + t & \partial - 1 \\ \partial & \partial - t & t & \partial \end{bmatrix} \in D^{4\times 4}, \tag{4.5.3}$$

y el D-módulo izquierdo finitamente presentado $M := D^{1\times 4}/(D^{1\times 4}R)$. Aplicando nuevamente el algoritmo 2.1 de [6] obtenemos un endomorfismo f de M definido por medio de las matrices

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} t+1 & 1 & -1 & -t \\ 1 & 1 & -1 & 0 \\ t+1 & 1 & -1 & -t \\ t & 1 & -1 & -t+1 \end{bmatrix}, \tag{4.5.4}$$

con $RP = QR$. Calculamos bases para $\ker(.P), Coim(.P), \ker(.Q)$ y $Coim(.Q)$ (véase la observación 4.3.11):

$$\begin{cases} U_1 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\ U_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \end{cases} \begin{cases} V_1 = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & t-1 & -t \end{bmatrix}, \\ V_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}. \end{cases}$$

Para la forma triangular en bloques del teorema 3.3.4 se calcula U^{-1} y se obtiene

$$\overline{R} = VRU^{-1} = \begin{bmatrix} -\partial & 1 & 0 & 0 \\ t\partial - t & -\partial - t & 0 & 0 \\ \partial + t & \partial - 1 & \partial & -t \\ -\partial & 1 & 0 & \partial \end{bmatrix}.$$

Ejemplo 4.5.4. Consideremos nuevamente el álgebra de Weyl $D := A_1(\mathbb{Q})$ y $M := D^{1\times 4}/(D^{1\times 4}R)$ definido en el ejemplo 4.5.3, con R como en (4.5.3). Sea f el endomorfismo de M inducido por la pareja de matrices (P, Q) dadas en (4.5.4). Podemos verificar que $P^2 = P$, luego por el lema 3.4.1, $f^2 = f$, es decir, f es un idempotente no trivial de $End_D(M)$. Para las matrices del teorema 3.5.3 se encontró en [6] que

$$S = \begin{bmatrix} \partial & -t & 0 & 0 \\ 0 & \partial & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L = \begin{bmatrix} 1 & 0 & t & \partial \\ 1 & t & \partial & -1 \\ 1 & 0 & \partial + t & \partial - 1 \\ 1 & 1 & t & \partial \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Puesto que $\ker(.S) = 0$, entonces $S_2 = 0$. El teorema 3.5.3 garantiza que $R\eta = 0$ es equivalente a la integración de los sistemas $S\zeta = 0$ y $L\tau = 0$. Con respecto al primero un cálculo directo muestra que

$$\zeta_1 = \frac{1}{2}C_1 t^2 + C_2, \quad \zeta_2 = C_1, \quad \zeta_3 = 0, \quad \zeta_4 = 0,$$

donde C_1 y C_2 son constantes arbitrarias del cuerpo K. Para $L\tau = 0$ se tiene

$$\begin{cases} \tau_1 = 0, \\ \tau_2 = 0, \\ t\tau_3 + \partial\tau_4 = 0, \\ \partial\tau_3 - \tau_4 = 0. \end{cases} \Leftrightarrow \begin{cases} \tau_1 = 0, \\ \tau_2 = 0, \\ \partial^2\tau_3 + t\tau_3 = 0, \\ \tau_4 = \partial\tau_3. \end{cases} \Leftrightarrow \begin{cases} \tau_1 = 0, \\ \tau_2 = 0, \\ \tau_3(t) = C_3\mathrm{Ai}(t) + C_4\mathrm{Bi}(t), \\ \tau_4(t) = C_3\partial\mathrm{Ai}(t) + C_4\partial\mathrm{Bi}(t), \end{cases}$$

donde $\mathrm{Ai}(t)$ y $\mathrm{Bi}(t)$ denotan las dos soluciones independientes de la ecuación $\partial^2 y(t) - ty(t) = 0$, mientras que C_3 y C_4 son constantes. Por consiguiente, la solución general de $R\eta = 0$ está dada por

$$\eta = \zeta + X\tau = \begin{bmatrix} \frac{1}{2}C_1t^2 + C_2 \\ C_1 \\ C_3\mathrm{Ai}(t) + C_4\mathrm{Bi}(t) \\ C_3\partial\mathrm{Ai}(t) + C_4\partial\mathrm{Bi}(t) \end{bmatrix}, \tag{4.5.5}$$

donde C_1, C_2, C_3 y C_4 son constantes arbitrarias de K.

Concluimos con algunos problemas que surgen de los temas estudiados y de los resultados presentados en esta monografía.

Problema 4.5.5. (i) La mayoría de los resultados de los capítulos 2 y 3 se probaron para dominios noetherianos a izquierda, y algunos, asumiendo adicionalmente la condición de Noether a derecha (véase el teorema 2.3.3 y el corolario 2.3.5). Así, los resultados pueden ser aplicados a SLF sobre extensiones PBW torcidas biyectivas con coeficientes en dominios noetherianos a izquierda (derecha), véase [21]. Resulta entonces interesante descubrir nuevos ejemplos concretos de SLF sobre extensiones PBW torcidas en áreas como física, biología, informática, ingeniería, etc. y, para estos sistemas, aplicar las propiedades estudiadas a lo largo de la monografía.

(ii) Dada una extensión PBW torcida es una tarea útil y desafiante calcular un cogenerador inyectivo para su categoría de módulos (véase la observación 2.1.10 y el teorema 2.3.2).

(iii) Implementar en `MAPLE` los procedimientos y algoritmos señalado en la observación 4.3.12.

(iv) Mediante técnicas algebraicas constructivas similares a las que se presentaron en los capítulos 2 y 3, estudiar *sistemas no lineales* de ecuaciones diferenciales. Por ejemplo, en [1], parte II, capítulo 4, se estudia la observabilidad de sistemas no lineales de ecuaciones diferenciales con retardo en tiempo discreto y se muestran aplicaciones de los resultados al análisis de modelos biológicos. Los criterios algebraicos presentados en [1] para decidir si un sistema es observable tienen la ventaja de evitar los cálculos clásicos directos, los cuales son complicados y tediosos al tener que manipular ecuaciones de entrada-salida. Las técnicas algebraicas en [1] son sencillas y se reducen a calcular el rango del Jacobiano de un sistema de ecuaciones algebraicas sobre una extensión de Ore.

Bibliografía

[1] **Anguelova, M.**, *Observability and identifiability of nonlinear systems with applications in biology*, Ph.D. Thesis, Chalmers University of Technology and Göteborg University, Sweden, 2007. 73

[2] **Boudellioua, M. and Quadrat, A.**, *Serre's reduction of linear functional systems*, INRIA rapport 7214, February 2010. 11

[3] **Bueso, J., Gómez-Torrecillas, J. and Verschoren, A.**, *Algorithmic Methods in Non-Commutative Algebra: Applications to Quantum Groups*, Kluwer, 2003. v, 49, 51

[4] **Chyzak, F., Quadrat, A. and Robertz, D.**, *Effective algorithms for parametrizing linear control systems over Ore algebras*, AAECC, 16, 2005, 319–376. iv, 11, 14, 19, 20, 70

[5] **Chyzak, F., Quadrat, A. and Robertz, D.**, *OreModules: A Symbolic Package for the Study of Multidimensional Linear Systems*, INRIA, 2007 (preprint). 11, 49, 64, 70

[6] **Cluzeau, T. and Quadrat, A.**, *Factoring and decomposing a class of linear functional systems*, Lin. Alg. And Its Appl., 428, 2008, 324–381. iii, 11, 19, 20, 31, 35, 41, 42, 44, 46, 47, 49, 64, 69, 70, 71, 72

[7] **Dubois, F., Petit, N. and Rouchon, P.**, *Motion planning and nonlinear simulations for a tank containing a fluid,* , Proceedings of the 5th European Control Conference, Karlsruhe, Germany, 1999. iii, 19

[8] **Fajardo, W.**, *A computational Maple library for skew PBW extensions*, Fund. Inform., 176, 2019, 159-191. 49, 55, 56, 64

[9] **Fliess, M.**, *Some basic structural properties of generalized linear systems*, Systems & Control Letters, 15, 1990, 391–396. iii

[10] **Fliess, M. and Mounier, H.**, *Controllability and observability of linear delay systems: an algebraic approach*, ESAIM: Control, Optimisation and Calculus of Variations, 3, 1998, 301–314. iii

[11] **Gallego, C. and Lezama, O.**, *Gröbner bases for ideals of $\sigma - PBW$ extensions*, Comminications in Algebra, 39, 2011, 50-75. iv, 1, 7, 51

[12] **Goodearl, K. and Warfield, R. Jr.**, *An Introduction to Noncommutative Noetherian Rings*, London Mathematical Society, ST 61, 2004. iv

[13] **http://www.singular.uni-kl.de** 49

[14] **Kashiwara, M.**. *D-modules and Microlocal Calculus*, volume 217 of Translations of Mathematical Monographs, American Mathematical Society, 2003. iii

[15] **Levandovskyy, V.**, *Non-commutative Computer Algebra for polynomial Algebras: Gröbner bases, applications and implementation*, Ph. D. Thesis, Univ. Kaiserslautern, Germany, 2005. v, 49, 51

[16] **Lezama, O.**, *Cuadernos de Álgebra, No. 2: Anillos*, SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, sites.google.com/a/unal.edu.co/sac2 iv

[17] **Lezama, O.**, *Cuadernos de Álgebra, No. 3: Módulos*, SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, sites.google.com/a/unal.edu.co/sac2 iv

[18] **Lezama, O.**, *Cuadernos de Álgebra, No. 6: Anillos y módulos*, SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, sites.google.com/a/unal.edu.co/sac2 iv

[19] **Lezama, O.**, *Cuadernos de Álgebra, No. 8: Álgebra homológica*, SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, sites.google.com/a/unal.edu.co/sac2 iv, 13, 24, 25, 26, 29

[20] **Lezama, O.**, *Cuadernos de Álgebra, No. 9: Álgebra no conmutativa*, SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, sites.google.com/a/unal.edu.co/sac2 iv, v, 1, 2, 6, 7

[21] **Lezama, O., Fajardo, W., Gallego, C., Reyes, A., Suárez, H., and Venegas, H.**, *Skew PBW Extensions: Ring and module theoretic properties, matrix and Gröbner methods, applications*, to be published by Springer. iv, v, 1, 31, 33, 49, 51, 54, 55, 56, 57, 58, 59, 60, 64, 67, 73

[22] **Lezama, O. and Reyes, M.A.**, *Some homological properties of skew PBW extensions*, Communications in Algebra, 42, 2014, 1200-1230. iv, 1, 7

[23] **Li, H.**, *Noncommutative Gröbner Bases and Filtered-Graded Transfer*, Lecture Notes in Mathematics, Vol. 1795, Springer, 2002. v, 49, 51

[24] **Malgrange, B.**, Systèmes à coefficients constants, Séminaire Bourbaki 1962/1963, 1–11. iii, iv, 18

[25] **McConnell, J. and Robson, J.**, *Noncommutative Noetherian Rings*, Graduate Studies in Mathematics, AMS, 2001. iv, v

[26] **Oberst, U.**, *Multidimensional constant linear systems*, Acta Appl. Math., 20, 1990, 1–175. iii, 21

[27] **Ore, O.**, *Theory of non-commutative polynomials*. Ann. Math. 34, 1933, 480-508. iv

[28] **Palamodov, V.**, *Linear Differential Operators with Constant Coefficients*, Springer, 1970. iii

[29] **Pommaret, J.**, *Partial Differential Control Theory*, Mathematics and Its Applications, Vol. 530, Kluwer, 2001. iii, 11, 70

[30] **Pommaret, J. and Quadrat, A.**, *Algebraic analysis of linear multidimensional control systems*, IMA Journal of Control and Information, 16, 1999, 275–297. iii, 11

[31] **Pommaret, J. and Quadrat, A.**, *Equivalences of linear control systems*, CERMICS, preprint. 11, 16

[32] **Pommaret, J. and Quadrat, A.**, *A functorial approach to the behaviour of multidimensional control systems*, Int. J. Appl. Math. Comput. Sci., 13, 2003, 7-13. 11

[33] **Quadrat, A., Robertz, D.**, *Computation of bases of free modules over the Weyl algebras*, J. Symb. Comp., 42, 2007, 1113–1141. iii, 11

[34] **Quadrat, A.**, *Une introduction à l'analyse algébrique constructive et à ses applications*, INRIA, Rapport de Recherche No. 7354, july 2010. iii, 11, 19

[35] **Rotman, J.J.**, *An Introduction to Homological Algebra*, Academic Press, 1979. 13, 25

[36] **Rotman, J.**, *An Introduction to Homological Algebra*, Springer, 2009. iv, 24

[37] **Sato, V, Kawai, T. and Kashiwara, M.**, *Microfunctions and pseudo-differential equations*. In Komatsu, editor, Hyperfunctions and pseudo-differential equations, Lecture Notes in Mathematics, Springer, 1973, pages 265–529. iii