FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Análise Alxébrica Construtiva

Alfredo Crespo Otero

2020-2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO EN MATEMÁTICAS

Traballo Fin de Grao

Análise Alxébrica Construtiva

Alfredo Crespo Otero

Xullo, 2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Análise matemática
Título: Análise alxébrica construtiva
Breve descrición do contido
A Análise Alxébrica estuda sistemas lineares de ecuacións diferenciais e en derivadas parciais baseándose en Teoría de Módulos e Álxebra Homolóxica. Máis concretamente, a un sistema de ecuacións dado asóciaselle un módulo sobre un determinado anel de operadores diferenciais que reflicte as propiedades estruturais do conxunto de solucións do devandito sistema. Recentemente, a Análise Alxébrica está a ser estudada desde unha perspectiva máis construtiva. O obxectivo deste traballo é chegar a coñecer os aspectos básicos da Análise Alxébrica Construtiva e presentar algunhas aplicacións á Teoría do Control.
Recomendacións
Ter superado as materias Introdución ás Ecuacións Diferenciais Ordinarias e Estruturas Alxébricas

Índice xeral

Resumo

A Análise Alxébrica é unha teoría desenvolta a mediados do século pasado que estuda sistemas lineares de ecuacións baseándose esencialmente en Teoría de Módulos e Álxebra Homolóxica. O punto de partida é o isomorfismo de Malgrange. Este, xunto con outros resultados, permite probar que as propiedades de todo sistema linear poden caracterizarse estudando un determinado módulo asociado, dalgún xeito, ao sistema.

Nos últimos anos, con todo, adoptouse un enfoque construtivo, co deseño e a implementación de algoritmos que dotan de efectividade e utilidade moitos dos resultados achados xa nos inicios da Análise Alxébrica. Ademais, tamén son cada vez máis relevantes as aplicacións á Teoría do Control.

Así pois, neste traballo proporcionamos un tratamento introdutorio, pero detallado e rigoroso, á Análise Alxébrica Construtiva, centrándonos especialmente naqueles resultados, algoritmos e conceptos que teñan un especial impacto na Teoría do Control.

Abstract

Algebraic Analysis is a theory developed in the second half of the last century which studies linear systems of equations based on Module Theory and Homological Algebra. The starting point is an abelian group isomorphism (Malgrange's isomorphism) which states that every linear system can be studied by means of a module associated to the system.

Recently, a constructive approach has been adopted and therefore a large number of algorithms have also been developed in order to implement the first ideas of Algebraic Analysis. Moreover, Algebraic Analysis applications are nowadays important in other fields such as Control Theory.

Thus, the purpose of this work is to give an introductory, detailed and rigorous treatment of Constructive Algebraic Analysis focusing mainly on those results and algortihms that are useful in Control Theory.

1. Introdución

A importancia e a utilidade das ferramentas da Álxebra no estudo de ecuacións diferenciais son, en certos casos, moi coñecidas. A xeito de exemplo, lembremos o seguinte resultado fundamental, enunciado para o caso de sistemas lineares de ecuacións diferenciais ordinarias.

Teorema 1.1. *Sexa a ecuación homoxénea*

$$x' = A(t)x,\ t \in I, \tag{1.1}$$

onde $A\colon t \in I \mapsto A(t) \in M_{n\times n}(\mathbb{R})$ *é unha función continua definida no intervalo aberto* I*. O conxunto de solucións de* (1.1) *é un espazo vectorial de dimensión* n *e isomorfo a* $\mathbb{R}^n$*.*

Ademais, no caso de que A sexa unha matriz constante, sabemos que e^{tA} é unha *matriz fundamental* da ecuación (1.1), isto é, podemos calcular unha base do espazo vectorial de solucións. Nestas circunstancias o que estamos a facer é transformar un sistema linear de ecuacións diferenciais nun sistema linear de ecuacións alxébricas, que sabemos resolver de forma fácil e eficiente.

Un caso conectado co anterior e de interese en moitas áreas do coñecemento (por exemplo, en Física) é o da ecuación diferencial linear de orde n con coeficientes constantes,

$$x^{n)} + a_1 x^{n-1)} + a_2 x^{n-2)} + \cdots + a_{n-1}x' + a_n x = 0,\ a_i \in \mathbb{R}. \tag{1.2}$$

A anterior ecuación linear pódese representar como unha ecuación diferencial de primeira orde aumentando a dimensionalidade:

$$\begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_{n-1}' \\ x_n' \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & \cdots & -a_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix}, \tag{1.3}$$

que abreviadamente podemos escribir como $x' = Ax$. Lembrando a definición de matriz fundamental é fácil obter unha base do espazo de solucións: simplemente debemos calcular e^{tA}. Un cálculo puramente alxébrico permite probar o seguinte resultado.

Proposición 1.2. *Sexa* A *a matriz do sistema* (1.3)*. O polinomio característico de* A *é:*

$$\lambda^n + a_1\lambda^{n-1} + \cdots + a_{n-1}\lambda + a_n = 0.$$

Así pois, neste caso o que estamos a facer é transformar unha ecuación diferencial linear de orde superior nun problema de autovalores e autovectores, para o que ademais temos unha expresión explícita do polinomio característico. Para calcular os autovectores basta

resolver un número finito de sistemas de ecuacións lineares. Isto amosa que o cálculo dunha base do espazo de solucións da ecuación (1.2) pode ser realizado cos métodos de resolución de sistemas lineares coñecidos. Ademais, os devanditos métodos son habitualmente fáciles de implementar en calquera linguaxe de programación. Así pois, está claro que a Álxebra é tamén a responsable de que sexamos capaces de resolver aquelas ecuacións que requiran de cálculos máis tediosos ou complicados utilizando computadores.

Sendo coñecedores da relevancia de todos os resultados e feitos que vimos de presentar, é natural preguntarse se teorías máis avanzadas da Álxebra como a Álxebra Homolóxica ou a Teoría de Módulos xogan tamén un papel relevante no estudo de sistemas lineares de ecuacións diferencias. Historicamente, os máis importantes pensadores enxalzaron a curiosidade como o motor do coñecemento. Así pois, non resulta estraño que matemáticos como Bernard Malgrange ou Mikio Sato realizaran os primeiros avances neste sentido, xa no século pasado, tratando de estudar (desde un punto de vista alxébrico) sistemas lineares de ecuacións en derivadas parciais. Estas personalidades iniciaron o que hoxe coñecemos como *Análise Alxébrica*, obtendo importantes resultados con impacto noutras teorías, por exemplo, a *Física matemática* ou a *Teoría de Sistemas Matemáticos*.

Recentemente, matemáticas e matemáticos como Eva Zerz e Alban Quadrat trataron de facer construtivas as ideas da Análise Alxébrica, o que permitiu implementar algoritmos que fan efectivos importantes teoremas deducidos hai case medio século. Ademais, nos últimos anos tamén se trataron de xeneralizar os devanditos resultados e algoritmos ao estudo doutro tipo de sistemas lineares, aplicándoos esencialmente á Teoría do Control.

A *Teoría do Control* é unha disciplina cuxo obxecto de estudo é o comportamento dos sistemas dinámicos. Neste contexto entendemos por *sistema dinámico* unha función do tempo que en calquera instante temporal proporciona o *estado* do sistema, isto é, un conxunto de números reais nun determinado espazo xeométrico. O obxectivo último da Teoría do Control é atopar modelos que permitan relacionar os argumentos de entrada do sistema cos estados que este poida tomar na súa evolución temporal. Algunhas das propiedades que se estudan na Teoría do Control son a a *controlabilidade* e a *observabilidade*. A controlabilidade caracteriza a posibilidade de manipular o estado do sistema utilizando só certos argumentos de entrada, mentres que a observabilidade é a noción dual: caracteriza a posibilidade de coñecer o estado do sistema utilizando só certos argumentos de saída.

Na Teoría do Control unha boa parte dos modelos de sistemas dinámicos pódense escribir como ecuacións ou sistemas lineares, e aí comeza a relación coa Análise Alxébrica. Aínda que poida parecer inofensivo, o estudo da Teoría do Control desde unha perspectiva alxébrica non é sinxelo. Así, a literatura sobre estes temas é con frecuencia moi avanzada, e dáse por feito que o lector ten un amplo coñecemento de Teoría de Módulos e Álxebra Homolóxica. É interesante e necesario entón realizar un tratamento introdutorio á teoría da Análise Alxébrica desde un punto de vista construtivo, que permita comprender as ideas básicas que se aplican, e este é o principal obxectivo do noso traballo. Para guiar a exposición concentrarémonos nos resultados que teñen un especial impacto na Teoría do Control. O tratamento pretende ser rigoroso e formal, mais verémonos na obriga de tomar prestados certos resultados pola limitación de tempo e espazo.

Para acadar o devandito propósito, precisaremos en primeiro lugar definir o que entendemos por sistema linear e tratar de ver como se pode estudar desde un punto de vista

alxébrico. Tales tarefas realízanse no capítulo 2. Así, definiremos o concepto de *álxebra de Ore* e probaremos un importante teorema (debido a Malgrange) que nos di cal é a estrutura alxébrica a estudar para caracterizar as propiedades dun sistema linear. Para comprender a natureza deste resultado precisamos introducir antes unha serie de definicións e propiedades básicas da Teoría de Módulos. Finalmente, tamén presentamos un tipo de aneis que nos serán de utilidade no posterior tratamento: os *aneis noetherianos*. Deste xeito, no primeiro capítulo tratamos de contextualizar o estudo que pretendemos realizar e de proporcionar as ferramentas máis básicas. Introducimos tamén varios exemplos, que agardamos axuden a facer máis lixeira a lectura, así como a comprender os conceptos que se van introducindo.

No capítulo 3 presentamos xa conceptos e resultados bastante máis avanzados que resultan imprescindibles na teoría da Análise Alxébrica, especialmente na versión construtiva que imos tratar. O máis importante será o de *resolución libre e finita* dun módulo pola esquerda finitamente presentado, que é a estrutura alxébrica que podemos asociar a todo sistema linear. A partir deste introdúcense os *grupos abelianos das extensións*, fundamentais en resultados que veremos están xa moi preto de poder aplicarse á Teoría do Control. Con todo, no enfoque construtivo é tamén moi importante que os conceptos introducidos poidan ser calculados ou caracterizados. Neste sentido veremos que é posible deseñar un algoritmo que calcule unha resolución libre e finita dun módulo pola esquerda finitamente presentado. O fundamento de tal algoritmo atópase nas técnicas de *bases de Gröbner*. Así pois, para comprendelo precisaremos definir que é unha base de Gröbner e adaptar a definición e os resultados existentes ao contexto no que nós nos atopamos.

No capítulo 4 tratamos de darlle sentido á exposición realizada no capítulo 3 expoñendo os resultados e teoremas de inmediata aplicación e exemplificándoos con importantes exemplos da Física Matemática: a *sucesión gradiente-rotacional-diverxencia* e as *ecuacións de Maxwell*. Máis concretamente, veremos que nestes resultados son esenciais os grupos abelianos das extensións introducidos no capítulo 3. Aínda que nas referencias máis recentes de Análise Alxébrica o tratamento é moi xeral, nós traballaremos neste capítulo baixo unha serie de hipóteses que simplifican a exposición, e agardamos que tamén axuden a facilitar a lectura. Finalmente, introducimos unha serie de conceptos propios da Teoría do Control e vemos como poden ser estudados a partir das ideas expostas.

Cómpre sinalar, antes de comezar, as aportacións máis persoais a este traballo. De forma máis xeral, como xa indicamos, o tratamento que presentamos é moito máis detallado (e agardamos que tamén sexa claro e didáctico) que as referencias habituais de Análise Alxébrica. Ademais, enfocamos os exemplos presentados dunha forma distinta, tratando de facer moito máis explícita a relación coa teoría exposta. Neste sentido é especialmente importante o exemplo das ecuacións de Maxwell, onde a exposición e presentación son marcadamente persoais. Ademais, é tamén este exemplo o escollido para exemplificar a utilidade dos algoritmos que no traballo presentamos, apoiándonos para iso en librarías do sistema de álxebra computacional SINGULAR [7].

2. Sistemas lineares e módulos pola esquerda finitamente presentados

Neste capítulo trataremos de amosar como os sistemas lineares de ecuacións en derivadas parciais (de agora en adiante, simplemente, sistemas lineares) poden ser estudados utilizando módulos pola esquerda finitamente presentados sobre un anel axeitado. O resultado fundamental é a existencia do *isomorfismo de Malgrange*, que veremos fai corresponder as solucións dun sistema linear con homomorfismos entre certos módulos pola esquerda.

2.1. Sistemas lineares e aneis de operadores diferenciais

Nesta sección imos introducir o concepto de anel de operadores diferenciais, que permite traballar cos sistemas lineares dunha forma sinxela e efectiva, e sobre o cal se desenvolve a teoría da Análise Alxébrica. Veremos tamén que isto encaixa no formalismo máis xeral das álxebras de Ore, que proporciona un marco común para expresar convenientemente todo tipo de sistemas de ecuacións funcionais lineares (sistemas de EDPs, EDOs ou ecuacións diferenciais con reflexión, por exemplo). A exposición que deseguido presentamos baséase nas feitas en [3,17,18], mais, porén, tentamos simplificala para facela facilmente entendible, tratando de xustificar a necesidade do devandito concepto.

O noso obxectivo é describir un sistema linear de EDPs na forma $R\eta = 0$, onde R é unha matriz con entradas nun determinado anel de polinomios e η é un vector de incógnitas. Pensemos, por exemplo, no oscilador harmónico simple, cuxa ecuación do movemento é de sobra coñecida:

$$\eta'' + \omega^2 \eta = 0. \tag{2.1}$$

Introducindo as variables $\eta_1 = \eta$ e $\eta_2 = \eta'$ a ecuación (2.1) escríbese do seguinte xeito:

$$\begin{aligned} \eta_1' - \eta_2 &= 0, \\ \eta_2' + \omega^2 \eta_1 &= 0. \end{aligned} \tag{2.2}$$

Empreguemos agora o operador derivada $\partial := \frac{d}{dt}$, que a cada $f \in \mathscr{C}^\infty(\mathbb{R})$ lle asigna a función $f' : t \in \mathbb{R} \to f'(t) := \frac{df}{dt}(t)$. Tamén podemos interpretar calquera $x \in \mathbb{R}$ fixado como o operador que a cada $f \in \mathscr{C}^\infty(\mathbb{R})$ lle asocia a función $x(f) := xf : t \in \mathbb{R} \to xf(t) := xf(t)$. Isto permite considerar o conxunto de operadores diferenciais $\sum_{i=0}^{r} a_i \partial^i$, con $a_i \in \mathbb{R}$, como o anel de polinomios $\mathbb{R}[\partial]$, entendendo que ∂^i denota a composición i-ésima do operador derivada consigo mesmo. Deste xeito, o sistema (2.2) pódese expresar como segue:

$$\begin{pmatrix} \partial & -1 \\ \omega^2 & \partial \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Así pois, conseguimos escribir (2.2) na forma $R\eta = 0$, sendo R unha matriz 2×2 con entradas en $\mathbb{R}[\partial]$. Aínda que o ilustramos mediante o caso particular do oscilador harmónico simple, está claro que isto xeneralízase a calquera sistema linear de EDOs con coeficientes constantes.

Así e todo, o noso obxectivo é describir sistemas lineares máis xerais, nos que os coeficientes poden ser polinomios nunha ou máis variables, ou mesmo funcións. Para tratar de formalizar todo isto convén introducir a noción de anel diferencial.

Definición 2.1. Un *anel diferencial* $(A, \{\delta_1, ..., \delta_n\})$ é un anel conmutativo A xunto cunhas *derivacións conmutativas*, $\delta_i : A \to A$, con $i = 1, ..., n$, isto é, aplicacións satisfacendo as seguintes propiedades:

(i)	$\delta_i \circ \delta_j = \delta_j \circ \delta_i,\ i, j = 1, ..., n.$	(conmutatividade)
(ii)	$\delta_i(a_1 + a_2) = \delta_i(a_1) + \delta_i(a_2),\ a_1, a_2 \in A,\ i = 1, ..., n.$	(linearidade)
(iii)	$\delta_i(a_1 a_2) = \delta_i(a_1)a_2 + a_1\delta_i(a_2),\ a_1, a_2 \in A,\ i = 1, ..., n.$	(regra de Leibniz)

Exemplo 2.2. Vexamos algúns exemplos sinxelos e ilustrativos de aneis diferenciais.

(1) Sexa $\mathscr{C}^\infty(\mathbb{R}^n)$ o conxunto das funcións infinitamente derivables definidas en todo $\mathbb{R}^n$, que claramente é un anel conmutativo. Entón $(\mathscr{C}^\infty(\mathbb{R}^n), \{\partial_1, ..., \partial_n\})$ é un anel diferencial, onde ∂_i, $i = 1, ..., n$, denotan as derivadas parciais, que baixo estas condicións de regularidade son conmutativas (en virtude do Teorema de Schwarz), e ademais sempre cumpren a linearidade e a regra de Leibniz.

(2) Sexa K un corpo. Entón o anel de polinomios nas variables $x_1, ..., x_n$ con coeficientes en K, $K[x_1, ..., x_n]$, ou o corpo de fraccións nas variables $x_1, ..., x_n$ con coeficientes en K, $K(x_1, ..., x_n)$, son tamén aneis diferenciais, onde as derivacións son as derivadas respecto das variables x_i, $\frac{\partial}{\partial x_i}$, con $i = 1, ..., n$.

Convén agora realizar un razoamento similar ao que nos permitiu atopar a forma matricial da ecuación do movemento do oscilador harmónico simple. Así, dado un anel diferencial $(A, \{\delta_1, ..., \delta_n\})$, interpretamos cada $a \in A$ como o operador que realiza a multiplicación (denotada pola xustaposición) por a, isto é, $a : b \in A \to ab \in A$. Podemos pensar tamén nos operadores que realizan as derivacións, que imos denotar polos símbolos ∂_i, $i = 1, ..., n$. Nestas circunstancias a multiplicación pasa a ser a composición de operadores.

Así pois, podemos considerar o conxunto de expresións $\sum_{i=0}^{r} a_i \partial_1^{i_1} \cdots \partial_n^{i_n}$, con $a_i \in A$ e $i_1, ..., i_n \in \mathbb{Z}_{\geq 0}$, onde $\mathbb{Z}_{\geq 0}$ denota o conxunto dos números enteiros non negativos. Notemos que este conxunto, que denotaremos por X, defínese de xeito idéntico ao conxunto subxacente ao anel de polinomios conmutativo nas variables $\partial_1, ...\partial_n$. A cuestión está en se X segue a ser un anel neste contexto máis xeral que vimos de introducir.

Baseándonos na teoría de polinomios non conmutativos de Ore desenvolta en [16], a primeira observación a realizar é que $(X, +)$ é claramente un grupo abeliano se definimos a operación $+$ como no caso conmutativo. Se queremos que $(X, +, \cdot)$ sexa un anel, debemos esixir que a multiplicación de polinomios cumpra a propiedade distributiva coa suma por ambos lados. Para iso só precisamos definir o produto de dous monomios: $a_1\partial_1^{i_1} \cdots \partial_n^{i_n}$ e $a_2\partial_1^{j_1} \cdots \partial_n^{j_n}$, isto é, $(a_1\partial_1^{i_1} \cdots \partial_n^{i_n})(a_2\partial_1^{j_1} \cdots \partial_n^{j_n})$. Xa que a multiplicación de polinomios (e de

monomios) debe ser tamén asociativa, e os operadores derivación conmutan entre si, chega con especificar que se entende por $\partial_j a$, con $j \in \{1,...,n\}$, para poder escribir o anterior produto como suma de monomios, isto é, como un elemento de X. Tomemos entón $a \in A$ calquera e vexamos como actúa o operador $\partial_j a$ sobre un $b \in A$ calquera, lembrando que a multiplicación en X é simplemente a composición de operadores:

$$(\partial_j a)(b) = \partial_j(a(b)) \overset{(i)}{=} \partial_j(ab) \overset{(ii)}{=} \delta_j(ab) \overset{(iii)}{=} a\delta_j(b)+\delta_j(a)b \overset{(iv)}{=} a\partial_j b+\delta_j(a)b = (a\partial_j+\delta_j(a))b.$$

En (i) utilizouse que o operador a realiza a multiplicación por a pola esquerda; en (ii) e (iv), a definición de ∂_j, e en (iii) a regra de Leibniz para a derivación. Tense entón a seguinte importante relación de conmutación:

$$\partial_j a = a\partial_j + \delta_j(a),\ j \in \{1,...,n\}. \tag{2.3}$$

De acordo co exposto en [16], as únicas condicións que debe cumprir (2.3) para que $(X,+,\cdot)$ sexa un anel son a linearidade e a regra de Leibniz, que se satisfán por definición. Así pois, atendendo a (2.3), é natural introducir un *anel de operadores diferenciais* do seguinte xeito.

Definición 2.3. Sexa $(A,\{\delta_1,...,\delta_n\})$ un anel diferencial. O *anel de operadores diferenciais parciais* en $\partial_1,...,\partial_n$, denotado por $D = A\langle\partial_1,...,\partial_n\rangle$, é o anel de polinomios en $\partial_1,...,\partial_n$ non conmutativo e con coeficientes en A, satisfacendo:

$$\partial_i\partial_j = \partial_j\partial_i,\ \partial_i a = a\partial_i + \delta_i(a),\ i,j = 1,...,n,\ a \in A.$$

Neste caso multidimensional, os elementos de D escríbense como $\sum_{|\nu|=0,...,r} a_\nu \partial^\nu$, con $a_\nu \in A$, $\nu = (\nu_1,...,\nu_n)^T \in \mathbb{N}^n$, $|\nu| = \nu_i + \cdots + \nu_n$ e $\partial^\nu = \partial^{\nu_1}\cdots\partial^{\nu_n}$.

Cando o anel diferencial $(A,\{\delta_1,...,\delta_n\})$ é o anel de polinomios $K[x_1,...,x_n]$ ou o corpo de fraccións $K(x_1,...,x_n)$, os aneis de operadores diferenciais parciais reciben un nome especial pola súa importancia histórica.

Definición 2.4. Sexa K un corpo. A *primeira álxebra de Weyl* é o anel de operadores diferenciais parciais $A_n(K) = K[x_1,...,x_n]\langle\partial_1,...,\partial_n\rangle$. A *segunda álxebra de Weyl* é o anel de operadores diferenciais parciais $B_n(K) = K(x_1,...,x_n)\langle\partial_1,...,\partial_n\rangle$.

As ferramentas introducidas permiten acadar o obxectivo marcado: expresar un amplo abano de sistemas lineares de EDPs na forma $R\eta = 0$, onde R é unha matriz con entradas nun anel de operadores diferenciais parciais. Isto encaixa nun marco aínda máis xeral no que non imos afondar, pero que convén coñecer, xa que a teoría da Análise Alxébrica é tamén aplicable en tal contexto. A exposición simple e concisa que se fai a continuación baséase na presentada en [3], os detalles pódense atopar en [18]. Antes de nada imos presentar a definición de K-álxebra, pois esixiremos que o conxunto sobre o que construímos a xeneralización do concepto de anel de operadores diferenciais teña esta estrutura.

Definición 2.5. Sexa K un corpo. Un espazo vectorial A sobre K dise unha *K-álxebra* se existe unha operación binaria $\cdot : A\times A \to A$ *bilinear*, isto é, que cumpre as seguintes propiedades:

(i) $(a+b)\cdot c = a\cdot c + b\cdot c$ $\quad a,b,c \in A.$
(ii) $c\cdot(a+b) = c\cdot a + c\cdot b$ $\quad a,b,c \in A.$
(iii) $(xa)\cdot(yb) = xy(a\cdot b)$ $\quad a,b \in A,\ x,by, \in K.$

Por simplicidade na notación, a anterior operación binaria tamén a denotaremos pola xustaposición, cando non haxa lugar á confusión.

Exemplo 2.6. $C^\infty(\mathbb{R}^n)$, $K[x_1,...,x_n]$ e $K(x_1,...,x_n)$ son K-álxebras sobre $\mathbb{R}$ e o corpo K, respectivamente.

Definición 2.7. Sexa A un anel. Sexa tamén $\sigma : A \to A$ un endomorfismo de aneis e $\delta : A \to A$ unha *σ-derivación*, isto é, unha aplicación que satisfai as seguintes propiedades:

$$\begin{array}{lll} (i) & \delta(a_1+a_2)=\delta(a_1)+\delta(a_2),\ a_1,a_2\in A. & \text{(linearidade)} \\ (ii) & \delta(a_1a_2)=\delta(a_1)a_2+\sigma(a_1)\delta(a_2),\ a_1,a_2\in A. & \text{(regra de Leibniz modificada)} \end{array}$$

Dicimos que o anel de polinomios en ∂ coa relación de conmutación

$$\partial a = \sigma(a)\partial + \delta_i(a),\ a\in A,$$

é unha *extensión de Ore*, e denotámolo por $A[\partial;\sigma,\delta]$. Se ademais A é unha K-álxebra, a anterior construción pode ser iterada. Así, para cada $m\in\mathbb{N}$, chamamos *álxebra de Ore* á extensión de Ore

$$(\cdots((A[\partial_1;\sigma_1,\delta_1])[\partial_2;\sigma_2,\delta_2])\cdots)[\partial_m;\sigma_m,\delta_m],$$

na que para cada $i=1,\dots,m$, os endomorfismos $\sigma_i : A_i \to A_i$ e as aplicacións $\delta_i : A_i \to A_i$, con $A_i =: ((\cdots(A[\partial_1;\sigma_1,\delta_1])\cdots)[\partial_{i-1};\sigma_{i-1},\delta_{i-1}])$, satisfán as seguintes condicións:

$$\begin{array}{lll} (i) & \delta_i\circ\delta_j=\delta_j\circ\delta_i,\ \sigma_i\circ\sigma_j=\sigma_j\circ\sigma_i,\ \sigma_i\circ\delta_j=\delta_j\circ\sigma_i, & \\ & \delta_i\circ\sigma_j=\sigma_j\circ\delta_i,\ j<i. & \text{(conmutatividade)} \\ (ii) & \delta_i(a_1+a_2)=\delta_i(a_1)+\delta_i(a_2),\ a_1,a_2\in A. & \text{(linearidade)} \\ (iii) & \delta_i(a_1a_2)=\delta_i(a_1)a_2+\sigma_i(a_1)\delta_i(a_2),\ a_1,a_2\in A. & \text{(regra de Leibniz modificada)} \\ (iv) & \sigma_i(\partial_j)=\partial_j,\ \delta_i(\partial_j)=0,\ j<i. & \end{array}$$

Denotaremos á anterior álxebra de Ore $A[\partial_1;\sigma_1,\delta_1]\cdots[\partial_m;\sigma_m,\delta_m]$.

Observación 2.8. A condición (iv) da anterior definición garante a conmutatividade das variables ∂_i, $i=1,\dots,m$ na álxebra de Ore $A[\partial_1;\sigma_1,\delta_1]\cdots[\partial_m;\sigma_m,\delta_m]$, tal e como se demostra en [18]. Como se demostra en [21], esta construción é análoga á do conxunto de polinomios nas variables $\partial_1,\dots,\partial_m$ con coeficientes na K-álxebra A e coa relación de conmutación

$$\partial_i a = \sigma_i(a)\partial_i + \delta_i(a),\ a\in A,\ i=1,...,m,$$

onde os endomorfismos σ_i e as aplicacións δ_i cumpren as condicións da anterior definición, para $i=1,\dots,m$.

Exemplo 2.9. Da anterior definición séguese inmediatamente que os aneis de operadores diferenciais parciais, $D=A\langle\partial_1,...,\partial_n\rangle$, son álxebras de Ore cando A é unha K-álxebra, tomando como endomorfimos σ_i a identidade do anel diferencial: $\sigma_i=\mathrm{Id}_A$, $i=1,...,n$. Así pois, de acordo co Exemplo 2.6, a primeira e a segunda álxebra de Weyl son álxebras de Ore, pero tamén $\mathscr{C}^\infty(\mathbb{R}^n)\langle\partial_1,...,\partial_n\rangle$, sendo ∂_i, $i=1,...,n$, as derivadas parciais usuais.

Da exposición realizada debemos observar que as ecuacións do estilo $R\eta = 0$, con R unha matriz con entradas nunha álxebra de Ore, representan case todo tipo de sistemas lineares de ecuacións funcionais (por exemplo, sistemas de ecuacións diferenciais con retardo temporal). Deste xeito, os resultados que presentaremos neste traballo (no que particularizamos para sistemas lineares de EDPs) son en realidade válidos para moitos outros tipos de sistemas lineares.

Así e todo, cómpre sinalar que o obxectivo da introdución do concepto de álxebra de Ore é só amosar a existencia de determinados aneis de polinomios que resultan idóneos de cara a formular sistemas lineares. A teoría que se desenvolverá nas seguintes seccións e capítulos formúlase en condicións máis xerais, nas que a matriz R do sistema $R\eta = 0$ ten as súas entradas, simplemente, nun anel D. En ocasións será necesario esixir que este cumpra algunhas propiedades adicionais, que en calquera caso as álxebras de Ore satisfán. Así pois, por claridade na exposición, consideramos en xeral que D é un anel, esixindo ademais a estrutura de álxebra de Ore cando resulte conveniente ou necesario.

Para concluír imos definir de forma precisa o que nós entenderemos por sistema linear e por conxunto de solucións dun sistema linear. Todo o exposto ata o momento permitiunos caracterizar a matriz R dun sistema linear $R\eta = 0$, pero nada dixemos do vector de incógnitas η. Se as entradas de R se atopan nun anel D, e R ten q filas e p columnas, entón $R \in D^{q\times p}$, co que podemos escribir o sistema explicitamente como:

$$\begin{aligned} r_{11}\eta_1 + &\quad \dots \quad + r_{1p}\eta_p = 0, \\ &\quad \dots \\ r_{q1}\eta_1 + &\quad \dots \quad + r_{qp}\eta_p = 0. \end{aligned}$$

As solucións η_j, $j = 1, \dots, p$, buscámolas nun espazo que nos permita multiplicar pola esquerda polos r_{ij}, $i = 1, \dots, q$, e sumar. Dito doutro xeito, buscamos as solucións η_j, $j = 1, \dots, p$ nun determinado *D-módulo pola esquerda* F. Cómpre sinalar que consideraremos sempre aneis con unidade, isto é, $1 \neq 0$. Por simplicidade na exposición obviaremos esta hipótese, sendo conscientes de que está implícita no enunciado *sexa D un anel*. Pasamos entón a definir que entendemos por un D-módulo pola esquerda. Tamén damos a definición de D-módulo pola dereita, por completitude e porque será de utilidade nos vindeiros capítulos.

Definición 2.10. Sexa D un anel. Un *D-módulo pola esquerda* é un grupo abeliano $(M, +)$ xunto cunha operación externa:

$$\begin{array}{ccc} D \times M & \longrightarrow & M \\ (d, m) & \longrightarrow & dm \end{array}$$

que cumpre as seguintes propiedades:

$$\begin{array}{lll} (i) & (d + d')m = dm + d'm, & d, d' \in D,\ m \in M. \\ (ii) & d(m + m') = dm + dm', & d \in D,\ m, m' \in M. \\ (iii) & (dd')m = d(d'm), & d, d' \in D,\ m \in M. \\ (iv) & 1m = m, & m \in M. \end{array}$$

De forma análoga, un *D-módulo pola dereita* é un grupo abeliano $(M, +)$ xunto cunha operación externa:

$$\begin{array}{ccc} D \times M & \longrightarrow & M \\ (d, m) & \longrightarrow & md \end{array}$$

que cumpre as seguintes propiedades:

$$\begin{array}{lll} (i) & m(d+d') = md + md', & d, d' \in D,\ m \in M. \\ (ii) & (m+m')d = md + m'd, & d \in D,\ m, m' \in M. \\ (iii) & m(dd') = (md)d', & d, d' \in D,\ m \in M. \\ (iv) & m1 = m, & m \in M. \end{array}$$

Exemplo 2.11. Imos retomar o exemplo do oscilador harmónico simple para tratar de exemplificar a teoría que vimos de introducir, e tamén para amosar a relevancia que teñen os módulos na Análise Alxébrica. Xa vimos que a ecuación do oscilador harmónico simple pódese escribir de forma matricial como segue:

$$\begin{pmatrix} \partial & -1 \\ \omega^2 & \partial \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \tag{2.4}$$

onde ∂ denota a derivada respecto da variable t. A frecuencia de oscilación ω é un número real no caso do oscilador harmónico simple. Así pois, podemos considerar que a matriz R que define o sistema ten as súas entradas no anel de operadores diferenciais $\mathbb{R}[\partial]$ (que é claramente unha álxebra de Ore). As solucións η debémolas buscar nun $\mathbb{R}[\partial]$-módulo pola esquerda. Vexamos que $\mathscr{C}^\infty(\mathbb{R})$ cumpre as propiedades $(i), (ii), (iii)$ e (iv) da definición de módulo pola esquerda definindo a operación externa como segue:

$$\left(\sum_{i=0}^{r} a_i \partial^i, f \right) \in \mathbb{R}[\partial] \times \mathscr{C}^\infty(\mathbb{R}) \to \sum_{i=0}^{r} a_i \partial^i f = \sum_{i=0}^{r} a_i \frac{d^i f}{dt^i}.$$

- En primeiro lugar, a operación externa está ben definida, por ser $\mathscr{C}^\infty(\mathbb{R})$ o conxunto das funcións reais (na variable t) infinitamente derivables.
- A propiedade (i) é consecuencia da linearidade da definición da operación externa.
- A propiedade (ii) é a linearidade da derivada.
- A propiedade (iii) é a asociatividade da composición de operadores.
- A propiedade (iv) é trivial.

Será necesario concretar tamén que se entende por *D-submódulo pola esquerda* dun D-módulo pola esquerda M.

Definición 2.12. Sexan $(D, +, \cdot)$ un anel e M un D-módulo pola esquerda. Un subconxunto N de M é un *D-submódulo pola esquerda* se é un D-módulo pola esquerda coa estrutura de M, isto é, se satisfai as seguintes propiedades:

$$\begin{array}{ll} (i) & (N, +) \text{ é un subgrupo aditivo de } (M, +). \\ (ii) & \text{Para cada } x \in N \text{ e cada } d \in D,\ dx \in N. \end{array}$$

Considerando o anel D como un D-módulo pola esquerda, todo D-submódulo pola esquerda é un *ideal pola esquerda*. Se M é un D-módulo pola dereita, as definicións de *D-submódulo pola dereita* e *ideal pola dereita* son análogas, cambiando só a condición (ii) por $(ii)'$:

$$(ii)' \quad \text{Para cada } x \in N \text{ e cada } d \in D,\ xd \in N.$$

Exemplo 2.13. Vexamos que o conxunto de solucións da ecuación do oscilador harmónico (2.4) é un $\mathbb{R}[\partial]$-submódulo pola esquerda do $\mathbb{R}[\partial]$-módulo pola esquerda $\mathscr{C}^\infty(\mathbb{R})^2$.

- Para ver que o conxunto de solucións é un subgrupo aditivo de $\left(\mathscr{C}^\infty(\mathbb{R})^2, +\right)$ chega con comprobar que é non baleiro e que a resta de dúas solucións é tamén solución. Ambos aspectos son consecuencia de que (2.4) sexa unha ecuación homoxénea, pois por un lado tense a solución trivial $\eta = 0$, e polo outro $R(\eta_1 - \eta_2) = R\eta_1 - R\eta_2 = 0 - 0 = 0$ para η_1, η_2 solucións calquera.
- Para a segunda condición basta observar que $\mathbb{R}[\partial]$ é un anel conmutativo, lembrando a relación de conmutatividade máis xenérica dada en (2.3) e que a derivada de calquera número real é cero. Así, $R\left(\sum_{i=0}^{r} a_i \partial^i \eta\right) = \sum_{i=0}^{r} a_i \partial^i (R\eta) = \sum_{i=0}^{r} a_i \partial^i 0 = 0$.

Os Exemplos 2.11 e 2.13 amosan explicitamente como os conceptos de D-módulo e D-submódulo pola esquerda aparecen de xeito natural ao estudar este tipo de sistemas desde un punto de vista alxébrico. Os D-módulos pola esquerda cumpren, en xeral, as mesmas propiedades fundamentais que os D-módulos sobre aneis conmutativos, exceptuando algún caso puntual, que será indicado cando sexa necesario. No resto de situacións empregaremos os ben coñecidos resultados básicos sobre módulos. Uns dos conceptos dos que tiraremos máis proveito no que segue son os de *módulos pola esquerda finitamente xerados* e *finitamente presentados*. As definicións que a continuación amosamos son inmediatas xeneralizacións das do caso máis convencional no que temos un anel conmutativo e un módulo pola esquerda e pola dereita (en ocasións chamado *bimódulo*). Para presentalas cómpre introducir antes o que é un *homomorfismo de D-módulos pola esquerda*, que será tamén de utilidade na seguinte sección.

Definición 2.14. Sexan M, N dous D-módulos pola esquerda, onde D é un anel. Dicimos que unha aplicación $f : M \longrightarrow N$ é un *homomorfismo de D-módulos pola esquerda* se satisfai as seguintes propiedades:

$$\begin{array}{ll} (i) & f(m_1 + m_2) = f(m_1) + f(m_2), \quad m_1, m_2 \in M. \\ (ii) & f(dm) = df(m), \quad d \in D,\ m \in M. \end{array}$$

Para M, N dous D-módulos pola dereita, a definición de *homomorfismo de D-módulos pola dereita* é análoga, cambiando a condición (ii) por $(ii)'$:

$$(ii)' \quad f(md) = f(m)d, \quad d \in D,\ m \in M.$$

Sobre homomorfismos de D-módulos pola esquerda cómpre recordar o *Primeiro Teorema de Isomorfía*, que pasamos a enunciar. A demostración pódese consultar, por exemplo, en [21]. Notemos que para o caso de homomorfismos de D-módulos pola dereita tense un resultado análogo, mais non o utilizaremos no posterior tratamento.

Teorema 2.15 (Primeiro Teorema de Isomorfía). *Sexa $f : M \longrightarrow N$ un homomorfismo de D-módulos pola esquerda, con D un anel. Entón existe un isomorfismo de D-módulos pola esquerda*

$$\phi : M/\ker f \longrightarrow \mathrm{Im} f$$

dado por

$$\phi : m + \ker f \longmapsto f(m).$$

Definición 2.16. Sexa D un anel e M un D-módulo pola esquerda. Dicimos que M é *finitamente xerado* se existe $\{a_1,...,a_n\}$ un conxunto finito xerador de M, isto é, se $x \in M$, entón $x = d_1a_1 + d_2a_2 + \cdots + d_na_n$, con $d_1, d_2, ..., d_n \in D$. Equivalentemente, se existe un homomorfismo de D-módulos pola esquerda sobrexectivo:

$$\begin{array}{rccc} \pi: & D^{1\times n} & \longrightarrow & M \\ & (d_1\ d_2\ \cdots\ d_n) & \longrightarrow & d_1a_1 + d_2a_2 + \cdots + d_na_n \end{array}$$

para algún $n \in \mathbb{N}$. Nestas circunstancias, se o D-submódulo pola esquerda $\ker(\pi)$ de $D^{1\times n}$ é tamén finitamente xerado, M dise *finitamente presentado*. Dicimos entón que π é unha *presentación libre e finita* de M, e que $\ker\pi$ é o *módulo de relacións* de M. As definicións para un D-módulo pola dereita M son análogas: basta cambiar $x = d_1a_1 + d_2a_2 + \cdots + d_na_n$ por $x = a_1d_1 + a_2d_2 + \cdots + a_nd_n$, e o homomorfismo de D-módulos pola esquerda sobrexectivo π polo seguinte homomorfismo de D-módulos pola dereita sobrexectivo:

$$\begin{array}{rccc} \pi': & D^{n\times 1} & \longrightarrow & M \\ & (d_1\ d_2\ \cdots\ d_n)^T & \longrightarrow & a_1d_1 + a_2d_2 + \cdots + a_nd_n. \end{array}$$

Para rematar esta sección imos concretar a terminoloxía que utilizaremos no resto do traballo no que a sistemas lineares (e ás súas solucións) se refire.

Definición 2.17. Sexa $R \in D^{q\times p}$ unha matriz $q \times p$ con entradas nun anel, D. Chamamos *sistema linear* ao conxunto de ecuacións homoxéneas que define a matriz R, $R\eta = 0$. Dado un D-módulo pola esquerda, F, dicimos que $\eta \in F^{p\times 1}$ é unha *solución* do sistema linear se se cumpre a ecuación $R\eta = 0$. O *conxunto de solucións* do sistema linear:

$$\ker(R.) := \{\eta \in F^{p\times 1} | R\eta = 0\},$$

adoita chamarse tamén *comportamento*.

2.2. O isomorfismo de Malgrange

Unha vez exposto o noso marco de traballo estamos en condicións de presentar un dos resultados básicos da Análise Alxébrica, que establece que as propiedades do sistema linear $R\eta = 0$ poden ser estudadas mediante os D-módulos pola esquerda $M = D^{1\times p}/(D^{1\times q}R)$ e F. Máis concretamente, comprobaremos que se pode definir un isomorfismo de grupos abelianos entre $\ker(R.)$ e $\hom(M, F)$. Así e todo, cómpre realizar unha serie de observacións antes de enunciar e demostrar o devandito resultado.

En primeiro lugar notemos que se D é un anel e $p,\ q \in \mathbb{N}$, entón $D^{q\times p}$, isto é, o conxunto de matrices $q \times p$ con entradas en D, é un D-módulo pola esquerda coa suma de matrices e a multiplicación por elementos de D habituais. En particular, o conxunto de vectores fila ou columna de tamaño p ou q con entradas en D é tamén un D-módulo pola esquerda.

Sexa agora unha matriz $R \in D^{q\times p}$ e consideremos o sistema linear $R\eta = 0$. Tomemos unha solución $\eta = (\eta_1, ..., \eta_p)^T \in F^{p\times 1}$, con F un D-módulo pola esquerda. Como $R \in D^{q\times p}$ e $\eta \in F^{p\times 1}$, resulta que $R\eta \in F^{q\times 1}$. Deste xeito, as *consecuencias lineares* do sistema $R\eta = 0$

(ou restricións lineares que satisfai a solución η) obtéñense multiplicando a matriz R pola esquerda por matrices de q columnas. En efecto, se tomamos $S \in D^{r\times q}$, con $r \in \mathbb{N}$, resulta que $(SR)\eta = S(R\eta) = 0$.

Para caracterizar todas as consecuencias lineares do sistema habitualmente estúdase o conúcleo do homomorfismo de D-módulos pola esquerda $.R\colon D^{1\times q} \to D^{1\times p}$, que leva a cada $\mu \in D^{1\times q}$ en $.R(\mu) = \mu R \in D^{1\times p}$. O devandito conúcleo $M = D^{1\times p}/\mathrm{Im}(.R) = D^{1\times p}/(D^{1\times q}R)$ é tamén un D-módulo pola esquerda. Todo isto motiva a seguinte definición:

Definición 2.18. Sexa $R\eta = 0$ un sistema linear, onde $R \in D^{q\times p}$, e F é un D-módulo pola esquerda. Definimos o *módulo do sistema* $R\eta = 0$ como o seguinte D-módulo pola esquerda:

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

Observación 2.19. Tamén nos referiremos ao módulo do sistema $R\eta = 0$, $M = D^{1\times p}/(D^{1\times q}R)$, como o *$D$-módulo pola esquerda finitamente presentado por R*. Vexamos a continuación a razón de que empregemos esta denominación.

Denotemos por R_{i*}, con $i = 1, ..., q$, o vector fila de dimensión p que se obtén tomando a fila i-ésima de R, logo $R_{i*} \in D^{1\times p}$, $i = 1, ..., q$. Construamos agora o D-submódulo pola esquerda de $D^{1\times p}$ finitamente xerado por $R_{1*}, ..., R_{q*}$:

$$N = \{d_1R_{1*} + \cdots + d_qR_{q*} \mid d_1, ..., d_q \in D\}.$$

Para cada $\mu = (\mu_1, ..., \mu_q) \in D^{1\times q}$, recordando como se efectúa a multiplicación de matrices, resulta que $\mu R = \mu_1R_{1*} + \cdots + \mu_qR_{q*}$. Así:

$$N = \{\mu R \mid \mu = (\mu_1, ..., \mu_q) \in D^{1\times q}\} = \mathrm{Im}(.R) = D^{1\times q}R.$$

Consideremos agora a proxección canónica de $D^{1\times p}$ no D-módulo cociente pola esquerda $M = D^{1\times p}/(D^{1\times p}R)$:

$$\begin{array}{rcl} \pi : D^{1\times p} & \longrightarrow & M \\ \lambda & \longmapsto & \pi(\lambda) = \lambda + D^{1\times q}R \end{array}$$

que a cada $\lambda \in D^{1\times p}$ lle asigna a súa clase segundo a relación de equivalencia:

$$\lambda, \gamma \in D^{1\times p},\ \lambda \sim \gamma :\Longleftrightarrow \gamma - \lambda \in D^{1\times q}R.$$

A proxección canónica é un homomorfismo de D-módulos pola esquerda sobrexectivo, e $\ker \pi = D^{1\times q}R$. Daquela, como $D^{1\times p}$ é un D-módulo libre de rango finito (e $D^{1\times q}R$ é finitamente xerado) tense que π é unha presentación libre e finita de M, en base á Definición 2.16. Así, M é un D-módulo pola esquerda finitamente presentado, e depende só da matriz R, o que xustifica a nomenclatura introducida.

Coa discusión previa á anterior definición tratamos de explicar como aparece de xeito natural o módulo do sistema cando estudamos as relacións lineares que satisfán as compoñentes de calquera solución. Aínda así, a maior utilidade radica no resultado que a continuación presentamos e demostramos, baseándonos no exposto en [17]. Con todo, non nos limitamos a transcribir a propia demostración, pois tratamos de facela máis comprensible explicando en detalle cada paso. Posteriormente, no Exemplo 2.21 retomaremos o caso do oscilador harmónico simple para ilustrar as propiedades do módulo do sistema cun caso particular.

Teorema 2.20 (Isomorfismo de Malgrange). *Sexan D un anel, $R \in D^{q\times p}$ unha matriz $q \times p$ con entradas en D, M o módulo do sistema $R\eta = 0$ e $\pi\colon D^{1\times p} \to M$ a proxección canónica sobre M. Sexan tamén $\{f_1, ..., f_p\}$ a base canónica de $D^{1\times p}$, $y_j = \pi(f_j)$, $j = 1, ..., p$, e F un D-módulo pola esquerda. Entón tense o seguinte isomorfismo de grupos abelianos:*

$$\begin{array}{rcl} \hom(M,F) & \longrightarrow & \ker(R.) \\ \phi & \longmapsto & y = (\phi(y_1), ..., \phi(y_p))^T \end{array}$$

que denominaremos isomorfismo de Malgrange*, e que establece unha correspondencia entre os elementos de* $\hom(M,F)$ *e* $\ker(R.)$.

Demostración. Sexan $\{f_1, ..., f_p\}$, $\{y_1, ..., y_p\}$ como no enunciado do teorema, logo $y_j = \pi(f_j) = f_j + D^{1\times q}R$ para cada $j = 1, ..., p$. Empregando a sobrexectividade da proxección canónica:

$$m \in M,\ \exists \lambda \in D^{1\times p} \mid \pi(\lambda) = m. \tag{2.5}$$

Podemos ademais expresar λ en coordenadas da base canónica de $D^{1\times p}$, $\lambda = (\lambda_1, ..., \lambda_p)$, isto é, $\lambda_1 f_1 + ... + \lambda_p f_p$, con $\lambda_i \in D,\ i = 1, ..., p$. Utilizaremos agora que π é un homomorfismo de D-módulos pola esquerda, logo tomando $m \in M$ e $\lambda \in D^{1\times p}$ tal que $m = \pi(\lambda)$:

$$m = \pi(\lambda) = \pi\left(\sum_{i=1}^{p} \lambda_i f_i\right) \overset{(a)}{=} \sum_{i=1}^{p} \pi(\lambda_i f_i) \overset{(b)}{=} \sum_{i=1}^{p} \lambda_i \pi(f_i) = \sum_{i=1}^{p} \lambda_i y_i. \tag{2.6}$$

Na igualdade (a) empregamos que $\pi(\lambda + \mu) = \pi(\lambda) + \pi(\mu)$, con $\lambda, \mu \in D^{1\times p}$, e na (b), que $\pi(d\lambda) = d\pi(\lambda)\ \forall d \in D$, con $\lambda \in D^{1\times p}$, que son as propiedades que verifica todo homomorfismo de D-módulos pola esquerda. Xuntando (2.5) e (2.6) temos que $\{y_1, ..., y_p\}$ é un conxunto de xeradores de M.

Doutra banda, recuperando a notación $R_{i*} \in D^{1\times p}$ para os vectores fila de tamaño p que constitúen as filas de R, observamos que $R_{i*} = e_i R$, onde e_i é o vector i-ésimo da base canónica de $D^{1\times q}$. Como $\ker \pi = D^{1\times q}R$, $\pi(R_{i*}) = 0$, con $i = 1, ..., q$. Así,

$$\pi(R_{i*}) = \pi\left(\sum_{j=1}^{p} R_{ij} f_j\right) \overset{(a)}{=} \sum_{j=1}^{p} \pi(R_{ij} f_j) \overset{(b)}{=} \sum_{j=1}^{p} R_{ij}\pi(f_j) = \sum_{j=1}^{p} R_{ij} y_j = 0,$$

onde empregamos (a), (b) e que $R_{i*} = \sum_{i=1}^{p} R_{ij} f_j$. Isto ocorre para cada $i = 1, ..., q$, de xeito que $\{y_1, ..., y_p\}$ é un conxunto de xeradores de M coas relacións $\sum_{j=1}^{q} R_{ij} y_j = 0$.

Definimos agora a seguinte aplicación:

$$\begin{array}{rcl} \chi : \ker(R.) & \longrightarrow & \hom(M,F) \\ \eta & \longmapsto & \chi(\eta) = \phi_\eta : \begin{array}{rcl} M & \longrightarrow & F \\ \pi(\lambda) & \longmapsto & \phi_\eta(\pi(\lambda)) = \lambda\eta = \lambda_1\eta_1 + ... + \lambda_p\eta_p \end{array} \end{array}$$

Tense que:

- $(\ker(R.), +)$ é un grupo abeliano, onde $+$ é a operación suma definida no D-módulo pola esquerda F. Tamén $(\hom(M,F), +)$ é un grupo abeliano, onde a suma de homomorfismos defínese da forma usual.

- *A aplicación χ está ben definida.* Chega con comprobar que $\chi(\eta) \in \hom(M,F)$ para calquera $\chi \in \ker(R.)$. Sexa entón $\eta \in \ker(R.)$ arbitrariamente fixado.

  En primeiro lugar imos ver que a imaxe de calquera $m \in M$ por $\chi(\eta)$ non depende do representante escollido, isto é:

  $$m = \pi(\lambda) = \pi(\lambda'),\ \lambda, \lambda' \in D^{1\times p} \Longrightarrow \phi_\eta(\pi(\lambda)) = \phi_\eta(\pi(\lambda')).$$

  Lembrando que π é a proxección canónica en $M = D^{1\times p}/(D^{1\times q}R)$, chegamos a que $\pi(\lambda) = \pi(\lambda') \iff \lambda' - \lambda \in D^{1\times q}R$. Entón podemos escribir, para algún $\nu \in D^{1\times q}R$, $\lambda' - \lambda = \nu R$. Así pois, xa que $\eta \in \ker(R.)$, tense que $R\eta = 0$, e daquela:

  $$\phi_\eta(\pi(\lambda)) = \lambda\eta = (\lambda' - \nu R)\eta = \lambda'\eta - \nu(R\eta) = \lambda'\eta = \phi_\eta(\lambda'),$$

  que era o que queriamos probar. Ademais, cómpre observar que $\lambda\eta \in F$ por ser F un D-módulo pola esquerda, e a notación empregada é compatible co produto de matrices (notemos que λ e η son vectores fila e columna do mesmo tamaño).

  Vexamos agora que $\phi_\eta \in \hom(M,F)$. Sexan $m, m' \in M$, $\pi(\lambda) = m$, $\pi(\lambda') = m'$ para $\lambda, \lambda' \in D^{1\times p}$ e $d \in D$ escollidos arbitrariamente. Utilizando a definición de ϕ_η e que a proxección canónica é un homomorfismo de D-módulos pola esquerda:

  $$\phi_\eta(\pi(\lambda) + \pi(\lambda')) = \phi_\eta(\pi(\lambda + \lambda')) = (\lambda + \lambda')\eta = \lambda\eta + \lambda'\eta' = \phi_\eta(\pi(\lambda)) + \phi_\eta(\pi(\lambda')),$$

  onde tamén se emprega a linearidade do produto de matrices. Tamén se ten que:

  $$\phi_\eta(d\pi(\lambda)) = \phi_\eta(\pi(d\lambda)) = (d\lambda)\eta = d(\lambda\eta) = d\phi_\eta(\lambda).$$

  Xuntando todo, temos que $\phi_\eta \in \hom(M,F)$, e daquela χ está ben definida.

- *χ é un homomorfismo de grupos abelianos*. Sexan $\eta_1, \eta_2 \in \ker(R.)$ calquera e comprobemos que $\chi(\eta_1 + \eta_2) = \chi(\eta_1) + \chi(\eta_2)$. Dado que $\chi(\eta) \in \hom(M,F)$ para cada $\eta \in \ker(R.)$, chega con ver que $\chi(\eta_1 + \eta_2)(\pi(\lambda)) = \chi(\eta_1)(\pi(\lambda)) + \chi(\eta_2)(\pi(\lambda))$, para un $\lambda \in D^{1\times p}$ arbitrario. Empregando de novo a linearidade do produto de matrices:

  $$\chi(\eta_1 + \eta_2)(\pi(\lambda)) = \lambda(\eta_1 + \eta_2) = \lambda\eta_1 + \lambda\eta_2 = \chi(\eta_1)(\pi(\lambda)) + \chi(\eta_2)(\pi(\lambda)),$$

  logo χ é, en efecto, un homomorfismo de grupos abelianos.

- *χ é inxectivo*. Como xa vimos que χ é un homomorfismo de grupos, basta comprobar que $\ker\chi = \{0\}$, onde 0 é o elemento neutro de $F^{p\times 1}$.

  Supoñamos $\chi(\eta) = 0$, de xeito que para calquera $\lambda \in D^{1\times p}$, $\chi(\eta)(\pi(\lambda)) = \lambda\eta = 0$. Tomando $\lambda = f_j$ o elemento j-ésimo da base canónica de $D^{1\times p}$:

  $$\chi(\eta)(\pi(f_j)) = f_j\eta = \eta_j = 0 \iff \eta_j = 0,$$

  onde utilizamos que, traballando en coordenadas da base canónica, o vector f_j ten só un 1 na posición j, e por ser F un D-módulo pola esquerda $1\zeta = \zeta$, con $\zeta \in F$. Como isto é certo para calquera $j = 1, ..., p$, tense que $\chi(\eta) = 0$ implica $\eta = 0$.

- χ *é sobrexectivo*. Sexa $\phi \in \hom(M,F)$ calquera e definamos $\eta = (\phi(y_1),...,\phi(y_p))$, que trivialmente é un elemento de $F^{1\times p}$. Comprobemos que ademais pertence a $\ker(R.)$, isto é $R\eta = 0$. Dado que $R\eta \in F^{1\times q}$, podemos verificar simplemente se satisfán as ecucións $\sum_{i=1}^{p} R_{ij}\eta_j = 0$ para cada $i = 1,...,q$.

$$\sum_{i=1}^{p} R_{ij}\eta_j = \sum_{i=1}^{p} R_{ij}\phi(y_j) \overset{(i)}{=} \phi\left(\sum_{i=1}^{p} R_{ij}y_j\right) \overset{(ii)}{=} \phi(0) \overset{(iii)}{=} 0 \ \forall i = 1,...,q.$$

  En (i) utilizamos as propiedades (a) e (b) que ϕ satisfai como homomorfismo de D-módulos pola esquerda; en (ii), as relacións que vimos cumpren os xeradores $\{y_1,...,y_p\}$, e en (iii), que $f(0) = 0$ para calquera f homomorfismo de D-módulos pola esquerda.

  Finalmente basta ver que $\chi(\eta) = \phi$. Para iso tomamos $\lambda \in D^{1\times p}$ calquera e comprobamos se $\chi(\eta)(\pi(\lambda)) = \phi(\pi(\lambda))$, o que resulta suficiente debido á sobrexectividade de π. Por unha banda:

$$\chi(\phi(y_1),...,\phi(y_p))(\pi(\lambda)) = \sum_{i=1}^{p} \lambda_i\phi(y_i),$$

  onde escribimos λ en coordenadas da base canónica de $D^{1\times p}$, $\lambda = (\lambda_1,...,\lambda_p)$. Pola outra banda, utilizando as propiedades de π e ϕ como homomorfismos de D-módulos pola esquerda, e lembrando que $y_j = \pi(f_j)$ para cada $j = 1,...,p$:

$$\phi(\pi(\lambda)) = \phi\left(\pi\left(\sum_{i=1}^{p}\lambda_i f_i\right)\right) = \phi\left(\pi\sum_{i=1}^{p}\lambda_i y_i\right) = \sum_{i=1}^{p}\lambda_i\phi(y_i)$$

  o que demostra a sobrexectividade de χ.

Así pois, acabamos de comprobar que χ é un isomorfismo de grupos abelianos. Aínda máis, utilizando o último punto, no que vimos a sobrexectividade de χ, queda claro que o isomorfismo inverso, χ^{-1}, está dado por:

$$\begin{aligned} \chi^{-1} : \hom(M,F) &\longrightarrow \ker(R.) \\ \phi &\longrightarrow y = (\phi(y_1),...,\phi(y_p))^T \end{aligned}$$

que é o isomorfismo de Malgrange. Isto remata a demostración. ■

Este resultado dinos que o sistema linear $R\eta = 0$ pode ser estudado mediante o módulo do sistema, $M = D^{1\times p}/(D^{1\times q}R)$, e o D-módulo pola esquerda F no que se buscan as solucións. As propiedades de M como D-módulo pola esquerda veremos que proporcionan abondosa información teórica sobre o sistema linear. Para rematar esta sección ilustraremos o teorema que vimos de probar co seguinte exemplo.

Exemplo 2.21. Consideremos de novo o caso do oscilador harmónico:

$$\begin{pmatrix} \partial & -1 \\ \omega^2 & \partial \end{pmatrix}\begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{2.7}$$

Xa vimos que a matriz R do sistema ten as súas entradas no anel de operadores diferenciais $\mathbb{R}[\partial]$, e que podemos buscar as solucións no $\mathbb{R}[\partial]$-módulo pola esquerda $\mathscr{C}^\infty(\mathbb{R})^2$.

Imos utilizar este caso sinxelo para ilustrar a correspondencia que se segue do isomorfismo de Malgrange, así como as propiedades do módulo do sistema no que a relacións lineares se refire. En primeiro lugar, notemos que o módulo do sistema é simplemente $M = \mathbb{R}[\partial]^{1\times 2}/(\mathbb{R}[\partial]^{1\times 2}R)$, e que a proxección canónica, por ser un homomorfismo de $\mathbb{R}[\partial]$-módulos pola esquerda, queda definida proporcionando a imaxe de $f_1 = (1,0)$ e $f_2 = (0,1)$:

$$\begin{array}{rcl} \pi : \mathbb{R}[\partial]^{1\times 2} & \longrightarrow & M = \mathbb{R}[\partial]^{1\times 2}/(\mathbb{R}[\partial]^{1\times 2}R) \\ f_1 & \longmapsto & f_1 + \mathbb{R}[\partial]^{1\times 2}R = y_1 \\ f_2 & \longmapsto & f_2 + \mathbb{R}[\partial]^{1\times 2}R = y_2 \end{array}$$

Podemos comprobar que y_1 e y_2 satisfán as relacións dadas polas filas de R. Dado que se trata de cálculos moi similares, exemplificámolo só para a primeira fila:

$$\begin{array}{rl} \partial y_1 - y_2 & = \partial(f_1 + \mathbb{R}[\partial]^{1\times 2}R)) - (f_2 + \mathbb{R}[\partial]^{1\times 2}R) \\ & \overset{(a)}{=} (\partial f_1 + \mathbb{R}[\partial]^{1\times 2}R) - (f_2 + \mathbb{R}[\partial]^{1\times 2}R) \\ & \overset{(b)}{=} (\partial f_1 - f_2) + \mathbb{R}[\partial]^{1\times 2}R \overset{(c)}{=} 0. \end{array} \tag{2.8}$$

En (a) e en (b) empregáronse, respectivamente, a multiplicación por elementos de $\mathbb{R}[\partial]$ e a suma en M. En (c) utilizouse que $\partial f_1 - f_2 = (1,0)R$, logo $\partial f_1 - f_2 \in \mathbb{R}[\partial]^{1\times 2}R$.

Dada unha solución $\eta = (\eta_1, \eta_2)^T \in F^2$ podemos describir explicitamente o homomorfismo que lle fai corresponder o isomorfismo de Malgrange:

$$\begin{array}{rcl} \phi : M & \longrightarrow & F \\ \pi(f_1) = y_1 & \longmapsto & f_1\eta = \eta_1 \\ \pi(f_2) = y_2 & \longmapsto & f_2\eta = \eta_2 \end{array}$$

Observemos que ϕ é un homomorfismo de D-módulos pola esquerda ben definido precisamente porque as relacións que satisfán os xeradores de M, $\{y_1, y_2\}$, son as mesmas ecuacións lineares en $\mathbb{R}[\partial]$ que cumpren η_1 e η_2.

Reciprocamente, dado $\phi : M \longrightarrow F$, $\eta = (\phi(y_1), \phi(y_2))^T$ é solución do sistema linear xusto pola mesma razón.

Unha observación a maiores é que neste caso particular $\ker(R.)$ ten estrutura de $\mathbb{R}[\partial]$-módulo pola esquerda, como xa probamos no Exemplo 2.13. Nel vimos como $\ker(R.)$ é sempre un grupo abeliano (algo que tamén se deduce do isomorfismo de Malgrange), e que a clave para que sexa un $\mathbb{R}[\partial]$-módulo pola esquerda está en que $\mathbb{R}[\partial]$ é un anel conmutativo. Isto fainos pensar que se trata dun resultado máis xeral, que aplicará, polo menos, aos sistemas lineares de coeficientes constantes.

Para facelo explícito imos restrinxirnos a sistemas do estilo $R\eta = 0$, con $R \in \mathbb{R}[\partial]^{q\times p}$. O conxunto de solucións $\ker(R.)$ é entón un $\mathbb{R}[\partial]$-módulo pola esquerda, pero tamén é un N-módulo pola esquerda, sendo N un subanel calquera do anel $\mathbb{R}[\partial]$. Se tomamos $N = \mathbb{R}$, como $\mathbb{R}$ é un corpo, este resultado estanos a dicir que o conxunto de solucións $\ker(R.)$ é un $\mathbb{R}$ espazo vectorial, algo que é de sobra coñecido no caso de sistemas lineares e homoxéneos de coeficientes constantes, pero que aquí deducimos utilizando outras ferramentas.

Como resultado importante desta sección debemos reter que dada unha matriz con entradas nun anel D, $R \in D^{q\times p}$, xunto cun D-módulo pola esquerda F, o sistema linear $R\eta = 0$ pode ser estudado a partir do D-módulo pola esquerda finitamente presentado por R, $M = D^{1\times p}/(D^{1\times q}R)$. Segundo o Teorema 2.20 tamén se debe ter en conta o conxunto no que buscamos as solucións, F. Con todo, asumiremos que este é un D-módulo pola esquerda *coxerador* e *inxectivo*. De momento non temos os ingredientes necesarios para entender que representan estes dous calificativos. Adiantamos que, baixo estas circunstancias, un bo número das propiedades relevantes na Teoría do Control do sistema linear $R\eta = 0$ dependen unicamente do módulo do sistema M. Todo isto, xunto coa definición concreta, verémolo no derradeiro capítulo, cando xa teñamos feita unha pequena revisión dos conceptos básicos da Álxebra Homolóxica.

2.3. Aneis noetherianos

Na sección 2.1 introducimos as álxebras de Ore como uns aneis moi xerais que permiten representar mediante a ecuación $R\eta = 0$ diversos tipos de sistemas lineares de ecuacións funcionais. Con todo, a xeneralidade de pouco serve se non dispoñemos de resultados que permitan avanzar no estudo dos devanditos sistemas lineares. Segundo vaiamos progresando na exposición deste traballo comprobaremos como ao restrinxirnos a casos máis concretos contamos con teorías e ferramentas de cálculo máis potentes. Na primeira parte desta sección damos o paso inicial neste sentido, pois veremos que se nos ocupamos de álxebras de Ore onde o anel A cumpre unha serie de propiedades, entón estas serán en particular aneis noetherianos pola esquerda, ou tamén dominios. O interesante e útil é que estes aneis están ben estudados, e existen abondosos resultados importantes para eles. Pasamos entón a presentar os devanditos conceptos.

Definición 2.22. Sexa D un anel. Dicimos que D é un *dominio* se non contén divisores de cero propios, isto é, $d_1d_2 = 0$ implica $d_1 = 0$ ou $d_2 = 0$.

As álxebras de Ore $D = A\langle\partial_1, ..., \partial_m\rangle$, sendo A un anel diferencial como os introducidos (por exemplo, $A = K$, $A = K[x_1, ..., x_n]$ ou $A = K(x_1, ..., x_n)$, con K un corpo) son dominios. É máis, todas elas satisfán unha propiedade adicional que as converte nun tipo moi importante de anel, que a continuación definimos.

Definición 2.23. Sexa D un anel. Dicimos que D é un *anel noetheriano pola esquerda* se cada ideal pola esquerda de D é finitamente xerado, isto é, para cada ideal $I \subset D$ existen $a_1, ..., a_n \in D$ tales que $I = \{d_1a_1 + \cdots + d_na_n \mid d_i \in D, i = 1, ..., n\}$. Analogamente, dicimos que D é un *anel noetheriano pola dereita* se cada ideal pola dereita de D é finitamente xerado. Finalmente, un anel D é *noetheriano* se é noetheriano pola dereita e pola esquerda.

Exemplo 2.24. A maior parte dos aneis cos que estamos acostumados a traballar son dominios e aneis noetherianos. Por exemplo, calquera corpo K é un dominio. Para velo supoñamos que $ab = 0$ para determinados $a, b \in K$ non nulos, e tomemos $a^{-1} \in K$ tal que $a^{-1}a = 1$ (existe por ser K corpo). Multiplicando pola esquerda en $ab = 0$ séguese que $b = 0$ necesariamente. Ademais, todo corpo é tamén un anel noetheriano, pois só ten dous ideais: (0) e o propio corpo. Outro caso paradigmático é o dos *dominios de ideais principais pola*

esquerda: dominios D nos que todo ideal pola esquerda I é da forma $I = \{da \mid d \in D\}$ para certo $a \in I$. Está claro que son tamén aneis noetherianos, atendendo á Definición 2.23.

Como exemplo de dominio que non é anel noetheriano temos o anel de polinomios en infinitas variables sobre un corpo K, $K[X_1, ..., X_n, ...]$. Tomemos o ideal xerado por todas as variables X_i, chamémoslle I e supoñamos que é finitamente xerado. Nese caso podemos escribir $I = \{a_1 f_1 + \cdots \cdot a_t f_t \mid a_1, ..., a_t \in K[X_1, ..., X_n, ...]\}$, onde $f_1, ..., f_t \in I$. Como cada $f_i \in I$, existe un número finito de variables, $X_{v1}, ..., X_{vl}$ tales que $f_i = a_{i1}X_{v1} + \cdots + a_{il}X_{vl}$, e isto para $i = 1, ..., t$. Tomemos X_s unha variable distinta das $X_{v1}, ..., X_{vl}$. Como $X_s \in I$, $X_s = b_1 X_{v1} + \cdots + b_l X_{vl}$, para $b_1, ..., b_l \in K[X_1, ..., X_n, ...]$. Avaliando a derradeira igualdade en $X_{v1} = 0, ..., X_{vl} = 0$ obtemos $X_s = 0$, o que resulta unha contradición.

Debemos mencionar que a definición aquí proporcionada non é a que se adoita atopar nas referencias sobre aneis noetherianos. Con todo, para os nosos propósitos podemos empregala, pois é equivalente á definición tradicional, segundo a que un anel noetheriano pola esquerda é aquel no que cada cadea ascendente de ideais pola esquerda, $0 = I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots \subset D$ remata nun número finito de pasos, isto é, existe $n_0 \in \mathbb{N}$ tal que $I_n = D$ se $n \geq n_0$. A demostración da equivalencia de ambas definicións pódese atopar en [15]. Enunciamos tamén un resultado do que tiraremos proveito no seguinte capítulo, e cuxa demostración pode consultarse en [21]. Non a presentamos aquí, pois require de técnicas e resultados de Teoría de Módulos e Álxebra Homolóxica que van máis alá dos propósitos deste traballo.

Proposición 2.25. *Sexa D un anel noetheriano pola esquerda. Se M é un D-módulo pola esquerda finitamente xerado, entón todo D-submódulo pola esquerda de M é tamén finitamente xerado.*

Empregando o anterior próbase o seguinte corolario. Xa que a demostración é case inmediata e utiliza unicamente os conceptos de módulo finitamente xerado e finitamente presentado cos que debemos acostumarnos a traballar, decidimos incluíla neste caso.

Corolario 2.26. *Sexa D un anel noetheriano pola esquerda. Se M é un D-módulo pola esquerda finitamente xerado entón tamén é finitamente presentado.*

Demostración. Sexa D un anel noetheriano pola esquerda e consideremos M un D-módulo pola esquerda finitamente xerado, de xeito que existe un homomorfismo de D-módulos pola esquerda sobrexectivo $\pi : D^{1\times r_0} \longrightarrow M$, con $r_0 \in \mathbb{N}$. Tense que $\ker \pi$ é un D-submódulo pola esquerda do D-módulo pola esquerda $D^{1\times r_0}$. Como este último é libre e de rango finito, é finitamente xerado e, empregando a Proposición 2.25 tense que $\ker \pi$ é tamén finitamente xerado, de maneira que M é entón finitamente presentado. ■

Na sección 2.1 introducimos as álxebras de Ore de xeito iterativo, definindo o concepto en primeiro lugar para o caso no que temos un só endomorfismo $\sigma : A \longrightarrow A$ e unha soa σ-derivación $\delta : A \longrightarrow A$, isto é, $A[\partial; \sigma, \delta]$. Esta estrutura adoita chamarse *anel de polinomios nesgados*. Nestas circunstancias está claro que todo anel de polinomios nesgado é unha álxebra de Ore, e de acordo coa Definición 2.7, unha álxebra de Ore constrúese iterando aneis de polinomios nesgados. A utilidade disto está en que este tipo de aneis están moi ben caracterizados en [15]. En particular, amósase explicitamente que a iteración de aneis de polinomios nesgados é tamén un anel de polinomios nesgados. Así pois, unha álxebra

de Ore é un anel de polinomios nesgado, co que ambas nocións son, en realidade, equivalentes. Podemos aproveitar entón algúns dos resultados que se proban en [15], como a continuación amosamos.

Teorema 2.27. *Sexa A un anel e considermos $D = A[\partial_1; \sigma_1, \delta_1] \cdots [\partial_m; \sigma_m, \delta_m]$ unha álxebra de Ore. Entón:*

(1) Se A é un dominio e σ inxectivo, entón D é un dominio.

(2) Se A é un anel noetheriano pola esquerda e σ é un automorfismo de A, entón D é un anel noetheriano pola esquerda.

O teorema que se proba en [15] é lixeiramente distinto do que aquí amosamos, pois realízase para o caso dun anel de polinomios nesgados $A[\partial; \sigma, \delta]$. Con todo, tendo en conta a discusión do parágrafo previo ao Teorema 2.27 e a Definición 2.7, a extensión ao caso que nós presentamos é inmediata. Como exemplo de aplicación, o Teorema 2.27 permítenos asegurar que a primeira e a segunda álxebras de Weyl son dominios noetherianos pola esquerda, xa que o anel de polinomios e o corpo de fraccións deste sobre un corpo K son dominios noetherianos pola esquerda.

Doutra banda, como xa indicamos, na Análise Alxébrica a Teoría de Módulos xoga tamén un papel moi relevante. Na sección 2.1 xa introducimos as definicións básicas de D-módulo pola esquerda, D-submódulo pola esquerda e homomorfismo de D-módulos pola esquerda, mentres que na sección 2.2 asentamos os conceptos de módulo finitamente xerado e finitamente presentado. Así e todo, para comprender o posterior desenvolvemento precisamos seguir introducindo nocións e resultados adicionais, pois xa indicamos que as propiedades do módulo do sistema $M = D^{1\times p}/(D^{1\times q}R)$, sendo R unha matriz $q \times p$ sobre o anel D, proporcionan moita información sobre o sistema linear $R\eta = 0$.

Deste xeito, presentamos a continuación varias definicións propias da Teoría de Módulos, baseándonos en [3, 4, 17]. Aínda que se poden realizar en condicións máis xerais, nós imos restrinxirnos ao caso dun dominio D noetheriano pola esquerda e un D-módulo pola esquerda M finitamente xerado, pois son as circunstancias nas que nos atoparemos no resto do traballo, e nas que se desenvolven as principais ideas da Análise Alxébrica.

Definición 2.28. Sexan D un dominio noetheriano pola esquerda e M un D-módulo pola esquerda finitamente xerado.

(1) M dise *libre* se existe $r \in \mathbb{Z}_{\geq 0}$ tal que $M \simeq D^{1\times r}$. Nese caso r chámase o *rango* do D-módulo libre pola esquerda M, e denotarémolo por $\mathrm{rg}_D(M)$.

(2) M dise *proxectivo* se existen $r \in \mathbb{Z}_{\geq 0}$ e un D-módulo pola esquerda N tales que $M \bigoplus N \simeq D^{1\times r}$.

(3) M dise *reflexivo* se o seguinte *homomorfismo canónico de D-módulos pola esquerda*:

$$\begin{array}{rccc} \varepsilon: & M & \longrightarrow & \hom(\hom(M, D), D) \\ & m & \longmapsto & \varepsilon(m), \end{array}$$

onde $\varepsilon(m)(f) = f(m) \in M$ para cada $f \in \hom(M, D)$, é un isomorfismo de D-módulos pola esquerda.

(4) M dise *libre de torsión* se o *D-submódulo pola esquerda de torsión* de M:

$$t(M) = \{m \in M \mid \exists d \in D \setminus \{0\}, dm = 0\}$$

é tal que $t(M) = \{0\}$. Os elementos de $t(M)$ chámanse *elementos de torsión* de M.

(5) M dise un *módulo de torsión* se $t(M) = M$.

Observación 2.29. No caso dun anel conmutativo D e dun D-módulo pola esquerda M, compróbase que o submódulo de torsión $t(M)$ é, en efecto, un D-submódulo de M. Isto non é certo no caso non conmutativo. Así e todo, en [15] próbase que todo anel D noetheriano pola esquerda cumpre a *propiedade de Ore pola esquerda*, isto é, dados $d_1, d_2 \in D \setminus \{0\}$, existen $e_1, e_2 \in D \setminus \{0\}$ tales que $e_1 d_1 = e_2 d_2$. Utilizando esta propiedade é fácil demostrar que dados $m_1, m_2 \in t(M)$ e $d_1, d_2 \in D$, $d_1 m_1 + d_2 m_2 \in t(M)$, isto é $t(M)$ é, neste caso particular, un D-submódulo pola esquerda de M.

Os tipos de módulos introducidos na Definición 2.28 están relacionados entre si. Algunhas destas relacións son inmediatas a partir da definición, e enunciámolas no seguinte resultado, cuxa demostración non presentamos, por non tratarse do obxectivo deste traballo. Con todo, pódese consultar en [21].

Proposición 2.30. *Sexa D un dominio noetheriano pola esquerda. Se M é un D-módulo libre, entón é proxectivo; se é proxectivo, entón é reflexivo e, finalmente, se é reflexivo, entón é libre de torsión.*

Os recíprocos dos enunciados da anterior proposición non son certos en xeral. Así e todo, na segunda metade do século XX avanzouse notablemente na Teoría de Módulos e demostrouse que baixo determinadas circunstancias si que se teñen as implicacións nos sentidos opostos. Amosamos a continuación algún destes resultados, pois serán de utilidade posteriormente. As demostracións poden atoparse en [12, 19, 22, 23].

Teorema 2.31. *(1) Se D é un dominio de ideais principais pola esquerda, entón todo D-módulo pola esquerda finitamente xerado e libre de torsión é libre.*

*(2) Se $D = K[x_1, ..., x_n]$, con K un corpo, é un anel de polinomios conmutativo, entón todo D-módulo pola esquerda finitamente xerado e proxectivo é libre (*Teorema de Quillen-Suslin*).*

*(3) Se D é a primeira álxebra de Weyl $A_n(K)$ ou a segunda álxebra de Weyl, $B_n(K)$, para un corpo K de característica 0, entón todo D-módulo pola esquerda finitamente xerado proxectivo de rango maior ou igual que 2 é libre (*Teorema de Stafford*).*

Finalmente, cómpre mencionar que a introdución dos conceptos da Definición 2.28 realízase porque estes xogarán un papel relevante na parte final do traballo. Así, co Teorema 4.21 comprobaremos que cando o módulo do sistema linear $R\eta = 0$ é libre de torsión, proxectivo, ou libre téñense unha serie de propiedades interesantes desde o punto de vista da Teoría do Control. Todo isto asumindo que $R \in D^{q \times p}$ con D unha determinada álxebra de Ore que é un dominio noetheriano pola esquerda e F un D-módulo pola esquerda inxectivo e coxerador. Isto asenta o propósito dos vindeiros capítulos: presentar algoritmos (de xeito construtivo) que permitan comprobar cando un módulo pola esquerda finitamente xerado nestas circunstancias cumpre algunha destas propiedades. Para iso será necesario utilizar potentes

ferramentas de cálculo, como as técnicas das bases de Gröbner, e tamén acudir a resultados da Álxebra Homolóxica. Ambos aspectos serán os principais obxectos do seguinte capítulo.

3. Resolucións libres e finitas e grupos abelianos das extensións

Neste capítulo imos presentar en primeiro lugar as técnicas das bases de Gröbner para o caso máis convencional dun ideal nun anel de polinomios conmutativo e adaptalas ao caso dun submódulo dun D-módulo pola esquerda finitamente xerado, onde D é unha álxebra de Ore. Comprobaremos que será necesario que nos restrinxamos a álxebras de Ore que satisfán certas propiedades. A continuación utilizaremos isto para presentar un algoritmo que calcule unha resolución libre e finita dun D-módulo pola esquerda finitamente xerado, e para iso precisaremos introducir algúns conceptos propios da Álxebra Homolóxica. Finalmente, presentaremos os grupos abelianos das extensións no noso marco de traballo de forma precisa. A relevancia deste concepto na Análise Alxébrica farase máis evidente no vindeiro capítulo, mais trataremos de amosar como emerxe de forma natural na teoría de Sistemas Matemáticos.

3.1. Bases de Gröbner

Como xa adiantamos, o deseño de algoritmos que permiten implementar certas técnicas propias da Análise Alxébrica require, na maior parte dos casos, potentes ferramentas de cálculo. Máis concretamente, utilízanse técnicas de eliminación baseadas no cálculo de bases de Gröbner sobre álxebras de Ore non conmutativas. De cara a aplicalas, debemos restrinxirnos a álxebras de Ore sobre aneis de polinomios. Así pois, nesta sección consideraremos $D = A\langle\partial_1, ..., \partial_n\rangle$, con $A = K[x_1, ..., x_n]$, sendo en principio K un corpo calquera. Posteriormente deberemos restrinxirnos a unha clase máis pequena destas álxebras de Ore.

3.1.1. Bases de Gröbner de ideais sobre aneis de polinomios

Imos tratar de visualizar o que é unha base de Gröbner no caso máis convencional dun ideal no anel de polinomios $K[x_1, ..., x_n]$, que é o contexto no que se desenvolveu inicialmente a teoría das bases de Gröbner. Esta está moi ben documentada (por exemplo [5] é unha boa referencia), pero aquí realizaremos unha exposición moi breve que nos permita entender a relevancia e a utilidade do concepto.

O cálculo de bases de Gröbner permite desenvolver métodos que xeneralizan os algoritmos de división nun anel de polinomios, $K[x]$, e de eliminación gaussiana nun sistema de ecuacións lineares. Nos dous casos é fundamental poder ordenar os termos, aínda que habitualmente non se saliente este aspecto.

- No algoritmo de división en $K[x]$ a orde vén dada polas potencias de x:

$$x^{m+1} > x^m > \cdots x^2 > x > 1.$$

  Lembremos que o primeiro paso consiste en ordenar os termos do dividendo e do divisor de acordo con esta orde, de aí a súa importancia.

- No algoritmo de eliminación gaussiana as variables ordénanse da forma que resulte máis conveniente,

$$x_1 > x_2 > \cdots > x_n.$$

  Empregando esta orde construímos a matriz asociada ao sistema linear, e o método consiste en realizar operacións elementais que a transformen nunha matriz triangular superior. En función da orde escollida eliminamos antes unhas ou outras variables.

Atendendo á anterior discusión, está claro que é fundamental poder ordenar os termos de calquera polinomio $f \in K[x_1, ..., x_n]$. Para iso definimos os seguintes conceptos.

Definición 3.1. Unha *orde monomial* $\prec$ en $A = K[x_1, ..., x_n]$ é unha relación no conxunto de monomios de A, $\text{Mon}(A) = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{Z}_{\geq 0}, i = 1, ..., n\}$, cumprindo as seguintes propiedades:

(i) A relación $\prec$ é unha relación de orde en $\text{Mon}(D)$.
(ii) A relación $\prec$ é compatible co produto de monomios, isto é, se $m_1 \prec m_2$, para $m_1, m_2 \in \text{Mon}(D)$, entón $n \cdot m_1 \prec n \cdot m_2$, para todo $n \in \text{Mon}(D)$.
(iii) O conxunto $\text{Mon}(D)$ está ben ordenado coa relación de orde $\prec$ (isto implica que a relación de orde $\prec$ é total en $\text{Mon}(D)$).

Nestas circunstancias, dado un polinomio $f \in A$, definimos o *monomio líder* de f como o maior monomio de f con coeficiente non nulo, e denotámolo por $\text{lm}(f)$. O coeficiente asociado será o *coeficiente líder*, $\text{lc}(f)$, e finalmente, o *termo líder* é o produto $\text{lc}(f)\text{lm}(f)$, e denotarémolo por $\text{lt}(f)$.

Por simplicidade denotamos un monomio xenérico $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ por $\boldsymbol{x}^{\boldsymbol{\alpha}}$, con $\boldsymbol{\alpha} \in \mathbb{Z}_{\geq 0}^n$. Definamos entón que se entende por base de Gröbner dun ideal do anel de polinomios. Cómpre notar que hai varias definicións equivalentes de base de Gröbner (ver, por exemplo, [5]). Aquí tomamos a que nos resulta máis conveniente de cara á posterior xeneralización.

Definición 3.2. Sexa $\prec$ unha orde monomial en $A = K[x_1, ..., x_n]$. Un subcunxunto finito de xeradores dun ideal I, $G = \{g_1, ..., g_t\} \subset I \setminus \{0\}$ é unha *base de Gröbner* se para calquera $f \in I$, existe $j \in \{1, ..., t\}$ tal que $\text{lt}(g_j)$ divide a $\text{lt}(f)$, considerando a división usual de polinomios en varias variables.

As bases de Gröbner cumpren unha serie de propiedades que as fan moi interesantes. Por exemplo, para calquera $f \in K[x_1, ..., x_n]$ tense que $f \in I$ se e só se o resto da división de f polos polinomios de G é cero. Isto é consecuencia de que o resto da división de calquera polinomio $f \in K[x_1, ..., x_n]$ polos polinomios de G é único, algo que non sempre ocorre no caso da división de polinomios en varias variables. Así e todo, o máis relevante das bases de Gröbner é que, para calquera orde monomial, poden ser calculadas, empregando para iso o *algoritmo de Buchberger*. Este último pódese consultar en [5].

A última propiedade interesante das bases de Gröbner no caso convencional que queremos destacar coñécese como *teorema de eliminación*. Para enuncialo precisamos introducir antes unha orde monomial moi coñecida: a *orde lexicográfica*.

Definición 3.3. Sexan $\boldsymbol{x}^{\boldsymbol{\alpha}}$ e $\boldsymbol{x}^{\boldsymbol{\beta}}$ dous monomios no anel de polinomios $A = K[x_1, ..., x_n]$. Dicimos que $\boldsymbol{x}^{\boldsymbol{\alpha}} >_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}$ se a primeira compoñente non nula do vector $\boldsymbol{\alpha}-\boldsymbol{\beta} \in \mathbb{Z}^n_{\geq 0}$ é positiva. En particular tense que: $x_1 >_{\text{lex}} \cdots >_{\text{lex}} x_n$.

Observación 3.4. Notemos que a orde lexicográfica que vimos de introducir na anterior definición está inducida polo nome que reciben as distintas variables do anel de polinomios $A = K[x_1, ..., x_n]$, de aí que $x_1 >_{\text{lex}} \cdots >_{\text{lex}} x_n$. Con todo, calquera orde total no conxunto das variables $\{x_1, ..., x_n\}$ define unha orde lexicográfica: dados dous monomios $\boldsymbol{x}^{\boldsymbol{\alpha}}$ e $\boldsymbol{x}^{\boldsymbol{\beta}}$ basta ver o signo da *primeira* compoñente non nula do vector $\boldsymbol{\alpha} - \boldsymbol{\beta} \in \mathbb{Z}^n_{\geq 0}$ seguindo a orde nas variables $\{x_1, ..., x_n\}$. Deste xeito, hai $n!$ ordes lexicográficas distintas no conxunto dos monomios do anel de polinomios $A = K[x_1, ..., x_n]$: unha por cada maneira de ordenar as variables $x_1, ..., x_n$.

A comprobación de que se trata, en efecto, dunha orde monomial, podémola atopar en [5]. Con isto xa podemos enunciar o teorema de eliminación, que é o resultado da teoría de bases de Gröbner do que tiraremos máis proveito. A proba pode consultarse tamén en [5].

Teorema 3.5 (Teorema de eliminación). *Sexa $I \subset K[x_1, ..., x_n]$ un ideal non nulo, e G unha base de Gröbner de I respecto da orde lexicográfica con $x_1 >_{\text{lex}} \cdots >_{\text{lex}} x_n$. Daquela, para cada $0 \leq l \leq n$, o conxunto:*

$$G_l = G \cap K[x_{l+1}, ..., x_n]$$

é unha base de Gröbner do ideal de eliminación l-ésimo I_l*, isto é, o ideal $I \cap K[x_{l+1}, ..., x_n]$.*

3.1.2. Bases de Gröbner de ideais sobre álxebras de Ore

Pasamos agora a realizar a xeneralización a álxebras de Ore sobre o anel de polinomios $A = K[x_1, ..., x_n]$. Con todo, de cara a definir as bases de Gröbner neste contexto precisamos restrinxirnos a unha clase máis pequena das álxebras de Ore. Así, na Definición 2.7 imos introducir as seguintes condicións adicionais sobre os endomorfismos σ_i e as derivacións δ_i, $i = 1, ..., m$:

$$\sigma_i(x_j) = a_{ij}x_j + b_{ij}, \quad \delta_i(x_j) = c_{ij}, \quad i = 1, ..., m,\ j = 1, ..., n, \tag{3.1}$$

onde $a_{ij} \in K \setminus \{0\}$, $b_{ij} \in k$, $c_{ij} \in A$. Esixiremos ademais que en cada c_{ij} o termo maior u (de acordo cunha orde monomial $\prec$ admisible, que deseguido definimos) cumpra $u \prec x_j\partial_i$. Baixo estas circunstancias, a álxebra de Ore D é un *anel de polinomios resoluble*, como en [11] se demostra. Esencialmente, este é un anel de polinomios non conmutativos onde as relacións de conmutación compórtanse ben coa orde monomial escollida. Non imos definir con precisión este concepto, basta ter en conta que no contexto no que imos traballar poderemos aplicar os resultados dispoñibles sobre bases de Gröbner para a anterior clase de aneis de polinomios, que se poden consultar en [11]. A exposición que nós faremos baséase na realizada en [13]. Nesta as condicións sobre os endomorfismos e as derivacións son lixeiramente máis restritivas (tamén máis simples) que as de (3.1), pero son facilmente xeneralizables ás que nós presentamos.

Deste xeito, no que segue, D denotará a álxebra de Ore $D = A\langle\partial_1, ..., \partial_m\rangle$, onde $A = K[x_1, ..., x_n]$, e supoñemos que se satisfán as condicións de (3.1). Notemos que calquera polinomio en D pódese escribir como $f = \sum_{i=0}^{r} c_i m_i$, onde $c_i \in K$ son os coeficientes de f e $m_i = x_1^{\alpha_{i_1}} \cdots x_n^{\alpha_{i_n}} \partial_1^{\beta_{i_1}} \cdots \partial_m^{\beta_{i_m}} = \boldsymbol{x}^{\boldsymbol{\alpha_i}} \boldsymbol{\partial}^{\boldsymbol{\beta_i}}$ son os monomios de f, con $\boldsymbol{\alpha_i} \in \mathbb{Z}_{\geq 0}^n$ e $\boldsymbol{\beta_i} \in \mathbb{Z}_{\geq 0}^m$. Neste sentido é esencial a relación de conmutación da Definición 2.7 de ∂_i, $i = 1, ..., m$, cos elementos de A, pois é a que permite que os monomios se poidan escribir como $\boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}}$.

O primeiro que imos facer é introducir a noción de *cuasi-divisibilidade* de termos, xunto co concepto de orde *monomial admisible*. A continuación amosamos tamén a relación que hai entre ambos.

Definición 3.6. Sexan $c_1 m_1$ e $c_2 m_2$ dous termos en D, isto é, para $i = 1, 2$, $c_i \in K$ e $m_i = \boldsymbol{x}^{\boldsymbol{\alpha_i}} \boldsymbol{\partial}^{\boldsymbol{\beta_i}}$, con $\boldsymbol{\alpha_i} \in \mathbb{Z}_{\geq 0}^n$, $\boldsymbol{\beta_i} \in \mathbb{Z}_{\geq 0}^m$. Dicimos que $c_1 m_1$ *cuasi-divide* a $c_2 m_2$ se c_1 divide a c_2 no corpo K, $\boldsymbol{\alpha_1} \leq \boldsymbol{\alpha_2}$ e $\boldsymbol{\beta_1} \leq \boldsymbol{\beta_2}$, isto é, $\alpha_{1_i} \leq \alpha_{2_i}$ e $\beta_{1_i} \leq \beta_{2_i}$ para cada $i = 1, ..., n$.

Definición 3.7. Unha *orde monomial admisible* $\prec$ é unha relación de orde total no conxunto de monomios de D, isto é, $\mathrm{Mon}(D) = \{\boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}} \mid \boldsymbol{\alpha} \in \mathbb{Z}_{\geq 0}^n, \boldsymbol{\beta} \in \mathbb{Z}_{\geq 0}^m\}$, que satisfai as seguintes condicións:

- (i) Para cada $m \in \mathrm{Mon}(D)$, $1 \prec m$, sendo 1 a unidade do anel.
- (ii) Sexan $\boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}}$ e $\boldsymbol{x}^{\boldsymbol{a}} \boldsymbol{\partial}^{\boldsymbol{b}}$ dous monomios en D, onde $\boldsymbol{\alpha}, \boldsymbol{a} \in \mathbb{Z}_{\geq 0}^n$ e $\boldsymbol{\beta}, \boldsymbol{b} \in \mathbb{Z}_{\geq 0}^m$. Se $\boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}} \prec \boldsymbol{x}^{\boldsymbol{a}} \boldsymbol{\partial}^{\boldsymbol{b}}$, entón $\boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{u}} \boldsymbol{\partial}^{\boldsymbol{\beta}+\boldsymbol{v}} \prec \boldsymbol{x}^{\boldsymbol{a}+\boldsymbol{u}} \boldsymbol{\partial}^{\boldsymbol{b}+\boldsymbol{v}}$, e isto para cada $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_{\geq 0}^n$.

Unha orde monomial admisible é unha relación de orde en $\mathrm{Mon}(D)$ que é compatible coa *cuasi-divisibilidade*. Pódese comprobar que baixo estas circunstancias $\mathrm{Mon}(D)$ é un conxunto ben ordenado. En [13] demóstrase para o caso que estamos a tratar, mentres que en [11] faise para o caso máis xeral dos aneis de polinomios resolubles.

As definicións de monomio, coeficiente e termo líder xeneralízanse trivialmente unha vez temos definida unha orde monomial admisible. De cara a definir unha orde en D, como calquera polinomio en D é da forma $f = \sum_{i=0}^{r} c_i m_i$, $c_i \in K$, $m_i = \boldsymbol{x}^{\boldsymbol{\alpha_i}} \boldsymbol{\partial}^{\boldsymbol{\beta_i}}$, podemos tratar as variables $x_1, ..., x_n, \partial_1, ..., \partial_n$ como $2n$ variables dun anel de polinomios convencional, denotándoas por $y_1, ..., y_n, y_{n+1}, ..., y_{2n}$. Neste contexto podemos considerar a orde lexicográfica que induce o nome das anteriores variables: $y_1 >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} y_n >_{\mathrm{lex}} y_{n+1} >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} y_{2n}$, isto é, $x_1 >_{\mathrm{lex}} > \cdots >_{\mathrm{lex}} x_n >_{\mathrm{lex}} \partial_1 >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} \partial_n$. Cómpre lembrar aquí que, segundo o exposto na Observación 3.4, só necesitamos unha orde no conxunto das variables do anel de polinomios para poder definir unha orde lexicográfica no propio anel. En [11] próbase que a orde que vimos de introducir é admisible en calquera anel de polinomios resolubles e, daquela, tamén na álxebra de Ore D.

Visto isto, xa podemos definir unha base de Gröbner dun ideal I pola esquerda non nulo neste contexto máis xeral.

Definición 3.8. Sexa $D = A\langle\partial_1, ..., \partial_m\rangle$ unha álxebra de Ore sobre o anel de polinomios $K[x_1, ..., x_n]$ nas condicións (3.1), e $\prec$ unha orde monomial admisible. Sexa tamén $I \subset A$ un ideal pola esquerda non nulo. Un subcunxunto finito de xeradores de I, $G = \{g_1, ..., g_t\}$, é unha *base de Gröbner* se para calquera $f \in I$, existe $j \in \{1, ..., t\}$ tal que $\mathrm{lt}(g_j)$ cuasi-divide a $\mathrm{lt}(f)$.

Como vemos, a definición é moi similar á do caso convencional unha vez que concreta-

mos que é unha orde monomial admisible. O mesmo ocorre para as propiedades das bases de Gröbner. Imos presentar entón o teorema que enuncia o algoritmo de Buchberger neste caso máis xeral tal e como se expón en [4]. A proba pódese atopar en [11] ou [13].

Teorema 3.9. *Sexa $D = A\langle\partial_1, ..., \partial_m\rangle$, con $A = K[x_1, ..., x_n]$, unha álxebra de Ore nas condicións* (3.1)*, supoñendo $\prec$ unha orde monomial admisible. Sexa tamén I un ideal de D pola esquerda xerado por un conxunto finito de polinomios. Entón unha versión non conmutativa do algoritmo de Buchberger remata e calcula unha base de Gröbner de I para esta orde monomial admisible.*

Finalmente enunciamos o teorema de eliminación para este contexto máis xeral, pois a súa xeneralización ao caso de bases de Gröbner de módulos sobre álxebras de Ore é o resultado que se atopa detrás de case todos os algoritmos dos que falaremos no resto do traballo. A versión que aquí proporcionamos pódese atopar en [13].

Teorema 3.10. *Sexa $D = A\langle\partial_1, ..., \partial_m\rangle$, con $A = K[x_1, ..., x_n]$, unha álxebra de Ore nas condicións* (3.1)*, e I un ideal pola esquerda de D. Tomemos un subconxunto de variables de D,*

$$\{x_{i1}, ..., x_{ir}, \partial_{j1}, ..., \partial_{js}\} \subset \{x_1, ..., x_n, \partial_1, ..., \partial_m\},$$

e $\prec$ unha orde monomial admisible tal que:

$$\{x_{i1}, ..., x_{ir}, \partial_{j1}, ..., \partial_{js}\} \prec \{x_1, ..., x_n, \partial_1, ..., \partial_m\} \setminus \{x_{i1}, ..., x_{ir}, \partial_{j1}, ..., \partial_{js}\}.$$

Se G é unha base de Gröbner de I respecto de $\prec$, entón $G \cap A[x_{i1}, ..., x_{ir}]\langle\partial_{j1}, ..., \partial_{js}\rangle$ é unha base de Gröbner do ideal $I \cap A[x_{i1}, ..., x_{ir}]\langle\partial_{j1}, ..., \partial_{js}\rangle$.

3.1.3. Bases de Gröbner de módulos sobre álxebras de Ore

Para rematar esta sección realizaremos unha serie de comentarios sobre como a teoría exposta sobre bases de Gröbner pode ser estendida ao caso de módulos sobre álxebras de Ore, que é o contexto no que se vai aplicar. A maior parte do traballo está feito no anterior apartado, pois a xeneralización de aneis de polinomios a módulos sobre aneis de polinomios é case inmediata, como se pode comprobar en [6]. Deste xeito, unha vez que se estende a noción de orde monomial a módulos libres sobre o anel de polinomios $K[x_1, ..., x_n]$, o resto de resultados derívanse case identicamente aos casos tratado nos apartados previos.

Así e todo, como xa indicamos, a nós interésanos poder calcular bases de Gröbner de submódulos de $D^{1\times p}$, onde $D = A\langle\partial_1, ..., \partial_m\rangle$ é unha álxebra de Ore sobre o anel de polinomios $K[x_1, ..., x_n]$ nas condicións (3.1). Imos limitarnos entón a definir a orde monomial nestas circunstancias e proporcionar unha serie de referencias onde se pode consultar a posterior (e inmediata) xeneralización.

Sexa $\{f_1, ..., f_p\}$ a base canónica de $D^{1\times p}$. Un monomio en $D^{1\times p}$ é un elemento da forma $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \partial_1^{\beta_1} \cdots \partial_m^{\beta_m} f_i = \boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}} f_i$ para algún $i = 1, ..., p$, con $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0}$ e $\boldsymbol{\beta} \in \mathbb{Z}^m_{\geq 0}$, isto é, o produto dun monomio na álxebra de Ore D por un vector da base canónica de $D^{1\times p}$. De novo, todo elemento $f \in D^{1\times p}$ pódese escribir como $f = \sum_{i=0}^{r} c_i m_i$, onde $c_i \in K$ e m_i son monomios en $D^{1\times p}$.

O seguinte é introducir a relación de *cuasi-divisibilidade* en $D^{1\times p}$. Consideremos dous termos en $D^{1\times p}$, que podemos escribir como $c_1 x^{\alpha_1}\partial^{\beta_1} f_{i1}$ e $c_2 x^{\alpha_2}\partial^{\beta_2} f_{i2}$. Dicimos que $c_1 x^{\alpha_1}\partial^{\beta_1} f_{i1}$ *cuasi-divide* a $c_2 x^{\alpha_2}\partial^{\beta_2} f_{i2}$ se $i_1 = i_2$ e $c_1 x^{\alpha_1}\partial^{\beta_1}$ cuasi-divide a $c_2 x^{\alpha_2}\partial^{\beta_2}$ como monomios na álxebra de Ore D.

Definición 3.11. Sexa $\prec$ unha orde monomial admisible no conxunto de monomios da álxebra de Ore $D = A\langle\partial_1, ..., \partial_m\rangle$, con $A = K[x_1, ..., x_n]$. Unha *orde monomial admisible no módulo* $D^{1\times p}$, denotada por $\prec_m$, é unha relación de orde total no conxunto de monomios de $D^{1\times p}$, isto é, $\mathrm{Mon}(D^{1\times p}) = \{\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i \mid \boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0}, \boldsymbol{\beta} \in \mathbb{Z}^m_{\geq 0}, i = 1, .., p\}$ que é compatible coa estrutura de D-módulo pola esquerda de $D^{1\times p}$ e coa orde monomial $\prec$ en D , é dicir, cúmprense as seguintes condicións:

(i) Sexan $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i$ e $\boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} f_j$ monomios, con $\boldsymbol{\alpha}, \boldsymbol{a} \in \mathbb{Z}^n_{\geq 0}$, $\boldsymbol{\beta}, \boldsymbol{b} \in \mathbb{Z}^m_{\geq 0}$, e $i, j \in \{1, ..., p\}$. Se $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i \prec_m \boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} f_j$ entón $\boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{u}}\boldsymbol{\partial}^{\boldsymbol{\beta}+\boldsymbol{v}} f_i \prec_m \boldsymbol{x}^{\boldsymbol{a}+\boldsymbol{u}}\boldsymbol{\partial}^{\boldsymbol{b}+\boldsymbol{v}} f_j$, e isto para cada $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}^n_{\geq 0}$.

(ii) Se $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} \prec \boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}$, con $\boldsymbol{\alpha}, \boldsymbol{a} \in \mathbb{Z}^n_{\geq 0}$ e $\boldsymbol{\beta}, \boldsymbol{b} \in \mathbb{Z}^m_{\geq 0}$, entón $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i \prec_m \boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i$, e isto para $i = 1, \ldots, p$.

Hai dous xeitos naturais de estender a orde $\prec$ a $D^{1\times p}$:

- A *orde TOP* (do inglés *term over position*) ordena primeiro empregando a orde monomial admisible $\prec$, e despois utiliza a posición do vector da base canónica $\{f_1, ..., f_p\}$ asociado. Así, dados $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i$ e $\boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} f_j$, con $\boldsymbol{\alpha}, \boldsymbol{a} \in \mathbb{Z}^n_{\geq 0}$, $\boldsymbol{\beta}, \boldsymbol{b} \in \mathbb{Z}^m_{\geq 0}$, e $i, j \in \{1, ..., p\}$:

$$\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i \prec_{\mathrm{TOP}} \boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} f_j : \Longleftrightarrow \boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} \prec \boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} \text{ ou } \boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} = \boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} \text{ e } i < j.$$

- A *orde POT* (do inglés *position over term*) ordena primeiro empregando a posición do vector da base canónica asociado, e despois utiliza a orde monomial admisible $\prec$. Así, dados $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i$ e $\boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} f_j$, con $\boldsymbol{\alpha}, \boldsymbol{a} \in \mathbb{Z}^n_{\geq 0}$, $\boldsymbol{\beta}, \boldsymbol{b} \in \mathbb{Z}^m_{\geq 0}$, e $i, j \in \{1, ..., p\}$:

$$\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} f_i \prec_{\mathrm{POT}} \boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}} f_j : \Longleftrightarrow i < j \text{ ou } i = j \text{ e } \boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} \prec \boldsymbol{x}^{\boldsymbol{a}}\boldsymbol{\partial}^{\boldsymbol{b}}.$$

Unha vez que se ten unha orde monomial admisible no conxunto de monomios de $D^{1\times p}$, poderiamos presentar o desenvolvemento da anterior sección para definir as bases de Gröbner e enunciar un resultado de finalización dunha versión modificada do algoritmo de Buchberger, seguindo a exposición de [6] para o caso de módulos sobre aneis de polinomios. Non imos realizar esta xeneralización, por exceder os obxectivos deste traballo. Con todo, consideramos que as nocións expostas amosan ben como se adaptan as técnicas das bases de Gröbner aos distintos casos, e de feito existen algoritmos implementados en sistemas de álxebra computacional como SINGULAR, *Maple* ou `Mathematica` que permiten realizar os cálculos nestes contextos máis complicados.

3.2. Conceptos básicos de Álxebra Homolóxica. Resolucións libres e finitas

Nesta sección presentamos unha serie de conceptos propios da Álxebra Homolóxica, que nos serán de gran utilidade no que segue. Máis concretamente, empregarémolos para

comprender a relación que existe entre as propiedades (desde o punto de vista da Teoría do Control) dun sistema linear $R\eta = 0$, con $R \in D^{p\times q}$ unha matriz con entradas nunha álxebra de Ore D, e o módulo do sistema $M = D^{1\times p}/(D^{1\times q}R)$. Tamén se atopan detrás da maior parte dos algoritmos existentes na Análise Alxébrica, que tratan de comprobar se un determinado módulo cumpre ou non as devanditas propiedades.

A exposición que aquí amosamos está baseada nas realizadas en [3, 17, 18], pois en calquera destas referencias resúmense (de forma moi concisa) as nocións que nos resultarán de maior interese. Porén, tratamos tamén de explicar todo isto de forma clara, profundizando naqueles conceptos que poidan resultar máis confusos. Unha exposición moito máis detallada pódese atopar, por exemplo, en [21].

Definición 3.12. (1) Un *complexo de D-módulos pola esquerda* (*pola dereita*) é unha sucesión de homomorfismos de D-módulos pola esquerda (pola dereita) $d_i : M_i \longrightarrow M_{i-1}$ entre D-módulos pola esquerda (pola dereita) cumprindo $\mathrm{Im}(d_{i+1}) \subset \ker(d_i)$ (equivalentemente, $d_i \circ d_{i+1} = 0$) para cada $i \in \mathbb{Z}$. Denotámolo por:

$$M_\bullet \ \ldots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \ldots \ . \tag{3.2}$$

Un *cocomplexo de D-módulos pola esquerda* (*pola dereita*) é unha sucesión de homomorfismos de D-módulos pola esquerda (pola dereita) $d_i : M_{i-1} \longrightarrow M_i$ entre D-módulos pola esquerda (pola dereita) cumprindo $\mathrm{Im}(d_{i-1}) \subset \ker(d_i)$ para cada $i \in \mathbb{Z}$. Denotámolo por:

$$M^\bullet \ \ldots \xleftarrow{d_{i+2}} M_{i+1} \xleftarrow{d_{i+1}} M_i \xleftarrow{d_i} M_{i-1} \xleftarrow{d_{i-1}} \ldots \ . \tag{3.3}$$

(2) Dado o complexo de D-módulos pola esquerda (pola dereita) $M_\bullet$ de (3.2), definimos o *defecto de exactitude* en M_i ou o *i-ésimo módulo de homoloxía* como o D-módulo pola esquerda (pola dereita) $H_i(M_\bullet) = \ker(d_i)/\mathrm{Im}(d_{i+1})$.

De forma análoga, dado o cocomplexo de D-módulos pola esquerda (pola dereita) $M^\bullet$ de (3.3), definimos o *defecto de exactitude* en M_i ou o *i-ésimo módulo de cohomoloxía* como o D-módulo pola esquerda (pola dereita) $H^i(M^\bullet) = \ker(d_{i+1})/\mathrm{Im}(d_i)$.

(3) O complexo $M_\bullet$ de (3.2) dise *exacto* en M_i se $H_i(M_\bullet) = 0$, isto é, se $\ker(d_i) = \mathrm{Im}\ (d_{i+1})$. Se isto ocorre para cada $i \in \mathbb{Z}$, entón chámase unha *sucesión exacta*. No caso dun cocomplexo $M^\bullet$, dise unha *sucesión exacta* se $H^i(M^\bullet) = 0$, isto é, se $\ker(d_i) = \mathrm{Im}(d_{i-1})$.

(4) Unha *sucesión exacta curta* é unha sucesión exacta da forma:

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

isto é, f é inxectivo, g é sobrexectivo e $\mathrm{Im}(f) = \ker g$.

(5) Unha *resolución libre e finita* do D-módulo pola esquerda M é unha sucesión exacta da forma:

$$\ldots \xrightarrow{.R_4} D^{1\times r_3} \xrightarrow{.R_3} D^{1\times r_2} \xrightarrow{.R_2} D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0, \tag{3.4}$$

onde $R_i \in D^{r_i \times r_{i-1}}$, $.R_i : D^{1\times r_i} \longrightarrow D^{1\times r_{i-1}}$ é o homomorfismo de D-módulos pola esquerda dado por $(.R_i)(\lambda) = \lambda R_i \in D^{1\times r_{i-1}}$, $\lambda \in D^{1\times r_i}$, $i \in \mathbb{N}$, e π é un homomorfismo de D-módulos pola esquerda sobrexectivo.

Analogamente, unha *resolución libre e finita* do D-módulo pola dereita N é unha sucesión exacta da forma:

$$\ldots \xrightarrow{S_4\cdot} D^{s_3\times 1} \xrightarrow{S_3\cdot} D^{s_2\times 1} \xrightarrow{S_2\cdot} D^{s_1\times 1} \xrightarrow{S_1\cdot} D^{s_0\times 1} \xrightarrow{\kappa} N \longrightarrow 0, \tag{3.5}$$

onde $S_i \in D^{s_{i-1}\times s_i}$, $S_i. : D^{s_i\times 1} \longrightarrow D^{s_{i-1}\times 1}$ é o homomorfismo de D-módulos pola dereita dado por $(S_i.)(\mu) = S_i\mu \in D^{s_{i-1}\times 1}$, $\mu \in D^{s_i\times 1}$, $i \in \mathbb{N}$, e κ é un homomorfismo de D-módulos pola dereita sobrexectivo.

Se en (3.4) e (3.5) os D-módulos libres non son de rango finito falaremos, simplemente, de *resolucións libres*. Se os D-módulos pola esquerda non son libres, pero si proxectivos, falaremos de *resolución proxectiva*.

Nas definicións de complexo e cocomplexo de D-módulos pola esquerda o índice i chámase *grao*. Notemos que un complexo de D-módulos pola esquerda diminúe o grao do módulo de i a $i-1$, e un cocomplexo auméntao de $i-1$ a i.

Observación 3.13. É fácil comprobar que as aplicacións definidas en (3.4) son homomorfismos de D-módulos pola esquerda. En efecto, tomando $\lambda_1, \lambda_2 \in D^{1\times r_i}$ arbitrarios, temos que $(.R_i)(\lambda_1+\lambda_2) = (\lambda_1+\lambda_2)R_i = \lambda_1R_i + \lambda_2R_i = (.R_i)(\lambda_1) + (.R_i)(\lambda_2)$, e para calquera $d \in D$, $(.R_i)(d\lambda) = (d\lambda)R_i = d(\lambda R_i) = d(.R_i)(\lambda)$. Cun razoamento análogo compróbase tamén que as aplicacións $S_i.$ definidas en (3.5) son homomorfismos de D-módulos pola dereita.

Máis adiante aparecerán as aplicacións $R_i. : F^{r_{i-1}\times 1} \longrightarrow F^{r_i\times 1}$, que a cada $\zeta \in F^{r_{i-1}}$ lle fan corresponder $R_i\zeta \in F^{r_i\times 1}$, e onde F é un D-módulo pola esquerda. A condición $(R_i.)(\lambda_1 + \lambda_2) = (R_i.)(\lambda_1) + (R_i.)(\lambda_2)$ satisfaise claramente para calquera $\lambda_1, \lambda_2 \in F^{r_{i-1}\times 1}$. Así e todo, tomando $d \in D$ e $\lambda \in F^{r_{i-1}\times 1}$ calquera, debemos observar que en xeral $(R_i.)(d\lambda) = R_i(d\lambda)$ é distinto de $(dR_i)\lambda = d(R_i.)(\lambda)$, pois D non ten por que ser un anel conmutativo. No caso de que o sexa si que se ten a condición $(R_i.)(d\lambda) = d(R_i.)(\lambda)$ e así $R_i.$ é un homomorfismo de D-módulos pola esquerda.

Con todo, as aplicacións $R_i.$ si que son homomorfismos de grupos abelianos. Nestas circustancias a definición de cocomplexo dada en (3.3) xeneralízase facilmente ao caso no que os homomorfismos d_i son homomorfismos de grupos (notemos que os módulos M_i teñen, en particular, estrutura de grupos abelianos). Deste xeito, falaremos de *cocomplexos de grupos abelianos* cando sexa conveniente.

Imos probar agora un par de resultados que nos van permitir entender a relación que existe entre os conceptos que vimos de presentar e a teoría exposta nas anteriores seccións. A Proposición 3.14 indica simplemente que implicacións ten que un D-módulo pola esquerda sexa finitamente presentado. Doutra banda, a Proposición 3.15 constitúe o resultado máis importante desta sección, pois dinos que, baixo condicións moi xerais, todo D-módulo pola esquerda finitamente xerado admite unha resolución libre e finita.

Proposición 3.14. *Sexa D un anel, M un D-módulo pola esquerda e $\pi : D^{1\times r_0} \longrightarrow M$ unha presentación libre e finita de M, con $r_0 \in \mathbb{N}$. Entón tense a seguinte sucesión exacta curta:*

$$0 \longrightarrow \ker(\pi) \xrightarrow{i} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0,$$

onde $i\colon \ker(\pi) \longrightarrow D^{1\times r_0}$ *é a inclusión do* D*-módulo pola esquerda* $\ker(\pi)$ *en* $D^{1\times r_0}$.

Demostración. En efecto, xa que $\pi\colon D^{1\times r_0} \longrightarrow M$ é unha presentación libre e finita de M, tense que π é sobrexectiva. Doutra banda, a inclusión $i\colon \ker(\pi) \longrightarrow D^{1\times r_0}$ é trivialmente inxectiva, e tamén está claro que $\mathrm{Im}(i) = \ker(\pi)$. Cúmprense entón as condicións para que o complexo de D-módulos pola esquerda do enunciado sexa unha sucesión exacta curta. ■

Proposición 3.15. *Sexa* D *un anel noetheriano pola esquerda, e* M *un* D*-módulo pola esquerda finitamente xerado. Entón* M *admite unha resolución libre e finita.*

Demostración. En primeiro lugar observemos que por ser D un anel noetheriano pola esquerda e M un D-módulo pola esquerda finitamente xerado, en virtude do Corolario 2.26, M é tamén finitamente presentado, e daquela temos a seguinte sucesión exacta curta:

$$0 \longrightarrow \ker(\pi) \xrightarrow{i} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0,$$

como indicamos na Proposición 3.14. Como $\ker(\pi)$ é, de novo, un D-submódulo pola esquerda de $D^{1\times r_0}$, temos que é finitamente xerado, e daquela existe un homomorfismo sobrexectivo de D-módulos pola esquerda, $\kappa\colon D^{1\times r_1} \longrightarrow \ker(\pi)$, para algún $r_1 \in \mathbb{N}$. Definamos $.R_1 = i \circ \kappa\colon D^{1\times r_1} \longrightarrow D^{1\times r_0}$. A notación é axeitada, xa que se trata dun homomorfismo de D-módulos pola esquerda entre dous módulos libres de rango finito, de xeito que podemos atopar $R_1 \in D^{r_1\times r_0}$ tal que $i \circ \kappa(d_1, ..., d_{r_1}) = (d_1, ..., d_{r_1})R_1$, operando coa multiplicación de matrices habitual. Se tomamos as bases canónicas en $D^{1\times r_1}$ e $D^{1\times r_0}$ a matriz R_1 constrúese colocando os xeradores de $\ker \pi$ por filas, e entón $\ker \pi = D^{1\times r_1}R_1$.

Temos entón a seguinte sucesión exacta:

$$0 \longrightarrow \ker(.R_1) \xrightarrow{i_1} D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0.$$

Neste caso i_1 é a inclusión de $\ker(.R_1)$ en $D^{1\times r_1}$. A anterior é, en efecto, unha sucesión exacta, xa que $\mathrm{Im}(.R_1) = \mathrm{Im}(i \circ \kappa) = i(\mathrm{Im}(\kappa)) = i(\ker \pi) = \ker \pi$, onde empregamos que $\kappa\colon D^{1\times r_1} \longrightarrow \ker(\pi)$ é sobrexectivo, e $\mathrm{Im}(i_1) = \ker(.R_1)$ claramente. Repetindo este proceso atopamos unha resolución libre e finita de M:

$$\ldots \xrightarrow{.R_4} D^{1\times r_3} \xrightarrow{.R_3} D^{1\times r_2} \xrightarrow{.R_2} D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0,$$

de xeito que $\mathrm{Im}(.R_{i+1}) = D^{1\times r_{i+1}}R_{i+1} = \ker(.R_i)$, $i \in \mathbb{N}$. ■

En virtude da Proposición 3.15, de agora en adiante asumiremos que todo D-módulo pola esquerda finitamente presentado admite unha resolución libre e finita. Vistos estes resultados, cómpre introducir os *módulos de sicixia* dun D-módulo pola esquerda que admite unha resolución libre e finita, pois agora sabemos que esta vai ser a situación na que nos atopemos. A utilidade da seguinte definición para nós non vai máis alá dunha simplificación da notación, pero é relevante no marco da Álxebra Homolóxica.

Definición 3.16. Sexa D un anel e M un D-módulo pola esquerda que admite a seguinte resolución libre e finita:

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

O D-submódulo pola esquerda $\ker\pi$ de $D^{1\times r_0}$ chámase o *módulo de sicixia* de M, e o D-submódulo $\ker(.R_n)$ de $D^{1\times r_n}$ chámase o *n-ésimo módulo de sicixia* de M.

A continuación imos presentar un algoritmo que nos vai permitir calcular unha resolución libre e finita dun módulo finitamente xerado (isto é equivalente a calcular os seus módulos de sicixia) a partir das técnicas das bases de Gröbner. Debemos restrinxirnos a aneis noetherianos pola esquerda D que sexan álxebras de Ore nas condicións expostas en (3.1), pois é esta a situación na que se teñen xeneralizacións do algoritmo de Buchberger.

Algoritmo 3.17

Entrada: *Un conxunto de xeradores $\{R_1,...,R_q\}\subset D^{1\times p}$ dun D-submódulo pola esquerda N de $D^{1\times p}$, de xeito que ao colocar $R_1,...,R_q$ por filas tense unha matriz R que define o homomorfismo de D-módulos pola esquerda $.R\colon D^{1\times q}\longrightarrow D^{1\times p}$, e $N=D^{1\times q}R$.*

Saída: *Unha matriz $S\in D^{r\times q}$ tal que $\ker(.R)=D^{1\times r}S$.*

(1) Introducimos as variables $\eta_1,...,\eta_p$, $\zeta_1,...,\zeta_q$ e o conxunto, contido no D-módulo libre L xerado por $\eta_1,...,\eta_p$, $\zeta_1,...,\zeta_q$, $L=D\eta_1\bigoplus\cdots\bigoplus D\eta_p\bigoplus D\zeta_1\bigoplus\cdots\bigoplus D\zeta_q$:

$$\left\{\sum_{j=1}^{p}R_{ij}\eta_j-\zeta_i\mid i=1,...,q\right\}.$$

Consideramos P o D-submódulo pola esquerda xerado polo devandito conxunto.

(2) Calculamos unha base de Gröbner G de P en L respecto dunha orde admisible que elimina $\eta_1,...,\eta_p$.

(3) Realizamos a intersección $G\cap(D\zeta_1\bigoplus\cdots\bigoplus D\zeta_q)=\left\{\sum_{i=1}^{q}S_{ki}\zeta_i\mid k=1,...,r\right\}$, tomando os elementos de G que conteñen só variables ζ, e construímos a matriz $S=(S_{ij})\in D^{r\times q}$.

O algoritmo que vimos de presentar atópase explicado de forma esquemática en [3, 17], pero nós imos tratar de ver por que é efectivo á hora de achar o módulo de sicixia (Observación 3.18) e por que pode ser utilizado para calcular unha resolución libre e finita no marco da Análise Alxébrica (Observación 3.19).

Observación 3.18. Ollando o Algoritmo 3.17 está claro que son esenciais as técnicas das bases de Gröbner. Así e todo, a idea principal do algoritmo está baseada na noción de *condicións de compatibilidade* propia da teoría de Sistemas Matemáticos, como a continuación amosamos.

Supoñamos entón a situación do Algoritmo 3.17: un D-submódulo pola esquerda de $D^{1\times p}$, N, de xeito que $N=D^{1\times q}R$, con $R\in D^{q\times p}$. Supoñamos tamén que coñecemos a saída do algoritmo: unha matriz $S\in D^{r\times q}$ tal que $D^{1\times r}S=\ker(.R)$, sendo $.R\colon D^{1\times q}\longrightarrow D^{1\times p}$ o homomorfismo de D-módulos pola esquerda definido multiplicando pola dereita pola matriz R (como xa é habitual).

Tomemos agora $\lambda\in\ker(.R)$ arbitrario, logo $\lambda R=0$. Xa que $\ker(.R)=D^{1\times r}S$, $\lambda=\mu S$ para algún $\mu\in D^{1\times r}$. Escollamos tamén $\zeta\in D^{1\times p}$ calquera, e consideremos o sistema linear non homoxéneo $R\eta=\zeta$. Operando coa multiplicación de matrices usual: $\lambda\zeta=\lambda(R\eta)=(\lambda R)\eta=0$. Cambiando λ por μS: $(\mu S)\zeta=\mu(S\zeta)=0$. Xa que isto é certo para todo $\lambda\in\ker(.R)$, por

$\ker(.R) = D^{1\times r}S$ teremos que $\mu(S\zeta) = 0$ é certo para todo $\mu \in D^{1\times r}$, logo necesariamente $S\zeta = 0$. Dise nestas circunstancias que *as condicións de compatibilidade de* $R\eta = \zeta$ *están xeradas por* $S\zeta = 0$, isto é, para que $R\eta = \zeta$ teña solución debe terse que $S\zeta = 0$.

Isto permítenos comprender xa o fundamento do Algoritmo 3.17. A matriz S que buscamos xera as condicións de compatibilidade do sistema $R\eta = \zeta$, con $\zeta \in D^{1\times p}$ calquera. Se tomamos $\zeta = (\zeta_1, \ldots, \zeta_q)^T$ un vector de $D^{1\times p}$ xenérico, as mesmas condicións de compatibilidade podemos atopalas eliminando $\eta_1, ..., \eta_p$ do sistema sobredeterminado $R\eta - \zeta = 0$ nas variables $\eta_1, \ldots, \eta_p, \zeta_1, \ldots, \zeta_q$. Isto pode realizarse mediante as técnicas das bases de Gröbner se D é unha álxebra de Ore nas condicións de (3.1). A matriz S obtense expresando as condicións de compatibilidade de forma linear: $S\zeta = 0$.

Observación 3.19. A aclaración anterior permitiunos entender o fundamento do Algoritmo 3.17. Agora imos ver como pode ser este utilizado para calcular unha resolución libre e finita do D-módulo pola esquerda $M = D^{1\times p}/(D^{1\times q}R)$, onde $R \in D^{1\times p}$ e D é un anel noetheriano pola esquerda nas condicións (3.1). A proxección canónica en M, $\pi\colon D^{1\times p} \longrightarrow M$, é o primeiro elemento da resolución libre e finita de M, pois $\ker\pi = D^{1\times q}R$, co que a seguinte é unha sucesión exacta:

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

Agora podemos aplicar o Algoritmo 3.17 para obter unha matriz $S \in D^{r\times q}$ que cumpra a condición $\ker(.R) = D^{1\times r}S$, e que estende a anterior sucesión exacta:

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

Iterando este proceso vemos que o Algoritmo 3.17 permite calcular unha resolución libre e finita como a de (3.4) do módulo do sistema $M = D^{1\times p}/(D^{1\times q}R)$.

As Observacións 3.18 e 3.19 axudan a comprender a relevancia do Algoritmo 3.17 no marco da Análise Alxébrica. Para rematar esta sección imos presentar un exemplo de gran importancia desde un punto de vista físico e matemático, e no que o cálculo da resolución libre e finita se realiza utilizando os conceptos explicados na Observación 3.18, sen necesidade de aplicar o Algoritmo 3.17. Debemos notar, así e todo, que estamos aplicando as ideas baixo as que se constrúe o devandito algoritmo. A única excepción é a utilización das técnicas de bases de Gröbner, que polo de agora trataremos de evitar nos exemplos que pretendamos resolver de forma manual, aínda que resultan fundamentais cando isto non é posible.

Exemplo 3.20. En Física é ben coñecido que as condicións de compatibilidade do operador gradiente en $\mathbb{R}^3$ están definidas polo operador rotacional. Por exemplo, o campo electrostático pódese escribir como o gradiente do *potencial electrostático* (que é unha función escalar), $\vec{E} = -\vec{\nabla}\phi$, e necesariamente é *irrotacional*: $\vec{\nabla} \times \vec{E} = 0$. Do mesmo xeito, as condicións de compatibilidade do operador rotacional están definidas polo operador diverxencia. Por exemplo, o campo magnético sempre se pode escribir como o rotacional do *potencial vectorial*, $\vec{B} = \vec{\nabla} \times \vec{A}$, e necesariamente é *solenoidal*: $\vec{\nabla} \cdot \vec{B} = 0$. Recordemos que $\vec{\nabla}\phi$ é o gradiente dun campo escalar ϕ en $\mathbb{R}^3$, e $\vec{\nabla} \times \vec{F}$, $\vec{\nabla} \cdot \vec{F}$ representan, respectivamente, o rotacional e a diverxencia dun campo vectorial $\vec{F}$ en $\mathbb{R}^3$.

Empregando isto e a anterior observación temos a seguinte resolución libre e finita (de lonxitude finita):

$$0 \longrightarrow D \xrightarrow{.R_3} D^{1\times 3} \xrightarrow{.R_2} D^{1\times 3} \xrightarrow{.R_1} D \xrightarrow{\pi} M \longrightarrow 0,$$

onde $D = \mathbb{R}[\partial_1, \partial_2, \partial_3]$, $M = D/(D\partial_1 + D\partial_2 + D\partial_3) = D/(D^{1\times 3}R_1)$, e R_1, R_2, R_3 son as matrices que representan o gradiente, o rotacional e a diverxencia na álxebra de Ore D:

$$R_1 = (\partial_1\ \partial_2\ \partial_3)^T \in D^{3\times 1}, \quad R_2 = \begin{pmatrix} 0 & -\partial_3 & \partial_2 \\ \partial_3 & 0 & -\partial_1 \\ -\partial_2 & \partial_1 & 0 \end{pmatrix} \in D^{3\times 3}, \quad R_3 = R_1^T \in D^{1\times 3}.$$

3.3. Os grupos abelianos das extensións na Análise Alxébrica

Na anterior sección introducimos unha serie de conceptos básicos da Álxebra Homolóxica (máis concretamente, na Definición 3.12). Como principal resultado obtivemos que, baixo condicións moi xerais (D un anel noetheriano pola esquerda) o D-módulo do sistema $R\eta = 0$ admite unha resolución libre e finita, sendo R unha matriz $q \times p$ con entradas en D. Ademais, se D é unha álxebra de Ore nas condicións (3.1), esta resolución libre e finita pode ser calculada de xeito iterativo empregando o Algoritmo 3.17.

Pretendemos agora introducir outra das ferramentas da Álxebra Homolóxica na Análise Alxébrica: os grupos abelianos das extensións, $\mathrm{ext}^i_D(M, D)$, que poden ser calculados empregando calquera resolución libre e finita do D-módulo do sistema, M. Trataremos de motivar en primeiro lugar como estes aparecen de xeito natural na teoría de Sistemas Matemáticos, para despois definilos de forma máis precisa utilizando as nocións expostas na anterior sección. A súa utilidade farase evidente no vindeiro capítulo: veremos que permiten caracterizar as propiedades dos módulos introducidas na Definición 2.28 e que estas, á súa vez, están relacionadas con outras propiedades dos sistemas lineares moi comúns e interesantes na Teoría do Control.

Comecemos entón tratando de ver como aparecen os grupos abelianos das extensións no estudo de sistemas lineares. Supoñamos D un anel noetheriano pola esquerda e M o D-módulo pola esquerda finitamente presentado por R_1, con $R_1 \in D^{r_1\times r_0}$, $M = D^{1\times r_0}/(D^{1\times r_1}R_1)$. Nestas circunstancias podemos tomar unha resolución libre e finita de M:

$$\ldots \xrightarrow{.R_4} D^{1\times r_3} \xrightarrow{.R_3} D^{1\times r_2} \xrightarrow{.R_2} D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0. \tag{3.6}$$

Consideremos F un D-módulo pola esquerda e o sistema non homoxéneo $R_1\eta = \zeta$, con $\zeta \in F^{r_0\times 1}$ fixado e $\eta \in F^{r_1\times 1}$ un vector de incógnitas. Por ser (3.6) un complexo exacto tense que $\ker(.R_1) = \mathrm{Im}(.R_2) = D^{1\times r_2}R_2$. Tomemos $\mu \in D^{1\times r_2}$ calquera. Como $\mu R_2 \in \ker(.R_1) \subset D^{1\times r_1}$, resulta que $(\mu R_2)R_1 = 0$. Multipliquemos agora ambos lados da ecuación $R_1\eta = \zeta$ por μR_2: $(\mu R_2)R_1\eta = \mu R_2\zeta$. Utilizando $(\mu R_2)R_1 = 0$, chegamos a $(\mu R_2)\zeta = \mu(R_2\zeta) = 0$. Xa que isto é certo para calquera $\mu \in D^{1\times r_2}$, necesariamente $R_2\zeta = 0$.

Observación 3.21. Notemos que o razoamento utilizado é practicamente idéntico ao exposto na Observación 3.18. De feito, a única diferenza é que nesta última tomabamos ζ un vector con entradas no propio anel D, pois necesitabamos aplicar as técnicas de eliminación das bases de Gröbner á ecuación $R_1\eta - \zeta = 0$, e para iso precisamos que a ecuación se escriba só empregando elementos dun anel nas condicións (3.1). Así e todo, a conclusión é exactamente a mesma: unha condición necesaria (condición de compatibilidade) para resolver o sistema $R_1\eta = 0$ no D-módulo pola esquerda F é que $R_2\zeta = 0$, onde $\ker(.R_1) = D^{1\times r_2}R_2$.

Preguntámonos agora cando a anterior condición, ademais de necesaria, é suficiente. Esta cuestión podemos formulala empregando o seguinte cocomplexo de grupos abelianos:

$$F^{r_2\times 1} \xleftarrow{R_2\cdot} F^{r_1\times 1} \xleftarrow{R_1\cdot} F^{r_0\times 1} \tag{3.7}$$

onde os homomorfismos de grupos $R_i.\colon F^{r_{i-1}\times 1} \longrightarrow F^{r_i\times 1}$ levan a cada $\zeta \in F^{r_{i-1}\times 1}$ en $R_i.(\zeta) = R_i\zeta \in F^{r_i\times 1}$, con $i = 1,2$. Aínda que $F^{r_0\times 1}$, $F^{r_1\times 1}$ e $F^{r_2\times 1}$ son D-módulos pola esquerda, debemos lembrar a cuestión exposta na Observación 3.13: as aplicacións $R_i.$ non son, en xeral, homomorfismos de D-módulos pola esquerda, pero si homomorfismos de grupos, de aí que (3.7) sexa un cocomplexo de grupos abelianos.

Deste xeito, que $R_1\eta = \zeta$ implique $R_2\zeta = 0$ é equivalente a que $\zeta \in \mathrm{Im}(R_1.)$ implique $\zeta \in \ker(R_2.)$, o que asegura que (3.7) sexa, en efecto, un cocomplexo. Máis aínda, que a condición $R_2\zeta = 0$ sexa suficiente para poder resolver $R_1\eta = \zeta$ equivale a dicir que o cocomplexo (3.7) sexa exacto en $F^{r_1\times 1}$. Definindo $\mathrm{ext}^1_D(M,F)$ como o defecto de exactitude en $F^{r_1\times 1}$, isto é, $\mathrm{ext}^1_D(M,F) = \ker(R_2.)/\mathrm{Im}(R_1.)$, a condición é suficiente se e só se $\mathrm{ext}^1_D(M,F) = 0$. Comprobamos así como aparecen de maneira natural os grupos abelianos $\mathrm{ext}^1_D(M,F)$ no marco da teoría de Sistemas Matemáticos.

A continuación trataremos de definir de forma precisa o concepto que vimos de introducir, xunto cos grupos abelianos de orde superior $\mathrm{ext}^i_D(M,F)$. A exposición que aquí presentamos está baseada nas que se realizan en [3, 17], mais acudiremos con frecuencia aos resultados de Álxebra Homolóxica expostos en [21].

Imos ver en primeiro lugar que a resolución libre e finita de M dada en (3.6) induce un cocomplexo de grupos abelianos do que forma parte o cocomplexo (3.7). Para iso introducimos un cocomplexo de grupos abelianos asociado a toda resolución libre e finita dun D-módulo pola esquerda M. A definición poderíase facer máis xeral, considerando unha resolución proxectiva no canto dunha resolución libre e finita. Con todo, decidimos restrinxirnos ao marco no que son aplicables os resultados e as ideas da Análise Alxébrica.

Definición 3.22. Sexa D un anel noetheriano pola esquerda, M un D-módulo pola esquerda finitamente xerado, F un D-módulo pola esquerda e

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

unha resolución libre e finita de M. Entón pódese construír o seguinte cocomplexo de grupos abelianos:

$$\ldots \xleftarrow{(.R_4)^*} \hom(D^{1\times r_3},F) \xleftarrow{(.R_3)^*} \hom_D(D^{1\times r_2},F) \xleftarrow{(.R_2)^*} \hom(D^{1\times r_1},F) \xleftarrow{(.R_1)^*} \hom(D^{1\times r_0},F) \longleftarrow 0, \tag{3.8}$$

onde os homomorfismos defínense como $(.R_i)^*(f) = f\circ .R_i$ para $f \in \hom(D^{1\times r_{i-1}},F)$, $i \geq 1$. A partir deste definimos os grupos abelianos $\mathrm{ext}^i_D(M,F)$ utilizando os defectos de exactitude (ou cohomoloxías) do complexo anterior:

$$\begin{cases} \mathrm{ext}^0_D(M,F) = \ker((.R_1)^*) \\ \mathrm{ext}^i_D(M,F) = \ker((.R_{i+1})^*)/\mathrm{Im}((.R_i)^*),\ i \geq 1. \end{cases} \tag{3.9}$$

Observación 3.23. Podemos comprobar que (3.8) é, en efecto, un cocomplexo de grupos abelianos. Chega con verificar que se cumpre $(.R_{i+1})^*\circ(.R_i)^* = 0$ para todo $i \geq 1$. Sexa

entón $f \in \hom(D^{1\times r_{i-1}}, F)$ calquera, tense que

$$((.R_{i+1})^* \circ (.R_i)^*)(f) = (.R_{i+1})^*((.R_i)^*(f)) = (.R_{i+1})^*(f \circ .R_i) = (f \circ .R_i) \circ .R_{i+1}.$$

Xa que $((.R_{i+1})^* \circ (.R_i)^*)(f) \in \hom(D^{1\times r_i}, F)$, tomamos $\lambda \in D^{1\times r_i}$ e avaliamos:

$$((.R_{i+1})^* \circ (.R_i)^*)(f)(\lambda) = (f \circ .R_i) \circ .R_{i+1}.(\lambda) \overset{(a)}{=} f \circ (.R_i \circ .R_{i+1})(\lambda) \overset{(b)}{=} 0.$$

En (a) empregamos a asociatividade da composición de aplicacións, e en (b) que por ser (3.6) unha resolución libre e finita, en particular é un complexo de D-módulos pola esquerda, logo $.R_i \circ .R_{i+1} = 0$, $i \geq 1$. Isto proba que (3.8) é un cocomplexo de grupos abelianos.

No vindeiro capítulo necesitaremos calcular os grupos abelianos das extensións de D-módulos pola dereita. Cómpre sinalar que para o caso no que D é un anel noetheriano pola dereita e N un D-módulo pola dereita finitamente presentado tamén temos unha resolución libre e finita de n. A demostración é totalmente análoga á realizada na Proposición 3.15, razoando agora coa definición de D-módulo pola dereita finitamente presentado. Podemos entón presentar tamén o análogo da definición anterior para D-módulos pola dereita.

Definición 3.24. Sexa D un anel noetheriano pola dereita, N un D-módulo pola dereita finitamente xerado, F un D-módulo pola dereita e

$$\ldots \xrightarrow{S_4\cdot} D^{s_3\times 1} \xrightarrow{S_3\cdot} D^{s_2\times 1} \xrightarrow{S_2\cdot} D^{s_1\times 1} \xrightarrow{S_0\cdot} D^{s_0\times 1} \xrightarrow{\kappa} N \longrightarrow 0,$$

unha resolución libre e finita de N. Entón pódese construír o seguinte cocomplexo de grupos abelianos:

$$\ldots \xleftarrow{(S_4\cdot)^*} \hom(D^{s_3\times 1}, F) \xleftarrow{(S_3\cdot)^*} \hom_D(D^{s_2\times 1}, F) \xleftarrow{(S_2\cdot)^*} \hom(D^{s_1\times 1}, F) \xleftarrow{(S_1\cdot)^*} \hom(D^{s_0\times 1}, F) \longleftarrow 0,$$

onde os homomorfismos defínense como $(S_i\cdot)^*(f) = f \circ S_i$ para $f \in \hom(D^{s_{i-1}\times 1}, F)$, $i \geq 1$. A partir deste definimos os grupos abelianos $\operatorname{ext}^i_D(N, F)$ utilizando os defectos de exactitude (ou cohomoloxías) do complexo anterior:

$$\begin{cases} \operatorname{ext}^0_D(N,F) = \ker((S_1\cdot)^*) \\ \operatorname{ext}^i_D(N,F) = \ker((S_{i+1}\cdot)^*)/\operatorname{Im}((S_i\cdot)^*),\ i \geq 1. \end{cases} \tag{3.10}$$

Na linguaxe de Álxebra Homolóxica, o cocomplexo de grupos abelianos que vimos de introducir dise que se obtivo da resolución libre e finita do D-módulo pola esquerda M *aplicando o funtor contravariante* $\hom(-, F)$. Para nós o único relevante é que podemos aplicar os seguintes resultados ao noso contexto. O primeiro deles xustifica a notación empregada na anterior definición: os grupos abelianos $\operatorname{ext}^i_D(M, F)$ non dependen da resolución libre e finita de M empregada.

Proposición 3.25. *O grupo abeliano $\operatorname{ext}^i_D(M, F)$, con $i \in \mathbb{Z}_{\geq 0}$, só depende de M e de F (agás isomorfismos de grupos). Daquela, podemos escoller calquera resolución libre e finita de M para calculalo.*

Imos agora tratar de expresar o complexo de grupos abelianos da Definición 3.22 dunha forma conveniente. En primeiro lugar imos probar o seguinte resultado, aplicando o isomorfismo de Malgrange do Teorema 2.20.

Proposición 3.26. *Sexa D un anel noetheriano pola esquerda e F un D-módulo pola esquerda. Entón, se $r_i \in \mathbb{N}$, tense o seguinte isomorfismo de grupos abelianos:*

$$\theta_i : \hom(D^{1\times r_i}, F) \simeq F^{r_i\times 1}.$$

Demostración. Definamos a matriz $R_i = (0,\dots,0) \in D^{1\times r_i}$ e consideremos o D-módulo pola esquerda finitamente presentado por R_i, isto é, $M = D^{1\times r_i}/(DR_i)$. O Teorema 2.20 dános o isomorfismo de Malgrange, que é o seguinte isomorfismo de grupos abelianos:

$$\begin{array}{rcl} \chi^{-1} : \hom(M,F) & \longrightarrow & \ker(R_i.) \\ \phi & \longmapsto & y = (\phi(y_1),...,\phi(y_{r_i}))^T \end{array}$$

onde $y_j = \pi(f_j)$, $j = 1,\dots,r_i$ e $\{f_1,...,f_{r_i}\}$ é a base canónica de $D^{1\times r_i}$. Vexamos cal é este isomorfismo para o caso da matriz R_i e o módulo M que vimos de introducir.

- Para calquera $d \in D$, $dR_i = 0 \in D^{1\times r_i}$, de onde $DR_i = 0$. Deste xeito a proxección canónica en M, $\pi\colon D^{1\times r_i} \longrightarrow M$, leva cada $\lambda \in D^{1\times r_i}$ en $\pi(\lambda) = \lambda + DR_i = \lambda + 0 = \lambda$. Nestas circunstancias, π é un isomorfismo de D-módulos pola esquerda, e daquela o D-módulo pola esquerda finitamente presentado por R_i é isomorfo a $D^{1\times r_i}$.

- Empregando que a proxección canónica é un isomorfismo podemos definir a seguinte aplicación:

  $$\begin{array}{rcl} \widetilde{\pi} : \hom(M,F) & \longrightarrow & \hom(D^{1\times r_i}, F) \\ \phi & \longmapsto & \widetilde{\pi}(\phi) = \phi\circ\pi \end{array}$$

  que claramente está ben definida, tendo en conta o dominio e o rango da proxección canónica. Ademais, é un homomorfismo de grupos, pois para calquera par de homomorfismos $\phi_1, \phi_2 \in \hom(M,F)$, tense que $\widetilde{\pi}(\phi_1+\phi_2) = (\phi_1+\phi_2)\circ\pi = \phi_1\circ\pi + \phi_2\circ\pi$. Finalmente, tamén está claro que é bixectiva, pois a aplicación

  $$\begin{array}{rcl} \widetilde{\pi}^{-1} : \hom(D^{1\times r_i}, F) & \longrightarrow & \hom(M,F) \\ \psi & \longmapsto & \widetilde{\pi}^{-1}(\psi) = \psi\circ\pi^{-1} \end{array}$$

  é a súa inversa, como se comproba moi facilmente:

  $$\phi \in \hom(M,F),\ (\widetilde{\pi}^{-1}\circ\widetilde{\pi})(\phi) = \widetilde{\pi}^{-1}(\phi\circ\pi) = (\phi\circ\pi)\circ\pi^{-1} = \phi\circ(\pi\circ\pi^{-1}) = \phi.$$

- Doutra banda, consideremos o sistema linear $R_i\eta = 0$, e buscamos a solución en $F^{r_i\times 1}$. Xa que $R_i = (0,\dots,0)$, $R_i = 0$ para calquera $\eta \in F^{r_i\times 1}$, tense que o conxunto de solucións do sistema é $\ker(R.) = F^{r_i\times 1}$.

O isomorfismo $\theta_i\colon \hom(D^{1\times r_i}, F) \simeq F^{r_i\times 1}$ atopámolo compoñendo $\widetilde{\pi}^{-1}$ con χ^{-1}:

$$\begin{array}{rcl} \theta_i\colon \hom(D^{1\times r_i}, F) & \longrightarrow & F^{r_i\times 1} \\ \psi & \longmapsto & \chi^{-1}\left(\widetilde{\pi}^{-1}(\psi)\right) = \chi^{-1}\left(\psi\circ\pi^{-1}\right) = (\psi(f_1),\dots,\psi(f_{r_i}))^T \end{array} \quad (3.11)$$

onde empregamos que $y_j = \pi(f_j)$ para $j = 1,\dots,r_i$, e a definición do isomorfismo de Malgrange χ^{-1}, $\chi^{-1}\left(\psi\circ\pi^{-1}\right) = \left(\psi\left(\pi^{-1}(y_1)\right),\dots,\psi\left(\pi^{-1}(y_{r_i})\right)\right)^T$. ∎

Observación 3.27. Imos utilizar o anterior resultado para expresar o cocomplexo da Definición 3.22 de forma notablemente máis simple. Partimos entón do devandito cocomplexo:

$$\ldots \xleftarrow{(.R_3)^*} \hom(D^{1\times r_2}, F) \xleftarrow{(.R_2)^*} \hom(D^{1\times r_1}, F) \xleftarrow{(.R_1)^*} \hom(D^{1\times r_0}, F) \longleftarrow 0.$$

Pretendemos utilizar os isomorfismos $\theta_i : \hom(D^{1\times r_i}, F) \simeq F^{r_i\times 1}$ para cambiar cada grupo abeliano $\hom(D^{1\times r_i}, F)$ por $F^{r_i\times 1}$, e así ter un novo cocomplexo de grupos abelianos:

$$\ldots \xleftarrow{g_3} F^{r_2\times 1} \xleftarrow{g_2} F^{r_1\times 1} \xleftarrow{g_1} F^{r_0\times 1} \longleftarrow 0.$$

Os homomorfismos de grupos abelianos $g_i\colon F^{r_{i-1}\times 1} \longrightarrow F^{r_i\times 1}$ débense definir de maneira que respecten os isomorfismos $\theta_i : \hom(D^{1\times r_i}, F) \simeq F^{r_i\times 1}$. Dito doutra maneira, o seguinte diagrama debe ser conmutativo:

$$\begin{array}{ccc} \hom(D^{1\times r_i}, F) & \xleftarrow{(.R_i)^*} & \hom(D^{1\times r_{i-1}}, F) \\ \Big\downarrow{\scriptstyle \theta_i} & & \Big\uparrow{\scriptstyle \theta_{i-1}^{-1}} \\ F^{r_i\times 1} & \xleftarrow{g_i} & F^{r_{i-1}\times 1} \end{array}$$

Así pois, tomamos $\zeta \in F^{r_{i-1}\times 1}$ calquera e esiximos que se cumpra a anterior condición, isto é, $g_i(\zeta) = \left(\theta_i \circ (.R_i)^* \circ \theta_{i-1}^{-1}\right)(\zeta)$. Notemos que $\theta_{i-1}^{-1}(\zeta) \in \hom(D^{1\times r_{i-1}}, F)$, e empregando a definición de $(.R_i)^*$, $(.R_i)^*(\theta_{i-1}^{-1}(\zeta)) = \theta_{i-1}^{-1}(\zeta) \circ .R_i \in \hom(D^{1\times r_i}, F)$. Agora ben, utilizando isto último e a definición do isomorfismo θ_i dada en (3.11):

$$\left(\theta_i \circ (.R_i)^* \circ \theta_{i-1}^{-1}\right)(\zeta) = \theta_i\left(\theta_{i-1}^{-1}(\zeta) \circ .R_i\right) = \left(\theta_{i-1}^{-1}(\zeta)(f_1R_i), \ldots, \theta_{i-1}^{-1}(\zeta)(f_{r_i}R_i)\right)^T. \quad (3.12)$$

Introduzamos agora o isomorfismo inverso θ_{i-1}^{-1},

$$\begin{array}{rcl} \theta_{i-1}^{-1} : F^{r_{i-1}\times 1} & \longrightarrow & \hom(D^{1\times r_{i-1}}, F) \\ \zeta & \longmapsto & \theta_{i-1}^{-1}(\zeta) = \psi_\zeta : \quad \begin{array}{rcl} D^{1\times r_{i-1}} & \longrightarrow & F \\ \lambda & \longmapsto & \psi_\zeta(\lambda)) = \lambda\zeta = \lambda_1\zeta_1 + \ldots + \lambda_{r_{i-1}}\zeta_{r_{i-1}}. \end{array} \end{array}$$

A comprobación de que θ_{i-1}^{-1} é, en efecto, a aplicación inversa de θ_{i-1} é totalmente análoga á que realizamos na demostración do Teorema 2.20 para o isomorfismo de Malgrange. Así pois, para calquera $j \in \{1, \ldots, r_i\}$, como $R_i \in D^{r_i\times r_{i-1}}$ tense que $f_jR_i \in D^{1\times r_{i-1}}$, logo

$$\theta_{i-1}^{-1}(\zeta)(f_jR_i) = (f_jR_i)\zeta = R_{i_{j*}}\zeta.$$

Na derradeira igualdade empregamos que $\{f_1, \ldots, f_{r_i}\}$ é a base canónica de $D^{1\times r_i}$, e daquela ao multiplicar pola esquerda a matriz $R_i \in D^{r_i\times r_{i-1}}$ por f_j obtemos a fila j de R_i, que denotamos por $R_{i_{j*}}$. Finalmente, empregando isto último na ecuación (3.12) e utilizando o produto de matrices usual podemos escribir:

$$\left(\theta_i \circ (.R_i)^* \circ \theta_{i-1}^{-1}\right)(\zeta) = \left(R_{i_{1*}}\zeta, \ldots, R_{i_{r_i*}}\zeta\right) = R_i\zeta = (R_i.)\zeta.$$

Como $\zeta \in F^{r_{i-1}\times 1}$ foi escollido arbitrariamente, concluímos que $g_i = R_i.$, sendo $R_i.$ o homomorfismo de grupos que leva cada $\zeta \in F^{r_{i-1}\times 1}$ en $R_i\zeta \in F^{r_i\times 1}$. Así podemos empregar o seguinte cocomplexo asociado á resolución libre e finita de M dada en (3.6):

$$\ldots \xleftarrow{R_4\cdot} F^{r_3\times 1} \xleftarrow{R_3\cdot} F^{r_2\times 1} \xleftarrow{R_2\cdot} F^{r_1\times 1} \xleftarrow{R_1\cdot} F^{r_0\times 1} \longleftarrow 0. \tag{3.13}$$

Notemos que aparece aquí o cocomplexo (3.7) que saía de forma natural ao estudar as condicións de compatibilidade do sistema $R_1\eta = \zeta$, para $\zeta \in F^{r_0\times 1}$ fixado. Todo isto permite simplificar tamén a definición dos grupos abelianos $\mathrm{ext}^i_D(M,F)$:

$$\begin{cases} \mathrm{ext}^0_D(M,F) = \ker(R_1.) \\ \mathrm{ext}^i_D(M,F) = \ker(R_{i+1}.)/\mathrm{Im}(R_i.),\ i \geq 1. \end{cases}$$

Para o caso dun D-módulo pola dereita M podemos demostrar un resultado similar, e simplificar tamén a definición dos grupos abelianos $\mathrm{ext}^i_D(M,F)$:

$$\begin{cases} \mathrm{ext}^0_D(M,F) = \ker(.S_1) \\ \mathrm{ext}^i_D(M,F) = \ker(.S_{i+1})/\mathrm{Im}(.S_i),\ i \geq 1. \end{cases}$$

Como exemplo de aplicación da teoría exposta imos traballar cun caso moi sinxelo: o do D-módulo pola esquerda finitamente presentado polo operador gradiente en $\mathbb{R}^3$, onde D é o anel de operadores diferenciais $\mathbb{R}[\partial_1,\partial_2,\partial_3]$.

Exemplo 3.28. Sexa $D = \mathbb{R}[\partial_1,\partial_2,\partial_3]$, e consideremos o sistema linear $R\eta = 0$, onde R é o operador diverxencia en $\mathbb{R}^3$, $R = (\partial_1\ \partial_2\ \partial_3)$. No vindeiro capítulo veremos que os grupos abelianos das extensións relevantes de cara a caracterizar as propiedades do D-módulo pola esquerda finitamente presentado por R son $\mathrm{ext}^i_D(N,D)$, onde N é, neste caso particular, o D-módulo pola esquerda $N = D/(D^{1\times 3}R^T)$.

Calcularemos entón, a modo de exemplo, os grupos abelianos $\mathrm{ext}^i_D(N,D)$ para $0 \leq i \leq 3$. En primeiro lugar notemos que $R^T = (\partial_1\ \partial_2\ \partial_3)^T$, que coincide coa matriz R_1 do sistema do Exemplo 3.20. Sabemos entón que a seguinte é unha resolución libre e finita para N:

$$0 \longrightarrow D \xrightarrow{.R_3} D^{1\times 3} \xrightarrow{.R_2} D^{1\times 3} \xrightarrow{.R_1} D \xrightarrow{\kappa} N \longrightarrow 0,$$

con R_2 e R_3 as matrices calculadas no Exemplo 3.20:

$$R_2 = \begin{pmatrix} 0 & -\partial_3 & \partial_2 \\ \partial_3 & 0 & -\partial_1 \\ -\partial_2 & \partial_1 & 0 \end{pmatrix} \in D^{3\times 3}, \quad R_3 = R_1^T \in D^{1\times 3}.$$

Os D-módulos $\mathrm{ext}^i_D(N,D)$ son entón os defectos de exactitude do seguinte cocomplexo de grupos abelianos:

$$0 \longleftarrow D \xleftarrow{R_3\cdot} D^{3\times 1} \xleftarrow{R_2\cdot} D^{3\times 1}.$$

Notemos que neste caso particular o anterior é tamén un cocomplexo de D-módulos pola dereita, pois os homomorfimos $R_i.$ son homomorfismos de D-módulos pola dereita para $i = 1,2,3$. Daquela os grupos abelianos $\mathrm{ext}^i_D(N,D)$ pódense dotar de estrutura de D-módulo pola dereita. Pasamos a calcular os grupos abelianos $\mathrm{ext}^i_D(N,D)$ aplicando a definición:

- $\text{ext}^0_D(N,D) = \ker(R_1.)$.
  Notemos que $R_1.(d) = R_1 d = (\partial_1 d, \partial_2 d, \partial_3 d)^T \in D^{3\times 1}$, e isto para calquera $d \in D$. Xa que D é, neste caso, un anel conmutativo, resulta que $R_1.(d) = (d\partial_1, d\partial_2, d\partial_3) \in D^{3\times 1}$. Pero, para $i = 1,2,3$, por ser D un dominio e $\partial_i \neq 0$, obtemos que $d\partial_i = 0$ se e só se $d = 0$. Entón $\ker(R_1.) = 0 = \text{ext}^0_D(N,D)$.

- $\text{ext}^1_D(N,D) = \ker(R_2.)/\text{Im}(R_1.)$.
  Para $\lambda \in D^{3\times 1}$ calquera, resulta que $\lambda \in \ker(R_2.)$ se e só se $R_2\lambda = 0$. Operando co produto de matrices usual, $R_2\lambda = 0 \in D^{3\times 1}$ equivale a $(R_2\lambda)^T = \lambda^T R_2^T = 0 \in D^{1\times 3}$. Pero $R_2^T = -R_2$, logo $R_2\lambda = 0 \in D^{3\times 1}$ é equivalente a $\lambda^T R_2 = (.R_2)(\lambda^T) = 0 \in D^{1\times 3}$. Por definición, a resolución libre e finita de N é exacta en $D^{1\times 3}$, de maneira que $\ker(.R_2) = DR_3$. Finalmente, xa que $\lambda \in \ker(R_2.)$ se e só se $\lambda^T \in \ker(.R_2)$, concluímos que $\ker(R_2.) = R_3^T D = R_1 D = \text{Im}(R_1.)$. Entón $\text{ext}^1_D(N,D) = 0$.

- $\text{ext}^2_D(N,D) = \ker(R_3.)/\text{Im}(R_2.)$.
  Razoando como no caso anterior, $(R_3.)(\lambda) = 0$ equivale a $(.R_3^T)(\lambda^T) = (.R_1)(\lambda^T) = 0$. Por outro lado, $\ker(.R_1) = D^{1\times 3}R_2$, onde empregamos a exactitude en $D^{1\times 3}$ da resolución libre e finita de N. Deste xeito $\ker(R_3.) = R_2^T D^{1\times 3} = -R_2 D^{1\times 3} = R_2 D^{1\times 3} = \text{Im}(R_2.)$, de xeito que $\text{ext}^2_D(N,D) = 0$. Debemos notar que na penúltima igualdade utilizamos que $-R_2 D^{1\times 3}$ é un D-submódulo pola esquerda de $D^{1\times 3}$, e como $-1 \in D$, $(-1)(-1) = 1$, podemos multiplicar por (-1) pola esquerda e obter o mesmo submódulo.

- $\text{ext}^3_D(N,D) = \ker(D \to 0)/\text{Im}(R_3.)$.
  Xa que o rango de $R_3.$ é o propio anel D, $\text{Im}(R_3.) = R_3 D^{3\times 1} = D^{1\times 3} R_3^T = D^{1\times 3} R_1$. Doutra banda, o núcleo do homomorfismo $D \longrightarrow 0$ é necesariamente D. Así, concluímos que $\text{ext}^3_D(N,D) = D/(D^{1\times 3}R_1) = N$.

Finalmente, imos utilizar o cocomplexo de grupos abelianos asociado á resolución libre e finita de M para o D-módulo pola esquerda $F = \mathscr{C}^\infty(\mathbb{R})$:

$$0 \longleftarrow F \xleftarrow{R_3\cdot} F^{3\times 1} \xleftarrow{R_2\cdot} F^{3\times 1}.$$

Recordando que R_1, R_2 e R_3 representan, respectivamente, os operadores gradiente, rotacional e diverxencia en $\mathbb{R}^3$, temos aquí a coñecida *sucesión gradiente-rotacional-diverxencia*, que é outra forma de expresar o tamén coñecido *Lema de Poincaré*. Disto obtemos a seguinte importante información:

- Por $R_2.\circ R_1. = 0$ temos que o rotacional de calquera campo vectorial que é o gradiente dun campo escalar é cero.

- Por $R_3.\circ R_2. = 0$ temos que a diverxencia de calquera campo vectorial que é o rotacional doutro campo vectorial é cero.

Notemos que en ambos casos estamos utilizando simplemente que se trata dun cocomplexo de grupos abelianos, e polo tanto a composición de homomorfismos consecutivos é o homomorfismo nulo.

4. Estudo das propiedades do módulo dun sistema linear

No anterior capítulo introducimos unha serie de conceptos e ferramentas que nos permitiron deducir que, supoñendo $R \in D^{q\times p}$ e D un anel noetheriano pola esquerda, o D-módulo do sistema $R\eta = 0$ admite unha resolución libre e finita. Ademais, se D é unha álxebra de Ore nas condicións moi xerais de (3.1), esta resolución podémola calcular mediante o Algoritmo 3.17, que utiliza as técnicas das bases de Gröbner. Finalmente, tamén vimos que existe un cocomplexo de grupos abelianos asociado a toda resolución libre e finita dun D-módulo pola esquerda, e que neste contexto podemos definir os grupos abelianos $\text{ext}^i_D(M,F)$. Todo isto conseguímolo acudindo ás ferramentas e aos conceptos da Álxebra Homolóxica, o que fixo que nos afastásemos momentaneamente do noso principal propósito: caracterizar as propiedades das solucións do sistema linear $R\eta = 0$ estudando o D-módulo do sistema.

Pretendemos agora emprender o camiño de volta para acadar o devandito propósito. Para iso presentaremos, en primeiro lugar, unha serie de resultados que farán explícita a relevancia dos grupos abelianos das extensións á hora de estudar o D-módulo do sistema. A continuación trataremos de entender unha serie de algoritmos que fan efectivos os anteriores resultados de cara a caracterizar as propiedades do D-módulo do sistema. O seguinte será introducir o concepto de parametrización, que ten xa unha interpretación moi clara no estudo de sistemas lineares, pero que á vez está intimamente ligado ás propiedades do D-módulo do sistema. Finalmente introduciremos unha serie de ideas propias da Teoría do Control e veremos a relación que teñen coas propiedades do D-módulo do sistema tratadas ao longo do capítulo. Todo este proceso irémolo exemplificando paso a paso mediante casos sinxelos e de gran interese nas áreas da Física ou das Matemáticas.

4.1. Os grupos abelianos das extensións e o módulo dun sistema linear

Nesta sección veremos a utilidade dos grupos abelianos das extensións no marco da Análise Alxébrica. Para iso presentaremos unha serie de resultados en condicións algo máis restritivas que aquelas coas que vimos traballando ao longo do documento. Con esta simplificación a teoría que presentamos segue a ser válida para a maior parte de casos que nos interesan (isto trataremos de exemplificalo) e ao mesmo tempo permítenos empregar resultados concretos de Álxebra Homolóxica probados en [1, 2].

Con todo, cómpre mencionar que en [3] realízase un tratamento máis xeral. Este esixe introducir conceptos e resultados adicionais da Teoría de Módulos e da Álxebra Homolóxica, xunto con algoritmos que o fan efectivo. Todo isto excede os propósitos que pretendemos acadar, de aí que decidamos limitarnos a unha versión simplificada.

Así pois, imos restrinxir a nosa análise ao caso de aneis de operadores diferenciais conmutativos sobre un corpo K, $K[\partial_1,\dots,\partial_n]$. Sabemos que estes aneis son dominios e aneis noetherianos pola esquerda, en virtude do Teorema 2.27. Como ademais son conmutativos, resulta que os aneis $K[\partial_1,\dots,\partial_n]$ son *dominios noetherianos*. Temos entón o seguinte resultado, que se pode consultar en [1,2], debido a Auslander.

Proposición 4.1. *Sexa D un dominio noetheriano e M un D-módulo pola esquerda finitamente xerado. Sexa tamén*

$$P_1 \xrightarrow{d_1} P_0 \longrightarrow M \longrightarrow 0$$

unha sucesión exacta, onde P_1, P_0 son D-módulos proxectivos. Consideremos o cocomplexo de grupos abelianos asociado,

$$\hom(P_1,D) \xleftarrow{(d_1)^*} \hom(P_0,D) \longleftarrow 0,$$

e denotemos por N o conúcleo do homomorfismo de grupos $(d_1)^*$, que se pode dotar de estrutura de D-módulo pola dereita. Entón tense a seguinte sucesión exacta de grupos abelianos:

$$0 \longrightarrow \operatorname{ext}^1_D(N,D) \longrightarrow M \xrightarrow{\varepsilon} \hom(\hom(M,D),D) \longrightarrow \operatorname{ext}^2_D(N,D) \longrightarrow 0,$$

onde $\varepsilon\colon M \longrightarrow \hom(\hom(M,D),D)$ é o homomorfismo canónico da Definición 2.28.

Utilizando a anterior proposición podemos probar os seguintes dous resultados, que nos dan xa información sobre o D-módulo do sistema empregando os grupos abelianos das extensións introducidos no anterior capítulo.

Teorema 4.2. *Sexa D un dominio noetheriano e consideremos o sistema linear $R\eta = 0$, con $R \in D^{q\times p}$ unha matriz. Consideremos o D-módulo pola esquerda finitamente presentado por R, $M = D^{1\times p}/(D^{1\times q}R)$ e o D-módulo pola dereita $N = D^{p\times 1}/(RD^{q\times 1})$.*

(1) Tense a seguinte sucesión exacta de D-módulos pola esquerda:

$$0 \longrightarrow \operatorname{ext}^1_D(N,D) \longrightarrow M \xrightarrow{\varepsilon} \hom(\hom(M,D),D) \longrightarrow \operatorname{ext}^2_D(N,D) \longrightarrow 0, \qquad (4.1)$$

onde o homomorfismo de D-módulos pola esquerda ε é o homomorfismo canónico da Definición 2.28.

(2) M é reflexivo se e só se $\operatorname{ext}^i_D(N,D) = 0$ para $i = 1,2$.

(3) Se $\operatorname{ext}^1_D(N,D) = 0$ entón M é un D-módulo pola esquerda libre de torsión.

Demostración. Comezamos por (1). Tomamos a sucesión exacta obtida a partir da presentación libre de M, $\pi\colon D^{1\times p} \longrightarrow D^{1\times p}/(D^{1\times q}R)$:

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

Os D-módulos $D^{1\times p}$, $D^{1\times q}$ son libres, e daquela tamén son proxectivos, co que podemos aplicar a Proposición 4.1. Tomamos entón o cocomplexo de grupos abelianos do enunciado do devandito resultado:

$$\hom(D^{1\times q},D) \xleftarrow{(.R)^*} \hom(D^{1\times p},D) \longleftarrow 0.$$

Xa que D é tamén un D-módulo pola esquerda, empregando o resultado derivado na Observación 3.27 podemos substituír o anterior cocomplexo polo seguinte:

$$D^{q\times 1} \xleftarrow{R.} D^{p\times 1} \longleftarrow 0.$$

Sexa agora $N = D^{q\times 1}/(\mathrm{Im}(R.)) = D^{q\times 1}/(RD^{p\times 1})$. A Proposición 4.1 dá xa o enunciado de (1). Notemos que neste caso particular está claro que N ten estrutura de D-módulo pola dereita, pois $D^{q\times 1}$ e $D^{p\times 1}$ son D-módulos pola dereita e a aplicación $R.$ é un homomorfismo de D-módulos pola dereita, en virtude da Observación 3.13.

Vaiamos agora con (2). Supoñamos en primeiro lugar que M é reflexivo, isto é, que o homomorfismo canónico ε é un isomorfismo, segundo a Definición 2.28. Así pois, resulta que o homomorfismo ε é sobrexectivo e inxectivo. Razoamos coa sucesión exacta (4.1).

Notemos que $\ker(\mathrm{ext}^1_D(N,D) \to M) = \mathrm{Im}(0 \to \mathrm{ext}^1_D(N,D)) = 0$, onde utilizamos que a sucesión é exacta en $\mathrm{ext}^1_D(N,D)$. Tamén é exacta en M, logo $\ker(\varepsilon) = \mathrm{Im}(\mathrm{ext}^1_D(N,D) \to M)$. Xa que ε é inxectivo, temos que $\ker(\varepsilon) = 0$, e así o homomorfismo $\mathrm{ext}^1_D(N,D) \to M$ é tal que a súa imaxe e núcleo son ambos 0, logo necesariamente $\mathrm{ext}^1_D(N,D) = 0$.

Por outro lado, $\ker(\hom(\hom(M,D),D) \to \mathrm{ext}^2_D(N,D)) = \mathrm{Im}(\varepsilon) = \hom(\hom(M,D),D)$, onde empregamos que a sucesión é exacta en $\hom(\hom(M,D),D)$ e que ε é sobrexectivo. Disto séguese que $\mathrm{Im}(\hom(\hom(M,D),D) \to \mathrm{ext}^2_D(N,D)) = 0$, por ser o núcleo do homomorfismo igual ao dominio. Utilizando isto último e que a sucesión é exacta en $\mathrm{ext}^2_D(N,D)$, $0 = \ker(\mathrm{ext}^2_D(N,D) \to 0)$, pero o anterior núcleo coincide co dominio por tratarse do homomorfismo que leva todo elemento ao 0. Así, $\mathrm{ext}^2_D(N,D) = 0$.

Reciprocamente, se $\mathrm{ext}^i_D(N,D) = 0$, $i = 1,2$, entón tense a seguinte sucesión exacta:

$$0 \longrightarrow M \xrightarrow{\varepsilon} \hom(\hom(M,D),D) \longrightarrow 0.$$

Por ser exacta en M, $\ker(\varepsilon) = \mathrm{Im}(0 \longrightarrow M) = 0$, e por ser exacta en $\hom(\hom(M,D),D)$, $\hom(\hom(M,D),D) = \ker(\hom(\hom(M,D),D) \to 0) = \mathrm{Im}(\varepsilon)$. Daquela o homomorfismo canónico ε é sobrexectivo e inxectivo, isto é, é un isomorfismo, e polo tanto M é reflexivo.

Finalmente, probemos (3). Supoñamos $\mathrm{ext}^1_D(N,D) = 0$. Temos entón a seguinte sucesión exacta curta:

$$0 \longrightarrow M \xrightarrow{\varepsilon} \hom(\hom(M,D),D) \longrightarrow \mathrm{ext}^2_D(N,D) \longrightarrow 0.$$

Sabemos que nestas circunstancias ε é inxectivo. Tomemos agora $m \in M$ e $d \in D \setminus \{0\}$ arbitrarios, e supoñamos que $dm = 0$. Resulta que para calquera homomorfismo $f \in \hom(M,D)$, $f(dm) = f(0) = 0$, pero por outra parte $f(dm) = df(m)$, logo $df(m) = 0$. Xa que D é un dominio e $d \neq 0$, necesariamente $f(m) = 0$. Pero entón $\varepsilon(m) = 0$, atendendo á definición de ε, e por ser este un homomorfismo inxectivo, $m = 0$. Isto demostra que se m é un elemento de torsión, entón $m = 0$, isto é, $t(M) = 0$. ■

Observación 4.3. A afirmación (3) do Teorema 4.2 é, en realidade, unha equivalencia, pero non incluímos a proba aquí por requerir esta de ferramentas de Álxebra Homolóxica máis avanzadas e, polo tanto, exceder os obxectivos deste traballo. Con todo, indicamos que a demostración pode ser consultada en [3].

Finalmente, damos a seguinte caracterización dun D-módulo pola esquerda proxectivo. De novo, a demostración require de ferramentas de Álxebra Homolóxica e Teoría de Módulos máis avanzadas que as que vimos empregando ao longo do documento, logo tamén a

omitimos. Pódese consultar en [2], onde se dá tamén un enunciado máis xeral, que fai uso do concepto de *dimensión proxectiva* dun D-módulo pola esquerda.

Teorema 4.4. *Sexa $D = K[\partial_1, \ldots, \partial_n]$ un anel de operadores diferenciais sobre un corpo K, $R \in D^{q\times p}$ unha matriz e $M = D^{1\times p}/(D^{1\times q}R)$ o D-módulo pola esquerda finitamente presentado por R. Consideremos tamén o D-módulo pola dereita $N = D^{q\times 1}/(RD^{p\times 1})$. Entón M é un D-módulo pola esquerda proxectivo se e só se* $\operatorname{ext}^i_D(N, D) = 0$, $i = 1, \ldots, n$.

Os Teoremas 4.2 e 4.4 amosan que certas propiedades do D-módulo pola esquerda finitamente presentado M están caracterizadas polos grupos abelianos $\operatorname{ext}^i_D(N, D)$, de aí a relevancia deste concepto no marco da Análise Alxébrica. O D-módulo pola dereita $N = D^{q\times 1}/(RD^{p\times 1})$ recibe un nome especial, pola súa importancia histórica.

Definición 4.5. Sexa D un dominio noetheriano e consideremos o D-módulo pola esquerda finitamente presentado pola matriz $R \in D^{q\times p}$. O D-módulo pola dereita $N = D^{q\times 1}/(RD^{p\times 1})$ chámase a *trasposta de Auslander de M*.

Observación 4.6. Cando D é un anel conmutativo, $N = D^{q\times 1}/(RD^{p\times 1}) \simeq D^{1\times q}/(D^{1\times p}R^T)$, onde R^T denota a *matriz trasposta de R*, obtida cambiando as súas filas polas súas columnas. En efecto, para $x, y \in D^{q\times 1}$ calquera:

$$\begin{aligned} x + RD^{p\times 1} = y + RD^{p\times 1} &\iff y - x \in RD^{p\times 1} \iff y^T - x^T \in D^{1\times p}R^T \\ &\iff x^T + D^{1\times p}R^T = y^T + D^{1\times p}R^T \end{aligned}$$

e como $x \in D^{p\times 1} \iff x^T \in D^{1\times p}$, as relacións de equivalencia que definen os módulos cociente $D^{q\times 1}/(RD^{p\times 1})$ e $D^{1\times q}/(D^{1\times p}R^T)$ son a mesma, de aí o isomorfismo (de grupos abelianos). Deste xeito a trasposta de Auslander pode ser dotada tamén de estrutura de D-módulo pola esquerda.

Presentamos agora un algoritmo que permite calcular o grupo abeliano $\operatorname{ext}^1_D(N, D)$, con N a trasposta de Auslander do módulo do sistema, nas condicións simplificadas nas que estamos a traballar. Veremos que é fundamental o Algoritmo 3.17 que calcula os módulos de sicixia empregando técnicas de bases de Gröbner.

Algoritmo 4.7

Entrada: *Un anel conmutativo de operadores diferenciais $D = K[\partial_1, \ldots, \partial_n]$, con K un corpo, e unha matriz $R \in D^{q\times p}$.*

Dúas matrices $R' \in D^{q'\times p}$ e $P \in D^{p\times m}$ tales que:

Saída: $$\operatorname{ext}^1_D(N, D) = (D^{1\times q'}R')/(D^{1\times q}R),\ \ker(.P) = D^{1\times q'}R',$$

onde $N = D^{q\times 1}/(RD^{p\times 1})$ é a trasposta de Auslander de $M = D^{1\times p}/(D^{1\times q}R)$.

(1) Calculamos a matriz trasposta de R, $R^T \in D^{p\times q}$.

(2) Utilizando o Algoritmo 3.17, calculamos $Q \in D^{m\times p}$ tal que $\ker(.R^T) = D^{1\times m}Q$.

(3) Definimos $P = Q^T$, $P \in D^{p\times m}$.

(4) Utilizando o Algoritmo 3.17, calculamos $R' \in D^{q'\times p}$ tal que $\ker(.P) = D^{1\times q'}R'$.

Observación 4.8. Vexamos agora por que o anterior algoritmo é efectivo á hora de calcular $\text{ext}^1_D(N,D)$. En primeiro lugar, notemos que por ser D un anel conmutativo, podemos identificar a trasposta de Auslander de $M = D^{1\times p}/(D^{1\times q}R)$ con $N = D^{1\times q}/(D^{1\times p}R^T)$. Tomemos o seguinte comezo dunha resolución libre e finita de N:

$$D^{1\times m} \xrightarrow{.Q} D^{1\times p} \xrightarrow{.R^T} D^{1\times q} \xrightarrow{\overline{\pi}} N \longrightarrow 0,$$

onde $\overline{\pi}$ é a proxección canónica en $N = D^{1\times q}/(D^{1\times p}R^T)$. O cálculo da matriz $Q \in D^{m\times p}$ que define o homomorfismo $.Q\colon D^{1\times m} \longrightarrow D^{1\times p}$ faise co Algoritmo 3.17, como xa indicamos. Tomando o cocomplexo de grupos abelianos asociado (que neste caso é tamén un cocomplexo de D-módulos pola dereita, en virtude da Observación 3.13):

$$D^{m\times 1} \xleftarrow{Q.} D^{p\times 1} \xleftarrow{R^T.} D^{q\times 1} \longleftarrow 0,$$

o grupo abeliano $\text{ext}^1_D(N,D)$ é $\ker(Q.)/\text{Im}(R^T.)$. Definindo $P = Q^T$, debemos observar que os homomorfismos $.P\colon D^{1\times p} \longrightarrow D^{1\times m}$ e $Q.\colon D^{p\times 1} \longrightarrow D^{m\times 1}$ son tales que $(.P)(x) = xP = xQ^T = 0$ é equivalente a $(xQ^T)^T = Qx^T = (Q.)(x^T) = 0$, $x \in D^{1\times p}$. Empregando o Algoritmo 3.17 podemos calcular $R' \in D^{q'\times p}$ tal que $\ker(.P) = D^{1\times q'}R'$, logo $\ker(Q.) = (D^{1\times q'}R')^T$, atendendo ao anterior. Deste xeito, $\text{ext}^1_D(N,D) = (D^{1\times q'}R')^T/(R^TD^{q\times 1})$. Repetindo o razoamento realizado na Observación 4.6 deducimos que os conxuntos cociente $(D^{1\times q'}R')^T/(R^TD^{q\times 1})$ e $D^{1\times q'}R'/(D^{1\times q}R)$ son isomorfos, logo $\text{ext}^1_D(N,D) = (D^{1\times q'}R')/(D^{1\times q}R)$.

O Algoritmo 4.7 pódese xeneralizar para que permita calcular os grupos abelianos das extensións de orde superior, $\text{ext}^i_D(N,D)$. A continuación damos as ideas básicas da devandita xeneralización.

(1) Tomemos o inicio dunha resolución libre e finita do D-módulo do pola esquerda $N = D^{1\times q}/(D^{1\times p}R^T)$,

$$D^{1\times p} \xrightarrow{.R^T} D^{1\times q} \xrightarrow{\kappa} N \longrightarrow 0,$$

onde κ é a proxección canónica en N. Definamos $q_0 = q$, $q_1 = p$, $S_1 = R^T$. A partir do Algoritmo 3.17 podemos completar a anterior sucesión exacta a unha resolución libre e finita de N:

$$\ldots D^{1\times q_2} \xrightarrow{.S_2} D^{1\times q_1} \xrightarrow{.S_1} D^{1\times q_0} \xrightarrow{\kappa} N \longrightarrow 0.$$

(2) A partir desta podemos definir o seguinte cocomplexo de D-módulos pola esquerda:

$$\ldots D^{1\times q_2} \xleftarrow{.S_2^T} D^{1\times q_1} \xleftarrow{.S_1^T} D^{1\times q_0} \longleftarrow 0.$$

(3) Empregando o Algoritmo 3.17 calculamos $R'_i \in D^{q'_{i-1}\times q_i}$ tal que $\ker(.S_{i+1}^T) = D^{1\times q'_{i-1}}R'_i$.

(4) Concluímos que $\text{ext}^i_D(N,D) = (D^{1\times q'_{i-1}}R'_i)/(D^{1\times q_{i-1}}S_i^T)$.

Temos entón algoritmos que fan aplicables, desde un punto de vista práctico, as ideas dos Teoremas 4.2 e 4.4. Xa mencionamos que estes resultados son válidos en condicións máis xerais que aquelas nas que os enunciamos. De forma análoga, estes algoritmos xeneralízanse a sistemas lineares sobre aneis máis xerais, como se indica en [17], o que amosa que as ideas da Análise Alxébrica resultan efectivas nun amplo abano de situacións. Con todo,

para comprender o funcionamento do algoritmo nesas circunstancias cómpre traballar con conceptos como a *involución dunha matriz e dun anel* ou a *adxunta formal dunha matriz*, e todo isto faino menos intuitivo.

Presentamos agora un par de exemplos que permiten aplicar os Teoremas 4.2 e 4.4 empregando as ideas do Algoritmo 4.7 e da Observación 4.8 sen necesidade de acudir ao Algoritmo 3.17 para empregar as técnicas de bases de Gröbner. Ademais de ilustrar a teoría exposta, trátase de casos de gran interese e relevancia na Física e nas Matemáticas.

Exemplo 4.9. Consideremos o sistema linear do Exemplo 3.28, isto é, o definido pola matriz $R = (\partial_1 \ \partial_2 \ \partial_3) \in D$, con $D = \mathbb{R}[\partial_1, \partial_2, \partial_3]$, que representa o operador diverxencia en $\mathbb{R}^3$. O D-módulo do sistema é entón $M = D^{1\times 3}/(DR)$. Imos estudar as propiedades de M empregando os resultados dos Teoremas 4.2 e 4.4.

En primeiro lugar, xa que D é un anel conmutativo, a trasposta de Auslander é simplemente $N = D/(D^{1\times 3}R^T)$. No Exemplo 3.28 xa calculamos os grupos abelianos $\mathrm{ext}^i_D(N, D)$ para $i = 0, 1, 2, 3$, obtendo os seguintes resultados:

$$\mathrm{ext}^i_D(N, D) = 0, \text{ para } i = 0, 1, 2, \ \mathrm{ext}^3_D(N, D) = N.$$

Utilizando o Teorema 4.2 vemos que o D-módulo pola esquerda do sistema, M, é libre de torsión (pois $\mathrm{ext}^1_D(N, D) = 0$) e tamén reflexivo (pois $\mathrm{ext}^1_D(N, D) = 0$, $\mathrm{ext}^2_D(N, D) = 0$). Empregando o Teorema 4.4, como $n = 3$ e $\mathrm{ext}^3_D(N, D) = N \neq 0$ concluímos que M non é un D-módulo pola esquerda proxectivo.

Exemplo 4.10. Traballaremos agora cun exemplo algo máis complicado, pero de gran interese na Física, por tratarse das ecuacións básicas do Electromagnetismo clásico: as *ecuacións de Maxwell*. Empregaremos a notación introducida no Exemplo 3.20 para o gradiente, o rotacional e a diverxencia en $\mathbb{R}^3$, e denotaremos a derivada temporal por $\partial/\partial t = \partial_t$. Se $\vec{B}$ e $\vec{E}$ denotan os campos magnético e eléctrico, respectivamente, as ecuacións de Maxwell no baleiro (ver, por exemplo, [10]) escríbense como segue:

$$\begin{cases} \partial_t \vec{E} - \vec{\nabla} \times \vec{B} = \vec{0}, \\ \partial_t \vec{B} + \vec{\nabla} \times \vec{E} = \vec{0}, \\ \vec{\nabla} \cdot \vec{E} = 0, \\ \vec{\nabla} \cdot \vec{B} = 0. \end{cases} \tag{4.2}$$

Estas ecuacións representan matematicamente leis físicas obtidas de forma independente. Sen introducir leis adicionais, como a conservación da carga, ou condicións iniciais non podemos obter ningunha destas ecuacións en función das outras, tal e como se discute en [25]. Notemos que (4.2) é en realidade un sistema de oito ecuacións nas incógnitas $B_1, B_2, B_3, E_1, E_2, E_3$. Engadamos agora termos non homoxéneos no lado dereito:

$$\begin{cases} \partial_t \vec{E} - \vec{\nabla} \times \vec{B} = -\vec{J}_e, \\ \partial_t \vec{B} + \vec{\nabla} \times \vec{E} = \vec{J}_m, \\ \vec{\nabla} \cdot \vec{E} = \rho_e, \\ \vec{\nabla} \cdot \vec{B} = \rho_m. \end{cases} \tag{4.3}$$

Nas anteriores ecuacións $\vec{J}_e$ e $\vec{J}_m$ representan as densidades de corrente eléctrica e magnética, mentres que ρ_e e ρ_m representan as densidades de carga eléctrica e magnética. As ecuacións de Maxwell con fontes correspóndense coas anteriores tomando $\vec{J}_m = 0$ e $\rho_m = 0$, pois ata o momento non se demostrou a existencia de monopolos magnéticos, aínda que teña sentido desde o punto de vista matemático.

Como se indica en [10], as ecuacións (4.3) poden ser utilizadas para derivar as ecuacións de continuidade para $\vec{J}_e$, $\vec{J}_m$, ρ_e e ρ_m. Aplicando o operador diverxencia na primeira das ecuacións, obtemos que:

$$\vec{\nabla} \cdot \partial_t \vec{E} - \vec{\nabla} \cdot \vec{\nabla} \times \vec{B} = \vec{\nabla} \cdot (-\vec{J}_e).$$

Lembremos agora que, segundo vimos no Exemplo 3.28, a diverxencia de calquera campo vectorial que é o rotacional doutro campo vectorial é nula. Ademais, a diverxencia conmuta coa derivada temporal, de maneira que a anterior ecuación escríbese como:

$$\partial_t \vec{\nabla} \cdot \vec{E} + \vec{\nabla} \cdot \vec{J}_e = 0,$$

e finalmente, como $\vec{\nabla} \cdot \vec{E} = \rho_e$, recuperamos a ecuación de continuidade:

$$\partial_t \rho_e + \vec{\nabla} \cdot \vec{J}_e = 0. \tag{4.4}$$

Para $\vec{J}_m$, ρ_m tense unha ecuación análoga:

$$\partial_t \rho_m + \vec{\nabla} \cdot \vec{J}_m = 0. \tag{4.5}$$

En [8] próbase que (4.4) e (4.5) son exactamente as condicións de compatibilidade do sistema (4.3). Debemos observar que cada par de ecuacións do devandito sistema dá lugar a unha das condicións de compatibilidade.

A información exposta vainos ser útil de cara a aplicar os resultados dos Teoremas 4.2 e 4.4 a dúas das ecuacións de Maxwell de (4.2), a *lei de Maxwell-Faraday* e a *lei de Gauss para o magnetismo*, isto é, a segunda e a cuarta ecuacións de (4.2):

$$\begin{cases} \partial_t \vec{B} + \vec{\nabla} \times \vec{E} = \overrightarrow{0}, \\ \vec{\nabla} \cdot \vec{B} = 0. \end{cases} \tag{4.6}$$

Para aplicar os devanditos resultados debemos escoller un anel de operadores diferenciais que permita representar as anteriores ecuacións como un sistema linear. Para iso tomamos o anel conmutativo $D = \mathbb{R}[\partial_t, \partial_1, \partial_2, \partial_3]$. Recordando as expresións matriciais en $\mathbb{R}[\partial_1, \partial_2, \partial_3]$ do rotacional e da diverxencia que introducimos no Exemplo 3.20, é fácil ver que as ecuacións (4.6) pódense escribir como o seguinte sistema linear

$$R\eta = \begin{pmatrix} \partial_t & 0 & 0 & 0 & -\partial_3 & \partial_2 \\ 0 & \partial_t & 0 & \partial_3 & 0 & -\partial_1 \\ 0 & 0 & \partial_t & -\partial_2 & \partial_1 & 0 \\ \partial_1 & \partial_2 & \partial_3 & 0 & 0 & 0 \end{pmatrix} \eta = 0, \tag{4.7}$$

con R unha matriz 4×6 con entradas en D e $\eta = (B_1, B_2, B_3, E_1, E_2, E_3)^T$ un vector de incógnitas representando aos campos magnético e eléctrico.

A primeira observación a realizar é que a seguinte é unha resolución libre e finita do D-módulo do sistema, $M = D^{1\times 6}/(D^{1\times 4}R_1)$:

$$0 \longrightarrow D \xrightarrow{.R_2} D^{1\times 4} \xrightarrow{.R_1} D^{1\times 6} \xrightarrow{\pi} M \longrightarrow 0, \tag{4.8}$$

onde $R_2 = (\partial_1\ \partial_2\ \partial_3\ -\partial_t) \in D^{1\times 4}$ e $R_1 = R$. Notemos que a matriz R dá o comezo da resolución libre e finita (4.8), por ser M un D-módulo pola esquerda finitamente presentado por R. En canto a R_2, non hai máis que observar que é a matriz que define a condición de compatibilidade (4.5) do sistema non homoxéneo dado pola segunda e a cuarta ecuacións de (4.3) (tal e como indicamos previamente), logo $\ker(.R_1) = DR_2$, recordando a interpretación do Algoritmo 3.17. Finalmente, se denotamos por ∂_i calquera das compoñentes de R_2, resulta que para $d \in D$, $d\partial_i = 0$ se e só se $d = 0$, por ser D un dominio. Así, $\ker(.R_2) = 0$, o que remata a resolución libre e finita de M dada en (4.8).

Calculemos agora os grupos abelianos $\operatorname{ext}^i_D(N, D)$ da trasposta de Auslander de M, que é simplemente $N = D^{1\times 4}/(D^{1\times 6}R_1^T)$. Seguiremos os pasos do Algoritmo 4.7 e da súa xeneralización para os grupos abelianos das extensións de orde superior. Precisamos entón unha resolución libre e finita de N. O comezo desta témolo por ser N un D-módulo pola esquerda finitamente presentado pola matriz $R_1^T \in D^{6\times 4}$. Así, se denotamos $S_1 = R_1^T$, temos a seguinte sucesión exacta:

$$D^{1\times 6} \xrightarrow{.S_1} D^{1\times 4} \xrightarrow{\kappa} N \longrightarrow 0,$$

onde $\kappa\colon D^{1\times 4} \longrightarrow N$ denota a proxección canónica en N, e a matriz S_1 é (explicitamente):

$$S_1 = \begin{pmatrix} \partial_t & 0 & 0 & \partial_1 \\ 0 & \partial_t & 0 & \partial_2 \\ 0 & 0 & \partial_t & \partial_3 \\ 0 & \partial_3 & -\partial_2 & 0 \\ -\partial_3 & 0 & \partial_1 & 0 \\ \partial_2 & -\partial_1 & 0 & 0 \end{pmatrix} \in D^{6\times 4}$$

Para calcular o seguinte homomorfismo na resolución libre e finita de N necesitamos atopar unha matriz $S_2 \in D^{r\times 6}$ tal que $D^{1\times r}S_2 = \ker(.S_1)$, de acordo co Algoritmo 3.17. Imos achar as condicións de compatibilidade do sistema non homoxéneo que define S_1, e para iso convén expresar este último na forma das ecuacións de Maxwell de (4.6). Separando o vector de incógnitas nun campo vectorial $\vec{C}$ e noutro campo escalar G, temos o seguinte sistema:

$$\begin{cases} \partial_t \vec{C} + \vec{\nabla} G = \vec{F}, \\ -\vec{\nabla} \times \vec{C} = \vec{D}, \end{cases}$$

con $\vec{F}$ e $\vec{D}$ a parte non homoxénea do sistema. Aplicando o operador diverxencia na segunda ecuación:

$$\vec{\nabla} \cdot \left(-\vec{\nabla} \times \vec{C}\right) = \vec{\nabla} \cdot \vec{D},$$

e, de novo, a diverxencia dun campo vectorial que é o rotacional doutro campo vectorial é nulo. Deste xeito, obtemos xa unha primeira condición de compatibilidade:

$$\vec{\nabla} \cdot \vec{D} = 0. \tag{4.9}$$

Apliquemos agora o operador rotacional na primeira ecuación:

$$\vec{\nabla} \times \left(\partial_t \vec{C}\right) + \vec{\nabla} \times \left(\vec{\nabla} G\right) = \vec{\nabla} \times \vec{F}.$$

Xa que o rotacional dun campo vectorial que é o gradiente dun campo escalar é tamén nulo, o segundo termo do membro esquerdo da anterior ecuación anúlase. Utilizando isto último, que D é un anel conmutativo (logo a derivada temporal e o rotacional conmutan) e que $-\vec{\nabla} \times C = \vec{D}$, chegamos a unha segunda condición de compatibilidade:

$$\partial_t \vec{D} + \vec{\nabla} \times \vec{F} = 0. \tag{4.10}$$

As ecuacións (4.9) e (4.10) nos campos $\vec{F}$ e $\vec{D}$ son en realidade catro ecuacións nas incógnitas $F_1, F_2, F_3, D_1, D_2, D_3$. Notemos que coinciden coas ecuacións de (4.6) se identificamos $\vec{F} = \vec{E}$ e $\vec{G} = \vec{B}$. Entón pódense expresar como $S_2(F_1, F_2, F_3, D_1, D_2, D_3)^T = 0$, onde S_2 é a seguinte matriz:

$$S_2 = \begin{pmatrix} 0 & -\partial_3 & \partial_2 & \partial_t & 0 & 0 \\ \partial_3 & 0 & -\partial_1 & 0 & \partial_t & 0 \\ -\partial_2 & \partial_1 & 0 & 0 & 0 & \partial_t \\ 0 & 0 & 0 & \partial_1 & \partial_2 & \partial_3 \end{pmatrix}. \tag{4.11}$$

Así, resulta que $\ker(.S_1) = D^{1\times 4} S_2$. Ademais, é fácil comprobar que $\ker(.S_2) = DR_2$, facendo un desenvolvemento totalmente análogo ao realizado para deducir a ecuación de continuidade (4.4). Isto permite completar a resolución libre e finita de N a partir da de M,

$$0 \longrightarrow D \xrightarrow{.S_3} D^{1\times 4} \xrightarrow{.S_2} D^{1\times 6} \xrightarrow{.S_1} D^{1\times 4} \xrightarrow{\kappa} N \longrightarrow 0,$$

onde tamén definimos $S_3 = R_2$. A partir da resolución libre e finita de N definimos o seguinte cocomplexo de D-módulos pola esquerda:

$$0 \longleftarrow D \xleftarrow{.S_3^T} D^{1\times 4} \xleftarrow{.S_2^T} D^{1\times 6} \xleftarrow{.S_1^T} D^{1\times 4} \longleftarrow 0,$$

e con isto xa podemos pasar a calcular os grupos abelianos $\mathrm{ext}^i_D(N, D)$.

(1) Comececemos polo grupo abeliano $\mathrm{ext}^1_D(N, D)$. Aplicando a xeneralización do Algoritmo 4.7, precisamos antes de nada atopar unha matriz que xere o D-submódulo pola esquerda $\ker(.S_2^T)$ de $D^{1\times 6}$. Atendendo á forma das matrices R_1 e S_2 temos que para $\lambda = (\lambda_1\ \lambda_2\ \lambda_3\ \lambda_4\ \lambda_5\ \lambda_6) \in D^{1\times 6}$:

$$(\lambda_1\ \lambda_2\ \lambda_3\ \lambda_4\ \lambda_5\ \lambda_6) \in \ker(.R_1^T) \iff (\lambda_4\ \lambda_5\ \lambda_6\ \lambda_1\ \lambda_2\ \lambda_3) \in \ker(.S_2^T).$$

Introducindo a matriz

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \tag{4.12}$$

resulta que $\lambda \in \ker(.S_2^T)$ se e só se $\lambda U \in \ker(.R_1^T)$, logo $\ker(.S_2^T) = \ker(.R_1^T)U$. Por outro lado, empregando a resolución libre e finita de N obtemos que $\ker(.R_1^T) = D^{1\times 4} S_2$, e como $S_2 U = R_1$, resulta que $\ker(.S_2^T) = (D^{1\times 4} S_2)U = D^{1\times 4} R_1$. Así pois, volvendo á xeneralización do Algoritmo 4.7 obtemos que $\mathrm{ext}^1_D(N, D) = (D^{1\times 4} R_1)/(D^{1\times 4} S_1^T)$. Pero $S_1 = R_1^T$, logo $S_1^T = R_1$, de onde se segue que $\mathrm{ext}^1_D(N, D) = 0$.

(2) Vaiamos agora con $\text{ext}^2_D(N,D)$. De novo, precisamos atopar unha matriz que xere o D-submódulo pola esquerda $\ker(.S_3^T) = \ker(.R_2^T)$. Sexa $\lambda \in D^{1\times 4}$ calquera. Tense que $\lambda R_2^T = 0$ equivale a $R_2\lambda^T = 0$. Recordando que $R_2 = (\partial_1\ \partial_2\ \partial_3\ -\partial_t)$, temos que atopar as condicións de compatibilidade do seguinte sistema non homoxéneo:

$$\begin{cases} \vec{\nabla} f = \vec{L}, \\ -\partial_t f = g. \end{cases}$$

Cómpre aclarar que aquí $\vec{L}$ e g son simplemente a parte non homoxénea do sistema. Xa que o rotacional do gradiente dun campo escalar é nulo, $\vec{\nabla} \times \vec{L} = \vec{0}$. Aplicando o operador gradiente na segunda ecuación, conmutando coa derivada temporal e substituíndo a primeira, atopamos que:

$$\partial_t \vec{L} + \vec{\nabla} g = 0.$$

É fácil ver que estas dúas condicións de compatibilidade están definidas en D pola matriz $S_1 \in D^{6\times 4}$. Entón $\ker(.S_3^T) = D^{1\times 6}S_1$. Así, $\text{ext}^2_D(N,D) = (D^{1\times 6}S_1)/(D^{1\times 6}S_2^T)$. Pero $S_2U = R_1$, logo $U^TS_2^T = US_2^T = R_1^T = S_1$. Como U é unha matriz 6×6 invertible temos que $D^{1\times 6} = D^{1\times 6}U$. Entón $D^{1\times 6}S_1 = D^{1\times 6}(US_2^T) = (D^{1\times 6}U)S_2^T = D^{1\times 6}S_2^T$, de onde se segue claramente que $\text{ext}^2_D(N,D) = 0$.

(3) Calculemos, finalmente $\text{ext}^3_D(N,D)$. Notemos que, en efecto, é o último grupo abeliano das extensións que podería ser non nulo, tendo en conta o cocomplexo de D-módulos pola esquerda que estamos a utilizar. Claramente $\ker(D \to 0) = D$. Deste xeito, $\text{ext}^3_D(N,D) = D/(D^{1\times 4}S_3^T)$, e este grupo abeliano é non nulo, pois os elementos de $D^{1\times 4}S_3^T$ son da forma $d_1\partial_1 + d_2\partial_2 + d_3\partial_3 - d_4\partial_t$, e así $1 \notin D^{1\times 4}S_3^T$, pero $1 \in D$.

Concluímos que $\text{ext}^1_D(N,D) = 0$ e $\text{ext}^2_D(N,D) = 0$, o que amosa que $M = D^{1\times 6}/(D^{1\times 4}R_1)$ é un D-módulo pola esquerda libre de torsión e reflexivo, pero non é proxectivo, pois $\text{ext}^3_D(N,D) \neq 0$.

Coa presentación destes dous exemplos finalizamos a sección. Notemos que neste último exemplo poderiamos ter realizado o cálculo dos grupos abelianos das extensións directamente sobre o cocomplexo de grupos abelianos asociado á resolución libre e finita de N, tal e como fixemos no Exemplo 3.28. Como D é un anel conmutativo, o cálculo sería análogo ao que vimos de realizar. Con todo, se o sistema é máis complicado, achar as condicións de compatibilidade pode resultar unha tarefa complexa. É entón importante dispoñer dun método que nos permita atopar os grupos abelianos das extensións nestas situacións máis difíciles, de aí a necesidade do algoritmo presentado nesta sección, aínda nas condicións simplificadas dun anel conmutativo de operadores diferenciais.

4.2. Parametrizacións de sistemas lineares

Chegados a este punto, xa sabemos que todas as ideas de Álxebra Homolóxica e Teoría de Módulos tratadas no anterior capítulo teñen importantes implicacións á hora de estudar o D-módulo dun certo sistema linear, pero aínda non sabemos as implicacións que isto ten sobre

o propio sistema ou as súas solucións. Na vindeira sección esta relación farase evidente, pero estamos xa en condicións de presentar un concepto que se pode formular aínda no marco da Análise Alxébrica e que ten unha clara e inmediata interpretación en termos das solucións do sistema: a *parametrización do sistema linear*. Trataremos agora de introducir o devandito concepto e ver cal é a súa relevancia no noso estudo, e intentaremos ilustralo empregando os mesmos casos sinxelos tratados na anterior sección.

Comezamos entón presentando a definición de parametrización dun sistema linear e remarcando certos puntos sobre ela. Para iso baseámonos na exposición realizada en [20].

Definición 4.11. Sexa D un dominio noetheriano e consideremos o sistema linear $R\eta = 0$, con $R \in D^{q\times p}$. Sexa tamén F o D-módulo pola esquerda no que se buscan as solucións do sistema. Dicimos que o homomorfismo de grupos abelianos $P.\colon F^{m\times 1} \longrightarrow F^{p\times 1}$ (definido da forma usual), con $m \in \mathbb{N}$, é unha *parametrización do sistema linear en* $F^{p\times 1}$ se

$$F^{q\times 1} \xleftarrow{R.} F^{p\times 1} \xleftarrow{P.} F^{m\times 1}$$

é unha sucesión exacta de grupos abelianos. Habitualmente a matriz $P \in D^{p\times m}$ tamén recibe o nome de parametrización do sistema linear en $F^{p\times 1}$.

Observación 4.12.

- Se K é un corpo e consideramos o anel conmutativo de operadores diferenciais, $D = K[\partial_1, \ldots, \partial_n]$, entón os homomorfismos de grupos abelianos $R.$ e $P.$ son tamén homomorfismos de D-módulos pola esquerda, como xa sinalamos na Observación 3.13. Así, nas condicións simplificadas nas que presentamos os resultados da anterior sección, a parametrización dun sistema linear é un homomorfismo de D-módulos pola esquerda.

- Supoñamos $P \in D^{p\times m}$ unha parametrización do sistema linear $R\eta = 0$, con $R \in D^{q\times p}$. Daquela $F^{q\times 1} \xleftarrow{R.} F^{p\times 1} \xleftarrow{P.} F^{m\times 1}$ é unha sucesión exacta de grupos abelianos, e empregando a exactitude en $F^{p\times 1}$ resulta que $\ker(R.) = \mathrm{Im}(P.) = PF^{m\times 1}$. Como $\ker(R.)$ é o conxunto de solucións en $F^{p\times 1}$ de $R\eta = 0$,

  $$\ker(R.) = \{\eta \in F^{p\times 1} | R\eta = 0\},$$

  resulta que o devandito conxunto escríbese como $PF^{m\times 1}$, isto é, trátase de combinacións lineares das columnas de P,

  $$PF^{m\times 1} = \{P_{*1}f_1 + \cdots + P_{*m}f_m \mid f_1, \ldots, f_m \in F\}.$$

  Así, é natural dicir que P *parametriza* as solucións de $R\eta = 0$ en $F^{p\times 1}$.

Presentamos a continuación as definicións de D-módulo pola esquerda *coxerador* e *inxectivo*. Co establecemento do isomorfismo de Malgrange xa adiantamos que ao supoñer F un D-módulo pola esquerda con estas características as propiedades do sistema linear $R\eta = 0$ en $F^{p\times 1}$ dependen só do D-módulo do sistema, e con isto xusticamos o estudo do devandito obxecto. A razón de tal afirmación comprenderase coa presentación dos principais resultados desta sección e da seguinte.

Definición 4.13.

- Un D-módulo pola esquerda F dise *coxerador* se para cada D-módulo pola esquerda M o elemento neutro de M é o único elemento no núcleo de todo homomorfismo $M \longrightarrow F$.

- Un D-módulo pola esquerda F dise *inxectivo* se para toda sucesión exacta de D-módulos pola esquerda:
$$M_\bullet \ \ldots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \ldots \ .$$
o cocomplexo de grupos abelianos asociado é tamén exacto, sendo este:
$$\ldots \xleftarrow{(d_{i+2})^*} \hom(M_{i+1}, F) \xleftarrow{(d_{i+1})^*} \hom(M_i, F) \xleftarrow{(d_i)^*} \hom(M_{i-1}, F) \xleftarrow{(d_{i-1})^*} \ldots,$$
onde $(d_i)^*(f) = f \circ d_i$ para cada $f \in \hom(M_{i-1}, F)$. Isto é certo, en particular, para resolucións libres e finitas de D-módulos pola esquerda, de xeito que $\operatorname{ext}^i_D(M, F) = 0$ para todo D-módulo pola esquerda M e todo $i \geq 0$.

Exemplo 4.14. Sexa $K = \mathbb{R}$ ou $K = \mathbb{C}$ e tomemos o anel de operadores diferenciais con coeficientes en K, $D = K[\partial_1, \ldots, \partial_n]$. Consideremos o conxunto de funcións definidas en $\mathbb{R}^n$ infinitamente diferenciables, $F = \mathscr{C}^\infty(\mathbb{R}^n)$. Xa vimos en diversas ocasións que F é un D-módulo pola esquerda, pero resulta que ademais é coxerador e inxectivo, tal e como se indica en [14].

Enunciamos agora unha propiedade que satisfán os D-módulos pola esquerda coxeradores. Esta dedúcese inmediatamente a partir dun resultado enunciado e probado en [9, Teorema 3.1] baixo condicións máis xerais (para un determinado tipo de módulos pola esquerda nos que se encadran os coxeradores que vimos de presentar). O resultado que nós presentamos, seguindo o exposto en [20], é o común no marco da Análise Alxébrica.

Proposición 4.15. *Se un D-módulo pola esquerda F é coxerador, entón a exactitude do cocomplexo de grupos abelianos*
$$\ldots \xleftarrow{(.R_4)^*} \hom(D^{1\times r_3}, F) \xleftarrow{(.R_3)^*} \hom_D(D^{1\times r_2}, F) \xleftarrow{(.R_2)^*} \hom(D^{1\times r_1}, F) \xleftarrow{(.R_1)^*} \hom(D^{1\times r_0}, F) \longleftarrow 0,$$
implica a exactitude do complexo de D-módulos pola esquerda
$$\ldots \xrightarrow{.R_4} D^{1\times r_3} \xrightarrow{.R_3} D^{1\times r_2} \xrightarrow{.R_2} D^{1\times r_1} \xrightarrow{.R_1} D^{1\times r_0} \xrightarrow{\pi} M \longrightarrow 0.$$

A anterior propiedade vainos permitir probar un importante teorema que atangue á relación existente entre o concepto de parametrización dun sistema linear e as ferramentas que introducimos nas anteriores seccións, isto é, os grupos abelianos $\operatorname{ext}^i_D(N, D)$, onde N é a trasposta de Auslander do D-módulo do sistema. A relevancia deste resultado faise maior cando temos en conta as ideas expostas na Observación 4.12: estamos a caracterizar xa un concepto cunha clara interpretación en termos das solucións do sistema linear.

Teorema 4.16. *Sexa D un dominio noetheriano e consideremos o D-módulo pola esquerda finitamente presentado pola matriz $R \in D^{q\times p}$, isto é, $M = D^{1\times p}/(D^{1\times q}R)$. Sexa F un D-módulo pola esquerda inxectivo e coxerador. Entón existe unha parametrización $P \in D^{p\times m}$ do sistema $R\eta = 0$ en $F^{p\times 1}$ para algún $m \in \mathbb{N}$ se e só se $\operatorname{ext}^1_D(N, D) = 0$, con N a trasposta de Auslander de M (equivalentemente, $t(M) = 0$).*

Demostración. Supoñamos en primeiro lugar que $P \in D^{p\times m}$ é unha parametrización do sistema $R\eta = 0$ en $F^{p\times 1}$ para algún $m \in \mathbb{N}$. Entón tense a seguinte sucesión exacta de grupos abelianos:
$$F^{q\times 1} \xleftarrow{R.} F^{p\times 1} \xleftarrow{P.} F^{m\times 1}.$$

Empregando os resultados da Observación 3.27 sabemos que unha sucesión exacta equivalente é a que segue:

$$\hom(D^{1\times q}, F) \xleftarrow{R.} \hom(D^{1\times p}, F) \xleftarrow{P.} \hom(D^{1\times m}, F),$$

e por ser F un D-módulo pola esquerda coxerador, en virtude da Proposición 4.15 temos que a seguinte é tamén unha sucesión exacta:

$$D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.P} D^{1\times m}.$$

En particular $\ker(.P) = \mathrm{Im}(.R) = D^{1\times q}R$. Se agora aplicamos o Teorema 2.15 (Primeiro Teorema de Isomorfía) ao homomorfismo de D-módulos pola esquerda $.P$ obtemos que $D^{1\times p}/\ker(.P) \simeq \mathrm{Im}(.P) \subset D^{1\times m}$. Empregando que $\ker(.P) = D^{1\times q}R$, $M \simeq \mathrm{Im}(.P) \subset D^{1\times m}$. Agora basta observar que $d\lambda \neq 0$ para todo $d \in D$, $d \neq 0$ e todo $\lambda \in D^{1\times m}$, $\lambda \neq 0$, pois D é un dominio, e daquela $t(D^{1\times m}) = 0$. Pero $M \simeq \mathrm{Im}(.P) \subset D^{1\times m}$, e entón necesariamente $t(M) = 0$, e polo Teorema 4.2 e a Observación 4.3 isto é equivalente a que $\mathrm{ext}^1_D(N, D) = 0$, con N a trasposta de Auslander de M.

Supoñamos agora que $\mathrm{ext}^1_D(N, D) = 0$ (equivalentemente, $t(M) = 0$, de acordo co Teorema 4.2 e a Observación 4.3). Empregando o Algoritmo 4.7 temos que $(D^{1\times q'}R')/(D^{1\times q}R) = 0$, con $R' \in D^{q'\times p}$ cumprindo $\ker(.P) = D^{1\times q'}R'$, para $P \in D^{p\times m}$ tal que $\ker(.R^T) = D^{1\times m}P^T$. Pero entón $\ker(.P) = D^{1\times q'}R' = D^{1\times q}R = \mathrm{Im}(.R)$, e así a seguinte é unha sucesión exacta de D-módulos pola esquerda:

$$D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.P} D^{1\times m}.$$

Como F é un D-módulo pola esquerda inxectivo, tamén será exacto o cocomplexo de grupos abelianos

$$\hom(D^{1\times q}, F) \xleftarrow{R.} \hom(D^{1\times p}, F) \xleftarrow{P^T.} \hom(D^{1\times m}, F),$$

e disto séguese que $P.$ é unha parametrización do sistema linear $R\eta = 0$ en $F^{p\times 1}$, empregando de novo os resultados da Observación 3.27. ■

Debemos notar que na anterior demostración hai dous pasos fundamentais. Por un lado, poder transformar unha sucesión exacta de grupos abelianos, $F^{q\times 1} \xleftarrow{R.} F^{p\times 1} \xleftarrow{P.} F^{m\times 1}$, noutra sucesión exacta de D-módulos pola esquerda, $D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.P} D^{1\times m}$, e utilizar o Teorema 4.2 xunto coa Observación 4.3. Por outro lado, poder utilizar o Algoritmo 4.7 para ver que implicacións ten que $\mathrm{ext}^1_D(N, D) = 0$, onde N é a trasposta de Auslander do D-módulo do sistema. Así, razoando de forma totalmente análoga poderiamos derivar unha serie de resultados para os grupos abelianos $\mathrm{ext}^i_D(N, D)$ de orde superior ($i \geq 1$), empregando para iso os Teoremas 4.2 e 4.4 e a xeneralización do Algoritmo 4.7 a este caso. Os devanditos resultados resumímolos no seguinte corolario.

Corolario 4.17. *Sexa D un dominio noetheriano e consideremos o D-módulo finitamente presentado por R, con $R \in D^{q\times p}$. Sexa tamén F un D-módulo pola esquerda inxectivo e coxerador, e introduzamos as notacións $P_1 = R$, $p_1 = p$ e $p_0 = q$. Tense que:*

- *M é un D-módulo pola esquerda libre de torsión se e só se existe $P_2 \in D^{p_1\times p_2}$ de xeito que se teña a seguinte sucesión exacta de grupos abelianos:*

$$F^{p_0\times 1} \xleftarrow{P_1.} F^{p_1\times 1} \xleftarrow{P_2.} F^{p_2\times 1}.$$

- *M é un D-módulo pola esquerda reflexivo se e só se existen $P_2 \in D^{p_1 \times p_2}$ e $P_3 \in D^{p_2 \times p_3}$ de xeito que se teña a seguinte sucesión exacta de grupos abelianos:*

$$F^{p_0 \times 1} \xleftarrow{P_1 \cdot} F^{p_1 \times 1} \xleftarrow{P_2 \cdot} F^{p_2 \times 1} \xleftarrow{P_3 \cdot} F^{p_3 \times 1}.$$

- *Se $D = K[\partial_1, \ldots, \partial_n]$, M é un D-módulo pola esquerda proxectivo se e só se existen n matrices $P_i \in D^{p_{i-1} \times p_i}$, $i = 2, \ldots, n+1$, de xeito que se teña a seguinte sucesión exacta de grupos abelianos:*

$$F^{p_0 \times 1} \xleftarrow{P_1 \cdot} F^{p_1 \times 1} \xleftarrow{P_2 \cdot} F^{p_2 \times 1} \xleftarrow{P_3 \cdot} \cdots \xleftarrow{P_n \cdot} F^{p_n \times 1} \xleftarrow{P_{n+1} \cdot} F^{p_{n+1} \times 1}.$$

Para rematar con esta sección imos exemplificar os resultados do Teorema 4.16 e do Corolario 4.17 empregando os casos sinxelos cos que xa traballamos en seccións previas: a sucesión gradiente-rotacional-diverxencia e as ecuacións de Maxwell.

Exemplo 4.18. Sexa D o anel de operadores diferenciais con coeficientes en $\mathbb{R}$, isto é, $D = \mathbb{R}[\partial_1, \partial_2, \partial_3]$, e consideremos o sistema linear $R\eta = 0$, con $R = (\partial_1 \ \partial_2 \ \partial_3)$ a matriz representando o operador diverxencia en $\mathbb{R}^3$. Tomemos o D-módulo pola esquerda $F = \mathscr{C}^\infty(\mathbb{R})$, que segundo o comentado no Exemplo 4.14 é un D-módulo pola esquerda coxerador e inxectivo. Segundo vimos no Exemplo 4.9, o D-módulo do sistema, $M = D^{1\times 3}/(DR)$, é un D-módulo pola esquerda libre de torsión e reflexivo. O Corolario 4.17 dinos que nestas circunstancias existen dúas matrices $P_2 \in D^{p \times p_2}$ e $P_3 \in D^{p_2 \times p_3}$, con $p_2, p_3 \in \mathbb{N}$, de forma que $F \xleftarrow{R \cdot} F^{3\times 1} \xleftarrow{P_2 \cdot} F^{p_2 \times 1} \xleftarrow{P_3 \cdot} F^{p_3 \times 1}$ é unha sucesión exacta de grupos abelianos, pero non nos dá as devanditas matrices.

Para obtelas cómpre recordar a demostración do Teorema 4.16. Vimos que, no caso de que $\operatorname{ext}^1_D(N, D) = 0$, unha parametrización en $F^{p\times 1}$ viña dada pola matriz $P \in D^{p\times m}$ que devolve o Algoritmo 4.7. Ademais, na Observación 4.8 comprobamos que para calcular a matriz P chegaba con tomar unha resolución libre e finita de N (a trasposta de Auslander de M),

$$D^{1\times m} \xrightarrow{\cdot Q} D^{1\times p} \xrightarrow{\cdot R^T} D^{1\times q} \xrightarrow{\overline{\pi}} N \longrightarrow 0,$$

onde $\overline{\pi}$ é a proxección canónica en N, e definir $P = Q^T$. Para o caso que estamos a tratar xa calculamos no Exemplo 3.28 unha resolución libre e finita,

$$0 \longrightarrow D \xrightarrow{\cdot R_3} D^{1\times 3} \xrightarrow{\cdot R_2} D^{1\times 3} \xrightarrow{\cdot R_1} D \xrightarrow{\kappa} N \longrightarrow 0,$$

onde $R_1 = R^T$, R_2 e $R_3 = R$ son as matrices que representan aos operadores gradiente, rotacional e diverxencia en $\mathbb{R}^3$, que explicitamos no Exemplo 3.20. En base ao que vimos de comentar, definindo $P = R_2^T$ obtemos unha parametrización do sistema $R\eta = 0$ en $F^{3\times 1}$. Como $R_2^T = -R_2$, as solucións do sistema $R\eta = 0$ veñen dadas por $-R_2\zeta$, con $\zeta = (\zeta_1, \zeta_2, \zeta_3)^T \in F^{3\times 1}$. Notemos que podemos obviar o signo negativo, xa que $R\eta = 0$ é equivalente a $R(-\eta) = 0$, pola linearidade do sistema. Daquela o único que estamos a afirmar é que o operador rotacional en $\mathbb{R}^3$ (representado pola matriz R_2) parametriza as solucións do sistema $R\eta = 0$.

A matriz $P = -R_2$ é a matriz P_2 do Corolario 4.17. Razoando de forma análoga, a matriz P_3 pódese obter do seguinte homomorfismo da resolución libre e finita de N, traspoñendo a

matriz asociada. Neste caso particular teriamos $P_3 = R_3^T = R^T = R_1$. Empregando a sucesión exacta do Corolario 4.17, isto dinos que o operador gradiente en $\mathbb{R}^3$ (representado pola matriz R_1) parametriza as solucións do sistema $R_2\eta = 0$.

Os resultados que acabamos de expoñer son ben coñecidos. Traballando con campos vectoriais e escalares en $\mathbb{R}^3$ infinitamente diferenciables, todo campo solenoidal é o rotacional doutro campo vectorial, e todo campo irrotacional é o gradiente dun campo escalar.

Exemplo 4.19. Sexa o anel de operadores diferenciais $D = \mathbb{R}[\partial_t, \partial_1, \partial_2, \partial_3]$, e consideremos o sistema linear $R_1\eta = 0$, con R_1 a matriz dada en (4.7) no Exemplo 4.10, isto é, a matriz que define a lei de Maxwell-Faraday e a lei de Gauss para o magnetismo. Como D-módulo pola esquerda no que buscamos as solucións escollemos $F = \mathscr{C}^\infty(\mathbb{R}^4)$, isto é, o conxunto de funcións infinitamente diferenciables en catro variables.

Como no caso anterior, xa sabemos que o D-módulo do sistema, $M = D^{1\times 6}/(D^{1\times 4}R_1)$, é reflexivo e libre de torsión, atendendo aos resultados obtidos no Exemplo 4.10. Así, o Corolario 4.17 tamén nos asegura a existencia de dúas matrices $P_2 \in D^{p\times p_2}$ e $P_3 \in D^{p_2\times p_3}$, con $p_2, p_3 \in \mathbb{N}$, de forma que $F^{4\times 1} \xleftarrow{R_1\cdot} F^{6\times 1} \xleftarrow{P_2\cdot} F^{p_2\times 1} \xleftarrow{P_3\cdot} F^{p_3\times 1}$ sexa unha sucesión exacta de grupos abelianos. De cara a atopar as matrices P_2 e P_3, tomamos unha resolución libre e finita de $N = D^{1\times 4}/(D^{1\times 6}R_1^T)$, a trasposta de Auslander do D-módulo do sistema, $M = D^{1\times 6}/(D^{1\times 4}R_1)$. Esta calculámola xa no Exemplo 4.10, obtendo:

$$0 \longrightarrow D \xrightarrow{\cdot S_3} D^{1\times 4} \xrightarrow{\cdot S_2} D^{1\times 6} \xrightarrow{\cdot S_1} D^{1\times 4} \xrightarrow{\kappa} N \longrightarrow 0,$$

onde κ é a proxección canónica en N, $S_1 = R_1^T$, $S_2 = R_1U$ (U é a matriz invertible dada en (4.12)) e $S_3 = R_2 = (\partial_1\ \partial_2\ \partial_3\ -\partial_t)$. Deste xeito, razoando igual que no exemplo anterior, da demostración do Teorema 4.16 deducimos que $P_2 = S_2^T = (R_1U)^T = U^TR_1^T = UR_1^T$ e $P_3 = S_3^T = R_2^T$. Vexamos entón cal é a interpretación das parametrizacións neste caso particular.

- Xa que a matriz

$$UR_1^T = \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0 \end{pmatrix}\begin{pmatrix} \partial_t&0&0&\partial_1\\ 0&\partial_t&0&\partial_2\\ 0&0&\partial_t&\partial_3\\ 0&\partial_3&-\partial_2&0\\ -\partial_3&0&\partial_1&0\\ \partial_2&-\partial_1&0&0 \end{pmatrix} = \begin{pmatrix} 0&\partial_3&-\partial_2&0\\ -\partial_3&0&\partial_1&0\\ \partial_2&-\partial_1&0&0\\ \partial_t&0&0&\partial_1\\ 0&\partial_t&0&\partial_2\\ 0&0&\partial_t&\partial_3 \end{pmatrix}$$

é unha parametrización do sistema linear $R_1\eta = 0$ en $F^{6\times 1}$, os campos magnético e eléctrico, $\vec{B} = (B_1, B_2, B_3)$ e $\vec{E} = (E_1, E_2, E_3)$, pódense obter como

$$\begin{pmatrix} B_1\\ B_2\\ B_3\\ E_1\\ E_2\\ E_3 \end{pmatrix} = \begin{pmatrix} 0&\partial_3&-\partial_2&0\\ -\partial_3&0&\partial_1&0\\ \partial_2&-\partial_1&0&0\\ \partial_t&0&0&\partial_1\\ 0&\partial_t&0&\partial_2\\ 0&0&\partial_t&\partial_3 \end{pmatrix}\begin{pmatrix} \zeta_1\\ \zeta_2\\ \zeta_3\\ \zeta_4 \end{pmatrix},$$

con $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)^T \in F^{4\times 1}$. Definindo o *potencial vectorial* como $\vec{A} = -(\zeta_1, \zeta_2, \zeta_3) \in F^{3\times 1}$ e o *potencial escalar* como $\Phi = -\zeta_4 \in F$, e recuperando a notación $\vec{\nabla}\times\vec{F}$ para

o rotacional do campo vectorial $\vec{F} \in F^{3\times 1}$ e $\vec{\nabla} f$ para o gradiente do campo escalar $f \in F$, obtemos que:

$$\vec{B} = \vec{\nabla} \times \vec{A}, \quad \vec{E} = -\partial_t \vec{A} - \vec{\nabla}\Phi. \tag{4.13}$$

As anteriores son as expresións clásicas en Electrodinámica dos campos magnético e eléctrico en función dos potenciais vectorial e escalar, que se poden deducir directamente a partir das ecuacións de Maxwell e dos resultados que derivamos para a sucesión gradiente-rotacional-diverxencia, como se amosa en [10].

- Segundo os resultados expostos no Corolario 4.17 a seguinte é una sucesión exacta:

$$F^{4\times 1} \xleftarrow{R_1\cdot} F^{6\times 1} \xleftarrow{UR_1^T\cdot} F^{4\times 1} \xleftarrow{R_2^T\cdot} F.$$

Así, por definición, a matriz $R_2^T = (\partial_1 \ \partial_2 \ \partial_3 \ -\partial_t)^T \in D^{4\times 1}$ parametriza as solucións do sistema linear $UR_1^T\eta = 0$ en $F^{4\times 1}$. Nestas circunstancias, se para $\zeta \in F$ definimos $\vec{A'} \in F^{3\times 1}$ e $\Phi' \in F$ tales que $(\vec{A'}, \Phi') = (A'_1, A'_2, A'_3, \Phi') = R_2\zeta$, isto é,

$$\vec{A'} = (A'_1, A'_2, A'_3)^T = \vec{\nabla}\zeta, \quad \Phi' = -\partial_t\zeta$$

resulta que $UR_1^T(\vec{A'}, \Phi') = 0$, logo $\vec{\nabla} \times \vec{A'} = 0$ e $-\partial_t\vec{A'} - \vec{\nabla}\Phi' = 0$. Así pois, se os campos magnético e eléctrico están dados en función dos potenciais vectorial e escalar $\vec{A}$ e Φ a través de (4.13), isto dinos que podemos empregar $\vec{A} + \vec{\nabla}\zeta$ e $-\partial_t\zeta$, con $\zeta \in F$ unha función calquera, como potenciais vectorial e escalar, pois os campos magnético e eléctrico son os mesmos. En Electrodinámica este grao de liberdade adicional elimínase escollendo un *calibre* (máis coñecido polo nome en inglés, *gauge*). Os máis comúns son o *calibre de Coulomb*, $\vec{\nabla} \cdot \vec{A} = 0$, e o *calibre de Lorenz*, $\vec{\nabla} \cdot \vec{A} + \partial_t\Phi/c = 0$.

Os casos sinxelos que vimos tratando permítennos ver como a teoría exposta é aplicable a diversos problemas cuxa solución coñecemos. Deste xeito, é evidente que temos un marco común no que encadrar problemas aparentemente moi distintos, pero que se poden formular como sistemas lineares. Así e todo, vemos xa como no caso das ecuacións de Maxwell a cantidade de cálculos e desenvolvementos a realizar comeza a ser importante se só pretendemos empregar os algoritmos presentados como guía ou axuda, sen acudir ás implementacións destes en distintos softwares de cálculo numérico e simbólico. De considerar un caso máis complexo, a resolución do problema manualmente sería xa inviable. Na seguinte e derradeira sección poñeremos de manifesto a utilidade e a efectividade dos algoritmos tratados, aplicándoos directamente ao exemplo das ecuacións de Maxwell. Veremos como todas as tarefas se simplifican notablemente, o que xustifica a introdución de todas as ferramentas teóricas necesarias para presentar os devanditos algoritmos.

4.3. Relación entre as propiedades do sistema linear e do módulo do sistema

Nesta última sección imos introducir algunhas propiedades que caracterizan os sistemas lineares nos que estamos interesados, da forma $R\eta = 0$, con R unha matriz $q \times p$ con entradas nunha álxebra de Ore que é tamén un anel noetheriano pola esquerda. Notemos que

este é o marco xeral no que traballamos ao principio do noso tratamento. Estas propiedades obtéñense xeneralizando definicións propias da Teoría do Control, e pódense atopar en calquera referencia de Análise Alxébrica. Nós seguiremos esencialmente o exposto en [3].

A continuación consideraremos tamén que o D-módulo pola esquerda no que se buscan as solucións do sistema linear é coxerador e inxectivo. Xa vimos co Teorema 4.16 e co Corolario 4.17 que esta é a situación propicia de cara a relacionar o concepto de parametrización dun sistema linear coas propiedades do D-módulo do sistema. Veremos que isto é así tamén para o resto de conceptos que a continuación introducimos.

Definición 4.20. Sexa D unha álxebra de Ore noetheriana pola esquerda, $R \in D^{q\times p}$, e consideremos o sistema linear $R\eta = 0$. Sexa tamén F un D-módulo pola esquerda coxerador e inxectivo no que buscamos as solucións, e $\ker(R.) = \{\eta \in F^{p\times 1} \mid R\eta = 0\}$ o conxunto de solucións en $F^{p\times 1}$.

(1) Un *observable* de $\ker(R.)$ é calquera combinación linear pola esquerda con coeficientes en D das variables do sistema η_i, $i = 1, \ldots, p$, que denotamos por $\psi(\eta)$. Un observable $\psi(\eta)$ dise *autónomo* se satisfai unha ecuación non trivial en D, isto é, se existe algún $d \in D \setminus \{0\}$ tal que $d\psi(\eta) = 0$. Se un observable non é autónomo, entón dise que é *libre*.

(2) O sistema linear $R\eta = 0$ é *autónomo* se cada observable de $\ker(R.)$ é autónomo.

(3) O sistema linear $R\eta = 0$ é *autónomo-libre* ou *controlable* se cada observable de $\ker(R.)$ é libre.

(4) O sistema linear $R\eta = 0$ é *parametrizable* se admite unha parametrización $P \in D^{p\times m}$, con $m \in \mathbb{N}$, en $F^{p\times 1}$, no sentido da Definición 4.11 (equivalentemente, existe $P \in D^{p\times m}$ tal que $\ker(R.) = PF^{m\times 1}$). Isto quere dicir que para cada $\eta \in \ker(R.)$ existe $\xi \in F^{m\times 1}$ cumprindo $\eta = P\xi$. Nestas circunstancias dise que ξ é un *potencial*.

(5) Poñamos $R = (R_1\ R_2)$, con $R_1 \in D^{q\times r}$ e $R_2 \in D^{q\times(p-r)}$ para algún $r = 1, ..., p-1$, unha *partición* de R. Así, podemos escribir o conxunto de solucións do sistema linear como segue:
$$\ker(R.) = \{\eta = (\eta_1, \eta_2) \in F^{p\times 1} \mid R_1\eta_1 + R_2\eta_2 = 0\}.$$
Dicimos que η_1 é *observable desde* η_2 se η_1 está determinado unicamente por η_2 no seguinte sentido:
$$\zeta = (\zeta_1^T, \eta_2^T)^T \in F^{p\times 1} \in \ker(R.) \Rightarrow \zeta_1 = \eta_1.$$

(6) O sistema linear $R\eta = 0$ é *plano* se admite unha *parametrización inxectiva*, isto é, se existe unha parametrización $P \in D^{p\times m}$, $m \in \mathbb{N}$, que admita unha inversa $T \in D^{m\times p}$ pola esquerda: $TQ = I_m$. Equivalentemente, $R\eta = 0$ é plano se é parametrizable e cada compoñente ξ_i do potencial ξ é un observable do sistema. Dise entón que ξ é unha *saída plana* de $\ker(R.)$.

Notemos que os conceptos que vimos de introducir encádranse no formalismo da Teoría do Control, e non requiren de ningunha das ideas da Análise Alxébrica que estudamos

neste traballo. De feito, aquí vemos unha vez máis que o concepto de parametrización, que nós introducimos a partir dunha sucesión exacta, defínese en realidade empregando só o conxunto de solucións do sistema linear. Con todo, existe un *dicionario* entre as definicións que acabamos de presentar e as propiedades do D-módulo do sistema. Este pode ser consultado en calquera das referencias sobre Análise Alxébrica aplicada á Teoría do Control que fomos empregando, [3, 4, 17, 20]. Nós decidimos adoptar o proporcionado en [3] a través do enunciado e da demostración do seguinte teorema.

Teorema 4.21. *Sexa D unha álxebra de Ore noetheriana pola esquerda, $R \in D^{q\times p}$, F un D-módulo pola esquerda coxerador e inxectivo. Consideremos o sistema linear $R\eta = 0$ e o conxunto de solucións en $F^{p\times 1}$, $\ker(R.) = \{\eta \in F^{p\times 1} \mid R\eta = 0\}$. Sexa tamén $M = D^{1\times p}/(D^{1\times q}R)$ o módulo do sistema. Entón téñense os seguintes resultados:*

(1) Existe unha correspondencia entre os observables de $\ker(R.)$ *e os elementos de M.*

(2) Existe unha correspondencia entre os observables autónomos de $\ker(R.)$ *e os elementos de torsión de M.*

(3) O sistema linear $R\eta = 0$ é autónomo se e só se M é un D-módulo pola esquerda de torsión.

(4) O sistema linear $R\eta = 0$ é controlable se e só se M é un D-módulo pola esquerda libre de torsión.

(5) O sistema linear $R\eta = 0$ é parametrizable se e só se existe $P \in D^{p\times m}$, $m \in \mathbb{N}$, tal que $M \simeq D^{1\times p}P$.

(6) O sistema linear $R\eta = 0$ é plano se é so se M é un D-módulo pola esquerda libre. En tal caso existe unha correspondencia entre as bases de M e as saídas planas de $\ker(R.)$.

(7) Sexa $R = (R_1\ R_2)$ unha partición de R, con $R_1 \in D^{q\times r}$ e $R_2 \in D^{q\times(p-r)}$ para algún $r = 1, ..., p-1$. Sexa $\ker(R.) = \{\eta = (\eta_1, \eta_2) \in F^{p\times 1} \mid R_1\eta_1 + R_2\eta_2 = 0\}$ *o conxunto de solucións do sistema linear asociado á partición dada. En tal caso, η_1 é observable desde η_2 se e só se $M_1 = D^{1\times r}/(D^{1\times q}R_1) = 0$, isto é, se e só se R_1 admite unha inversa pola esquerda $S_1 \in D^{r\times q}$, logo $S_1R_1 = I_r$.*

Observación 4.22. Realicemos algún comentario sobre o Teorema 4.21, para ver que algunhas das súas teses encaixan na teoría exposta neste traballo. Consideraremos entón o caso dun anel de operadores diferenciais conmutativo, que é a principal hipótese simplificadora introducida neste capítulo. Debemos observar que (3) e (4) séguense inmediatamente de (2) a partir das definicións de sistema autónomo e sistema controlable. Ademais, (2) é consecuencia directa de (1) e das definicións de elemento de torsión e observable autónomo. Neste sentido, está claro que o resultado fundamental é a correspondencia entre os observables de $\ker(R.)$ e os elementos do D-módulo do sistema, $M = D^{1\times p}/(D^{1\times q}R)$. En [3] pódese comprobar que, en efecto, esa é a tese cuxa demostración require de maior traballo.

Doutra banda, a tese (5) podémola probar inmediatamente traballando coa definición de parametrización dada na Definición 4.11. Así, que o sistema linear $R\eta = 0$ sexa parametrizable en $F^{p\times 1}$ equivale a que exista $P \in D^{p\times m}$ tal que a seguinte é unha sucesión exacta:

$$F^{q\times 1} \xleftarrow{R.} F^{p\times 1} \xleftarrow{P.} F^{m\times 1}.$$

Pero F é un D-módulo coxerador e inxectivo, logo tamén equivale a que se teña a seguinte sucesión exacta:

$$D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.P} D^{1\times m}.$$

Por último, a exactitude en $D^{1\times p}$ do anterior complexo equivale a que $\ker(.P) = D^{1\times q}R$. Pero entón $M = D^{1\times p}/(D^{1\times q}R) = D^{1\times p}/\ker(.P)$, e polo Primeiro Teorema de Isomorfía (Teorema 2.15), $M \simeq \mathrm{Im}(.P) = D^{1\times p}P$.

Finalmente, para probar e facer construtivas as teses (6) e (7) necesitariamos introducir certos conceptos e algoritmos a maiores, como aqueles que permiten calcular inversas pola dereita. Un tratamento destas cuestións pódese atopar en [17]. Aquí limitámonos a expoñer os resultados, por ser estes habituais e esenciais na Análise Alxébrica.

Imos rematar este traballo presentando un exemplo de aplicación directa da teoría e dos algoritmos expostos. Para facer evidente a súa necesidade e utilidade escollemos de novo o exemplo das ecuacións de Maxwell, tratado nos Exemplos 4.10 e 4.19. Nos dous casos fomos capaces de obter información sobre o módulo do sistema logo de razoamentos teóricos apoiados en resultados que xa coñecemos, como as condicións de compatibilidade das ecuacións de Maxwell. Veremos a continuación que nada disto é necesario se acudimos á implementación dos Algoritmos 3.17 e 4.7. Máis concretamente, imos utilizar as librarías que o sistema de álxebra computacional SINGULAR nos proporciona [7].

Exemplo 4.23. Imos tomar o sistema que definen a lei de Gauss magnética e a lei de Maxwell-Faraday, que sabemos que pode ser escrito como $R\eta = 0$, con R a matriz dada en (4.7). Como xa argumentamos, podemos tomar o anel de operadores diferenciais $D = \mathbb{R}[\partial_t, \partial_1, \partial_2, \partial_3]$. Pretendemos agora aplicar os Algoritmos 3.17 e 4.7 explicitamente para ver que grupos abelianos $\mathrm{ext}^i_D(N, D)$ son nulos, con $i \geq 1$ e N a trasposta de Auslander do D-módulo do sistema. Como D é conmutativo sabemos que podemos identificar N co D-módulo pola esquerda finitamente presentado por R^T.

O sistema SINGULAR ten implementada a libraría `control.lib`, documentada en [24], por exemplo. Proporcionando o D-módulo do sistema $R\eta = 0$ poderiamos utilizar unha das súas funcións para averiguar directamente que grupos abelianos $\mathrm{ext}^i_D(N, D)$ se anulan. Con todo, a resposta xa a sabemos, en base ao que vimos no Exemplo 4.10. Pretendemos aquí ilustrar a importancia das técnicas das bases de Gröbner nos Algoritmos 3.17 e 4.7. Para iso, seguiremos os pasos dos devanditos algoritmos, apoiándonos en funcións implementadas en SINGULAR para realizar os cálculos de bases de Gröbner que sexan oportunos. O código empregado atópase no Anexo A1, aquí limitámonos a presentar os resultados.

Deste xeito, segundo o Algoritmo 4.7 e a súa xeneralización dada na Observación 4.8, o primeiro que necesitamos é unha resolución libre e finita de N. O inicio xa o temos, tendo en conta que N é un D-módulo pola esquerda finitamente presentado por R^T:

$$D^{1\times 6} \xrightarrow{.R^T} D^{1\times 4} \xrightarrow{\kappa} N \longrightarrow 0.$$

Definimos $S_1 = R^T$, $q_0 = 4$ e $q_1 = 6$. Para continuar coa resolución libre e finita de N necesitamos atopar unha matriz $S_2 \in D^{q_2\times 6}$ tal que $\ker(.S_1) = D^{1\times q_2}S_2$, para algún $q_2 \in \mathbb{N}$. Para iso aplicamos o Algoritmo 3.17, baseado nas técnicas das bases de Gröbner. Apoiándonos nas funcións `std` e `intersect` de SINGULAR obtemos a matriz S_2 dada en (A.2):

$$S_2 = \begin{pmatrix} 0 & 0 & 0 & \partial_1 & \partial_2 & \partial_3 \\ 0 & -\partial_3 & \partial_2 & \partial_t & 0 & 0 \\ \partial_3 & 0 & -\partial_1 & 0 & \partial_t & 0 \\ -\partial_2 & \partial_1 & 0 & 0 & 0 & \partial_t \end{pmatrix}.$$

No Anexo A1 indicamos explicitamente como se realiza o cálculo en SINGULAR tendo como guía os pasos do Algoritmo 3.17. Repetindo o proceso para S_2, obtemos a matriz S_3:

$$S_3 = (\partial_t \ -\partial_1 \ -\partial_2 \ -\partial_3) \in D^{1\times 4},$$

e se, finalmente, repetimos para S_3, obtemos a matriz $S_4 = 0$. Con isto temos xa calculada unha resolución libre e finita de N:

$$0 \xrightarrow{.S_4} D^{1\times 4} \xrightarrow{.S_3} D^{1\times 6} \xrightarrow{.S_2} D^{1\times 4} \xrightarrow{.S_1} D^{1\times 6} \xrightarrow{\kappa} N \longrightarrow 0.$$

Segundo a Observación 4.8 que xeneraliza o Algoritmo 4.7, a partir desta resolución libre e finita temos que definir o seguinte cocomplexo de D-módulos pola esquerda:

$$0 \xleftarrow{.R_4^T} D^{1\times 4} \xleftarrow{.S_3^T} D^{1\times 6} \xleftarrow{.S_2^T} D^{1\times 4} \xleftarrow{.S_1^T} D^{1\times 6} \longleftarrow 0.$$

e calcular, para $i = 1,2,3$, unhas matrices R_i' tales que $\ker(.S_{i+1}^T) = D^{1\times q_{i-1}'} R_i'$. Para $i = 3$ temos xa que $\ker(.S_4^T) = \ker(D^{1\times 4} \longrightarrow 0) = D^{1\times 4}$. No caso de $i = 1,2$, realizamos o cálculo, de novo, empregando SINGULAR. Como antes, este pode consultarse no Anexo A1. As matrices R_1' e R_2' son as calculadas en (A.3), e que a continuación amosamos:

$$R_1' = \begin{pmatrix} \partial_1 & \partial_2 & \partial_3 & 0 & 0 & 0 \\ \partial_t & 0 & 0 & 0 & -\partial_3 & \partial_2 \\ 0 & \partial_t & 0 & \partial_3 & 0 & -\partial_1 \\ 0 & 0 & \partial_t & -\partial_2 & \partial_1 & 0 \end{pmatrix} \in D^{4\times 6},\ R_2' = \begin{pmatrix} 0 & 0 & -\partial_3 & \partial_2 \\ 0 & -\partial_2 & \partial_1 & 0 \\ 0 & -\partial_3 & 0 & \partial_1 \\ \partial_1 & \partial_t & 0 & 0 \\ \partial_2 & 0 & \partial_t & 0 \\ \partial_3 & 0 & 0 & \partial_t \end{pmatrix} \in D^{6\times 4}.$$

Segundo a Observación 4.8, $\operatorname{ext}_D^i(N,D) = (D^{1\times q_{i-1}'} R_i')/(D^{1\times q_{i-1}} S_i^T)$, $i = 1,2,3$. Para $i = 1$, $\operatorname{ext}_D^1(N,D) = (D^{1\times 4} R_1')/(D^{1\times 4} S_1^T)$, pero $S_1^T = R$, e R_1' obtense de R intercambiando as tres últimas filas coa primeira, logo $D^{1\times 4} R_1' = D^{1\times 4} S_1^T$, e así $\operatorname{ext}_D^1(N,D) = 0$. O mesmo lle ocorre a $\operatorname{ext}_D^2(N,D) = (D^{1\times 6} R_2')/(D^{1\times 6} S_2^T)$, pois R_2' obtense de R_2^T multiplicando por -1 as filas primeira e terceira e intercambiando a segunda coa terceira, logo $\operatorname{ext}_D^2(N,D) = 0$. Finalmente, $\operatorname{ext}_D^3(N,D) = (D^{1\times 4})/(D^{1\times 4} S_3^T) \neq 0$, como xa argumentamos no Exemplo 4.10.

Como $\operatorname{ext}_D^1(N,D) = 0$, o D-módulo do sistema é libre de torsión. Así, sabemos que o sistema $R\eta = 0$ é controlable, en virtude do Teorema 4.21. Ademais, cos cálculos realizados podemos obter tamén unha parametrización do sistema, simplemente definindo $P = S_2^T$. De novo, S_2^T obtense da parametrización do Exemplo 4.19 intercambiando as tres primeiras columnas coa última, co que os resultados son equivalentes.

Coa presentación deste exemplo finalizamos o noso tratamento da teoría da Análise Alxébrica. Agardamos que este último exemplo fora especialmente ilustrativo á hora de amosar a potencia e a utilidade dos algoritmos presentados, especialmente atendendo ás súas inmediatas implicacións na Teoría do Control. Con todo, a exposición realizada (e aínda máis esta última parte) é só introdutoria: a Análise Alxébrica é aínda hoxe unha teoría en expansión e cuxas aplicacións seguirán moi probablemente ampliándose nos próximos anos.

Bibliografía

[1] Auslander, M.: *Coherent functors*. In: Proceedings of the Conference on Categorical Algebra, pp. 189–231. Springer (1966)

[2] Auslander, M., Bridger, M.: Stable module theory. American Mathematical Society (1969)

[3] Chyzak, F., Quadrat, A., Robertz, D.: *Effective algorithms for parametrizing linear control systems over Ore algebras*. Applicable Algebra in Engineering, Communication and Computing **16**(5), 319–376 (2005)

[4] Cluzeau, T., Koutschan, C., Quadrat, A., Tõnso, M.: *Effective algebraic analysis approach to linear systems over Ore algebras*. In: Algebraic and Symbolic Computation Methods in Dynamical Systems, pp. 3–52. Springer (2020)

[5] Cox, D., Little, J., O'Shea, D.: Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer Science & Business Media (2013)

[6] Cox, D.A., Little, J., O'Shea, D.: Using algebraic geometry. Springer Science & Business Media (2006)

[7] Decker, W., Greuel, G.M., Pfister, G., Schönemann, H.: SINGULAR *4-2-1 — A computer algebra system for polynomial computations*. `http://www.singular.uni-kl.de` (2021)

[8] Hausdorf, M., Seiler, W.M.: *On the numerical analysis of overdetermined linear partial differential systems*. In: International Conference on Symbolic and Numerical Scientific Computation, pp. 152–167. Springer (2001)

[9] Ishikawa, T.: *Faithfully exact functors and their applications to projective modules and injective modules*. Nagoya Mathematical Journal **24**, 29–42 (1964)

[10] Jackson, J.D.: Classical Electrodynamics. John Wiley & Sons (2012)

[11] Kredel, H.: *Solvable polynomial rings*. Ph.D. thesis, Reihe Mathematik. Verlag Shaker, Aachen, Germany (1993)

[12] Lam, T.Y.: Lectures on modules and rings. Springer Science & Business Media (2012)

[13] Li, Z., Zhang, Y.: *A note on Groebner bases of Ore polynomials over a PID*. `http://www.algebra.uni-linz.ac.at/people/yzhang/GB.pdf`

[14] Malgrange, B.: Sur les systèmes différentiels à coefficients constants. Collège de France (1962)

[15] McConnell, J.C., Robson, J.C., Small, L.W.: Noncommutative noetherian rings. American Mathematical Society (2001)

[16] Ore, O.: *Theory of non-commutative polynomials*. Annals of Mathematics **34**(3), 480–508 (1933)

[17] Quadrat, A.: *An introduction to constructive algebraic analysis and its applications*. Les cours du CIRM **1**(2), 281–471 (2010)

[18] Quadrat, A., Zerz, E.: Algebraic and Symbolic Computation Methods in Dynamical Systems. Springer (2020)

[19] Quillen, D.: *Projective modules over polynomial rings*. Inventiones Mathematicae **36**(1), 167–171 (1976)

[20] Robertz, D.: *Recent progress in an algebraic analysis approach to linear systems*. Multidimensional Systems and Signal Processing **26**(2), 349–388 (2015)

[21] Rotman, J.J.: An introduction to homological algebra. Springer Science & Business Media (2008)

[22] Stafford, J.T.: *Module structure of Weyl algebras*. Journal of the London Mathematical Society **2**(3), 429–442 (1978)

[23] Suslin, A.: *Projective modules over polynomial rings are free*. Doklady Akademii nauk SSSR **229**, 1063–1066 (1976)

[24] Zerz, E., Levandovskyy, V.: *Algebraic systems theory and computer algebraic methods for some classes of linear control systems*. In: Proceedings of the Mathematical Theory of Networks and Systems, pp. 536–541. Springer (2006)

[25] Zhou, X.: *On independence, completeness of Maxwell's equations and uniqueness theorems in electromagnetics*. Progress In Electromagnetics Research **64**, 117–134 (2006)

Anexos

A1. Código SINGULAR

Presentamos aquí as liñas de código de SINGULAR que empregamos para realizar os cálculos do Exemplo 4.23. Recordemos que se trataba do sistema linear $R\eta = 0$, onde R é a seguinte matriz:

$$R = \begin{pmatrix} \partial_t & 0 & 0 & 0 & -\partial_3 & \partial_2 \\ 0 & \partial_t & 0 & \partial_3 & 0 & -\partial_1 \\ 0 & 0 & \partial_t & -\partial_2 & \partial_1 & 0 \\ \partial_1 & \partial_2 & \partial_3 & 0 & 0 & 0 \end{pmatrix} \in D^{4\times 6},$$

e D o anel de operadores diferenciais conmutativo $D = \mathbb{R}[\partial_t, \partial_1, \partial_2, \partial_3]$.

O primeiro que temos que facer en SINGULAR é introducir o anel de polinomios sobre o que se van realizar os cálculos de bases de Gröbner. Para iso basta executar a seguinte liña de código.

```
1 ring D=0,(dt,d1,d2,d3),lp;
```

Co primeiro dos argumentos de `ring` indicamos que imos traballar sobre o corpo dos números racionais (o número 0 fai referencia á característica do corpo). A razón de que realicemos os cálculos sobre $\mathbb{Q}$ (e non sobre $\mathbb{R}$, como nos exemplos vistos) é que isto permite traballar dunha maneira totalmente simbólica (noutro caso traballaríase en punto flotante cunha determinada precisión). Veremos que neste caso particular non hai ningunha perda de xeneralidade ao realizar esta simplificación. A continuación debemos indicar as variables do devandito anel, neste caso `(dt,d1,d2,d3)` representa as variables $\partial_t, \partial_1, \partial_2$, e ∂_3, respectivamente. Finalmente, tamén temos que indicar a orde que se toma no anel de polinomios, neste caso escollemos a lexicográfica (`lp`).

Segundo se indica no Exemplo 4.23 precisamos atopar unha matriz $S_2 \in D^{q_2\times 6}$ tal que $\ker(.S_1) = D^{1\times q_2}S_2$, para algún $q_2 \in \mathbb{N}$, onde $S_1 = R$. Seguindo os pasos do Algoritmo 4.7, o primeiro que imos facer é introducir as variables auxiliares $\eta_1, \ldots, \eta_4, \zeta_1, \ldots, \zeta_6$ como os xeradores do D-módulo pola esquerda coas relacións que en (1) do devandito Algoritmo 3.17 se indican, e que a continuación recordamos (tomando aquí $q = 6$ e $p = 4$):

$$\left\{ \sum_{j=1}^{p} R_{ij}\eta_j - \zeta_i \mid i = 1, ..., q \right\}. \tag{A.1}$$

Así pois, as variables $\zeta_1, \ldots, \zeta_6$ correspóndense cos seis primeiros xeradores do módulo `P`, mentres que as variables $\eta_1, \ldots, \eta_4$ correspóndense cos catro últimos xeradores do mesmo módulo. Todo isto, xunto coas relacións de (A.1), indícase co seguinte código.

```
1 module P=[-1,0,0,0,0,0,dt,0,0,d1],[0,-1,0,0,0,0,0,dt,0,d2],
    ↪ [0,0,-1,0,0,0,0,0,dt,d3],[0,0,0,-1,0,0,0,d3,-d2,0],
    ↪ [0,0,0,0,-1,0,-d3,0,d1,0],[0,0,0,0,0,-1,d2,-d1,0,0];
```

A continuación calculamos unha base de Gröbner de P no D-módulo pola esquerda xerado por $\eta_1, \ldots, \eta_4, \zeta_1, \ldots, \zeta_6$:

```
1 std(P);
2 _[1]=d2*gen(9)-d3*gen(8)+gen(4)
```

```
_[2]=d1*gen(4)+d2*gen(5)+d3*gen(6)
_[3]=d1*gen(8)-d2*gen(7)+gen(6)
_[4]=d1*gen(9)-d3*gen(7)-gen(5)
_[5]=dt*gen(4)+d2*gen(3)-d3*gen(2)
_[6]=dt*gen(5)-d1*gen(3)+d3*gen(1)
_[7]=dt*gen(6)+d1*gen(2)-d2*gen(1)
_[8]=dt*gen(7)+d1*gen(10)-gen(1)
_[9]=dt*gen(8)+d2*gen(10)-gen(2)
_[10]=dt*gen(9)+d3*gen(10)-gen(3)
```

Por último, basta realizar a intersección co submódulo xerado por $\zeta_1,\dots,\zeta_6$. Para iso só temos que ter en conta como introducimos as relacións entre os xeradores do módulo P, pois cada compoñente está asociada cunha das variables $\zeta_1,\dots,\zeta_6,\eta_1,\dots,\eta_4$.

```
module PP=[1,0,0,0,0,0,0,0,0,0],[0,1,0,0,0,0,0,0,0,0],
   ↪ [0,0,1,0,0,0,0,0,0,0],[0,0,0,1,0,0,0,0,0,0],
   ↪ [0,0,0,0,1,0,0,0,0,0],[0,0,0,0,0,1,0,0,0,0];
intersect(std(P),PP);
_[1]=d1*gen(4)+d2*gen(5)+d3*gen(6)
_[2]=dt*gen(4)+d2*gen(3)-d3*gen(2)
_[3]=dt*gen(5)-d1*gen(3)+d3*gen(1)
_[4]=dt*gen(6)+d1*gen(2)-d2*gen(1)
```

Da saída obtemos a matriz $S_2 \in D^{4\times 6}$:

$$S_2 = \begin{pmatrix} 0 & 0 & 0 & \partial_1 & \partial_2 & \partial_3 \\ 0 & -\partial_3 & \partial_2 & \partial_t & 0 & 0 \\ \partial_3 & 0 & -\partial_1 & 0 & \partial_t & 0 \\ -\partial_2 & \partial_1 & 0 & 0 & 0 & \partial_t \end{pmatrix}. \tag{A.2}$$

Para o seu cálculo chega con sinalar de novo que `gen(1)`,…,`gen(6)` representa as variables $\zeta_1,\dots,\zeta_6$ e recordar a expresión de $S = S_2$ dada no Algoritmo 3.17, $G \cap (D\zeta_1 \bigoplus \cdots \bigoplus D\zeta_q) = \left\{\sum_{i=1}^{q} S_{ki}\zeta_i \mid k = 1,\dots,q_2\right\}$.

Agora repetimos exactamente o mesmo proceso, pero cambiando a matriz S_1 pola matriz S_2. Obviamos entón os comentarios, e presentamos directamente o código e a saída deste en SINGULAR.

```
module P=[-1,0,0,0,0,0,0,d1,d2,d3],[0,-1,0,0,0,-d3,d2,dt,0,0],
   ↪ [0,0,-1,0,d3,0,-d1,0,dt,0],[0,0,0,-1,-d2,d1,0,0,0,dt];
std(P);
_[1]=d1*gen(8)+d2*gen(9)+d3*gen(10)-gen(1)
_[2]=dt*gen(1)-d1*gen(2)-d2*gen(3)-d3*gen(4)
_[3]=dt*gen(8)+d2*gen(7)-d3*gen(6)-gen(2)
_[4]=dt*gen(9)-d1*gen(7)+d3*gen(5)-gen(3)
_[5]=dt*gen(10)+d1*gen(6)-d2*gen(5)-gen(4)
module PP=[1,0,0,0,0,0,0,0,0,0],[0,1,0,0,0,0,0,0,0,0],
   ↪ [0,0,1,0,0,0,0,0,0,0],[0,0,0,1,0,0,0,0,0,0];
intersect(std(P),PP);
_[1]=dt*gen(1)-d1*gen(2)-d2*gen(3)-d3*gen(4)
```

Obtemos $S_3 = (\partial_t \ -\partial_1 \ -\partial_2 \ -\partial_3) \in D^{1\times 4}$. Repetimos para S_3, e comprobamos que obtemos intersección nula (indicando o fin da resolución libre e finita de N).

```
module P=[-1,dt,-d1,-d2,-d3];
std(P);
_[1]=dt*gen(2)-d1*gen(3)-d2*gen(4)-d3*gen(5)-gen(1)
module PP=[1,0,0,0,0];
intersect(std(P),PP)
_[1]=0
```

A seguinte tarefa a realizar é o cálculo de matrices R'_i tales que $\ker(.S_{i+1}^T) = D^{q'_{i-1}}R'_i$, para $i = 1, 2$, tal e como se indica no Exemplo 4.23. Seguimos tamén o mesmo procedemento, e daquela presentamos directamente o cálculo para as dúas matrices.

```
module P1=[-1,0,0,0,0,0,0,0,d3,-d2],[0,-1,0,0,0,0,0,-d3,0,d1],
   ↪ [0,0,-1,0,0,0,0,d2,-d1,0],[0,0,0,-1,0,0,d1,dt,0,0],
   ↪ [0,0,0,0,-1,0,d2,0,dt,0],[0,0,0,0,0,-1,d3,0,0,dt];
module PP1=[1,0,0,0,0,0,0,0,0,0],[0,1,0,0,0,0,0,0,0,0],
   ↪ [0,0,1,0,0,0,0,0,0,0],[0,0,0,1,0,0,0,0,0,0],
   ↪ [0,0,0,0,1,0,0,0,0,0],[0,0,0,0,0,1,0,0,0,0];
intersect(std(P1),PP1);
_[1]=d1*gen(1)+d2*gen(2)+d3*gen(3)
_[2]=dt*gen(1)+d2*gen(6)-d3*gen(5)
_[3]=dt*gen(2)-d1*gen(6)+d3*gen(4)
_[4]=dt*gen(3)+d1*gen(5)-d2*gen(4)
module P2=[-1,0,0,0,dt],[0,-1,0,0,-d1],[0,0,-1,0,-d2],[0,0,0,-1,-d3
   ↪ ];
module PP2=[1,0,0,0,0],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0];
intersect(std(P2),PP2);
_[1]=d2*gen(4)-d3*gen(3)
_[2]=d1*gen(3)-d2*gen(2)
_[3]=d1*gen(4)-d3*gen(2)
_[4]=dt*gen(2)+d1*gen(1)
_[5]=dt*gen(3)+d2*gen(1)
_[6]=dt*gen(4)+d3*gen(1)
```

Utilizando a saída de SINGULAR xa podemos obter as matrices R'_1 e R'_2:

$$R'_1 = \begin{pmatrix} \partial_1 & \partial_2 & \partial_3 & 0 & 0 & 0 \\ \partial_t & 0 & 0 & 0 & -\partial_3 & \partial_2 \\ 0 & \partial_t & 0 & \partial_3 & 0 & -\partial_1 \\ 0 & 0 & \partial_t & -\partial_2 & \partial_1 & 0 \end{pmatrix} \in D^{4\times 6},\ R'_2 = \begin{pmatrix} 0 & 0 & -\partial_3 & \partial_2 \\ 0 & -\partial_2 & \partial_1 & 0 \\ 0 & -\partial_3 & 0 & \partial_1 \\ \partial_1 & \partial_t & 0 & 0 \\ \partial_2 & 0 & \partial_t & 0 \\ \partial_3 & 0 & 0 & \partial_t \end{pmatrix} \in D^{6\times 4}. \tag{A.3}$$