Métodos Algebraicos y Efectivos en Grupos Cuánticos.

Fco. Javier Lobillo Borrero

Universidad de Granada

Métodos Algebraicos y Efectivos en Grupos Cuánticos.

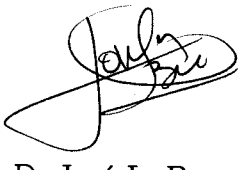
Métodos Algebraicos y Efectivos en Grupos Cuánticos.

Fco. Javier Lobillo Borrero

Universidad de Granada

Memoria realizada en el Departemento de Álgebra de la Universidad de Granada bajo la dirección de los doctores Dr. D. José Luis Bueso Montero y Dr. D. José Gómez Torrecillas para la obtención del grado de Doctor en Ciencias Matemáticas por la Universidad de Granada.

V. B. El Director

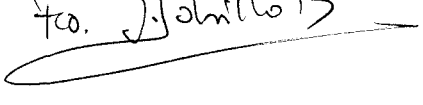


Dr. D. José L. Bueso Montero

V. B. El Director

Dr. D. José Gómez Torrecillas

El aspirante



Fco. Javier Lobillo Borrero

Introducción.

Existe una gran variedad de teorías matemáticas abstractas relevantes para la Física Matemática. En la década de los 80, ciertas estructuras algebraicas de complejidad considerable han resultado importantes en el contexto de la Teoría cuántica. Estos son los llamados grupos cuánticos, cuya motivación y ejemplos provienen del estudio de sistemas integrables cuánticos [22, 36, 23].

Existen distintos aspectos de la teoría algebraica de grupos cuánticos; dos de los más relevantes son los siguientes. De una parte, los grupos cuánticos han sido estudiados en tanto que álgebras de Hopf, es decir, álgebras en general no conmutativas enriquecidas con una estructura compatible de coálgebra. Algunas referencias pertinentes aquí son [57, 76, 53, 55, 40, 54, 20]. Otra aproximación es considerar un grupo cuántico como un álgebra cuadrática. Este es el punto de vista desarrollado sistemáticamente por Yu I. Manin [57], y está basado en la siguiente observación. Supongamos que cuantizamos el plano de fases, imponiendo a las coordenadas la relación de conmutación $YX = qXY$, donde $q = e^{\hbar}$. Es decir, estas son las relaciones de conmutación de Heisemberg en versión integrada. En tal caso, el grupo ordinario de simetrías del plano, $GL(2)$, queda inservible. Pero esta simetría rota queda restaurada si se imponen ciertas relaciones de conmutación no triviales sobre las entradas de las matrices de orden 2. Así se llega a la noción de matriz cuántica. De hecho, lo que se construye no es un grupo, sino el álgebra de coordenadas cuánticas $\mathcal{O}_q(GL(2))$ del grupo lineal general de orden 2 como una localización del álgebra de coordenadas cuánticas $\mathcal{O}_q(M_2(\Bbbk))$ de las matrices cuadradas de orden 2. El procedimiento es considerar el álgebra libre sobre cuatro variables y construir $\mathcal{O}_q(M_2(\Bbbk))$ como el álgebra no conmutativa cociente de aquella mediante un ideal bilátero generado por ciertas relaciones cuadráticas. De esta manera, se consigue que esta nueva álgebra no conmutativa actue sobre el plano cuántico, de manera análoga a como el álgebra conmutativa de funciones polinómicas sobre las matrices actua sobre el plano usual. Una propiedad relevante de esta aproximación es su generalidad. Así, partiendo de un espacio no conmutativo definido por ciertas relaciones, usualmente cuadráticas, sobre sus coordenadas no conmutativas, se obtiene un "semigrupo lineal general" y, tras localización, un "grupo lineal general" que actua sobre el espacio original. El primer objeto vuelve a ser un algebra definida como cociente del algebra libre por ciertas relaciones, y el segundo, el "grupo cuántico" es obtenido mediante localización. Además, esta localización se puede obtener mediante la adjunción de nuevas variables y nuevas relaciones mediante el uso de "determinantes cuánticos".

Así, una buena forma de entender qué es un grupo cuántico es considerarlo como la estructura algebraica que modela la geometría de un espacio

no commutativo. Esta idea, lejos de ser una mera motivación, es una línea fundamental de investigación en grupos cuánticos (referencias básicas aquí son las monografías de Manin para la Geometría Algebraica [57] y de Connes para la Geometría Diferencial [18]). La idea es la siguiente: Un álgebra afín commutativa es el anillo de funciones regulares sobre una variedad algebraica (la versión de este hecho en Análisis abstracto es el Teorema de Gelfand–Naimark, que reconoce toda álgebra de Banach conmutativa como el álgebra de las funciones continuas sobre cierto espacio topológico). Desde este punto de vista, un álgebra afín no conmutativa debe contener la información geométrica de un espacio no conmutativo. Nuestro punto de vista es el algebro-geométrico. Dado que, en contraste con el caso commutativo, los ideales biláteros pueden no ser suficientes para soportar un estudio geométrico no commutativo (piénsese en las álgebras de Weyl), hemos de sustituir éstos por alguna otra noción. Aparece así naturalmente la necesidad de estudiar las representaciones del álgebra, esto es, sus módulos. Este punto de vista ha sido recientemente desarrollado por Alexander Rosenberg [71]. Reseñemos no obstante que esto no implica que la información dada por los ideales biláteros sea desdeñable en algunos casos [38].

Una vez descrito brevemente el marco teórico general en que encuadrar esta memoria, pasamos a especificar algunos aspectos. Desde el punto de vista algorítmico, el primer problema que se plantea es disponer de una buena representación de los elementos. Una propiedad común a muchos ejemplos relevantes de grupos cuánticos es que verifican un "Teorema de Poincaré-Birkoff-Witt" en el sentido de que poseen una base formada por monomios estándar, es decir, los elementos del álgebra se pueden expresar de manera única como polinomios en un número finito de variables [82, 50, 70, 5]. El modelo clásico aquí son las álgebras envolventes de álgebras de Lie de dimensión finita y las álgebras de Weyl. Y, por supuesto, los anillos de polinomios conmutativos en un número finito de variables.

Existen precedentes del estudio de métodos computacionales para álgebras no conmutativas. Un punto de vista bastante general es el desarrollado por Teo Mora [61, 64, 62, 63, 65]. En estos trabajos se aborda el estudio de bases de Gröbner y se construyen procedimientos para su cálculo, análogos al algoritmo de Buchberger. Estos procedimientos no llegan a ser algoritmos , es decir, no se puede garantizar que terminen en un número finito de pasos, ya que las álgebras consideradas no son noetherianas en general. Como los grupos cuánticos son, usualmente, dominios noetherianos, usamos estas riqueza estructural para el desarrollo más nítido de los algoritmos básicos en el tratamiento de ideales. La idea clave es asignar a cada elemento del grupo cuántico un exponente que permite medir su tamaño con respecto de un orden admisible en $\mathbb{N}^p$. Surge así la noción de álgebra de Poincaré-Birkhoff-

Witt (ver [29]). Este planteamiento subyace, no explícitamente, en la noción de álgebra de polinomios solubles de Kandri-Rody y Weispfenning [39].

Para finalizar la introducción vamos a resumir brevemente el contenido de cada capítulo. En el capítulo primero recordamos algunos de los resultados más relevantes sobre el semigrupo $\mathbb{N}^p$, su estructura aditiva y distintos órdenes compatibles con la estructura aditiva. Además son definidos algunos ejemplos de los órdenes citados anteriormente, especialmente órdenes lexicográficos simples y graduados. También se incluye los primeros conceptos sobre ideales primos no conmutativos, así como la localización no conmutativa con respecto a conjuntos de Ore.

En el segundo capítulo comenzamos el desarrollo de las herramientas que se emplearan posteriormente. Se definen las llamadas álgebras de tipo PBW, y las bases de Gröbner para ideales de dichas álgebras. Se desarrollan los algoritmos de la división (fuerte y débil) y de Buchberger para el cálculo de bases de Gröbner de ideales a izquierda (o derecha) y biláteros. Se proporcionan las primeras aplicaciones del concepto de base de Gröbner, como la solución al problema de la pertenencia de un elemento a un ideal (izquierda, derecha o bilátero) dado por un sistema de generadores, cálculo de un conjunto de generadores de la intersección de dos ideales dados mediante generadores. También se estudia el problema de la eliminación de variables en extensiones de Ore.

El capítulo tres aborda el estudio efectivo de los módulos finitamente generados sobre un álgebra de tipo PBW. Se desarrollan los conceptos de base de Gröbner y los algoritmos que las acompañan para submódulos a izquierda (o derecha) de un módulo libre sobre un álgebra de tipo PBW. Se incluye el cálculo de sistemas de generadores de módulos de sicigias, los cuales nos permiten rehacer algunas de las aplicaciones vistas en el capítulo dos, como la intersección de submódulos desde un nuevo punto de vista. Además, las sicigias permiten calcular presentaciones de módulos, núcleos de homomorfismos, anuladores y transportadores. Una aplicación algo más elaborada incluida en este capítulo es el cálculo de $\mathrm{Ext}^i_R(M, R/I)$ con I un ideal bilátero de un álgebra de tipo PBW R. Se incluyen por último algunas cuestiones sobre realizar de manera efectiva las operaciones habituales en anillos de fracciones, suma, producto y cálculo de inversos. Esta última parte se usará en el capítulo siguiente.

El capítulo cuarto está dedicado a los ideales primos. Consta fundamentalmente de dos partes. La primera contiene el test de primalidad en extensiones iteradas de Ore. Se estudia por separado aquellos elementos que integran el test, incidiendo en aquellos que lo separan del test conmutativo de [26]. La segunda parte proporciona un método para calcular los primos minimales sobre un ideal bilátero dado en álgebras de operadores diferenciales.

Este cálculo permite calcular el radical de un ideal dado en conjunción con la intersección de ideales estudiada en los capítulos anteriores. Finalmente proporcionamos un método basado en técnicas de álgebra lineal para calcular el radical de un ideal cero–dimensional sin calcular sus primos minimales.

El quinto y último capítulo se ocupa del cálculo de la dimensión de Gelfand–Kirillov. Consiste en dar primero un método para calcular la dimensión de un monoideal para luego relacionar la dimensión de un ideal dado con la de su exponente. Es necesario que el orden considerado tenga condiciones de finitud, lo que se consigue con las casi–graduaciones.

Quiero expresar mi más sicero agradecimiento a los directores de esta Memoria, Dr. D. José Luis Bueso Montero y Dr. D. José Gómez Torrecillas, por su inapreciable ayuda y estímulo a lo largo de estos años, así como por la gran cantidad de enseñanzas recibidas. Este agradecimiento debe hacerse extensivo al Departamento de Álgebra de la Universidad de Granada, por poner a mi disposición todos sus medios humanos y materiales.

Aún a riesgo de olvidar a personas que han tenido relación directa o indirecta en la realización de esta Memoria, quiero citar expresamente a Dr. D. Francisco Jesús Castro Jiménez por haber ido siguiendo su desarrollo desde el principio, así como por sus valiosísimas sugerencias. Con él al Depratamento de Álgebra, Computación, Geometría y Topología de la Universidad de Sevilla, por numerosas visitas siempre agradables. También a las siguientes universidades: University of Wisconsin–Milwaukee, Universiteit Antwerpen, Universidad de Cantabria y Université d'Artois. En todas ellas he pasado momentos inolvidables durante el desarrollo de esta Memoria, especialmente a los profesores Mark L. Teply, Freddy Van Oystaeyen, Alain Verschoren, Laureano González Vega y André Leroy.

A mi familia: mi padre, mi madre, mi hermana y mi tata, por su constante apoyo y presencia. Y por supuesto a Eloisa María Olmedo Torres. Aún no sé como ha podido soportarme durante estos años.

ÍNDICE GENERAL

Introducción. vii

Índice General xii

1. Preliminares 1
1.1 Sobre $\mathbb{N}^p$. 1
1.1.1 Ordenes admisibles. 1
1.1.2 Monoideales. 2
1.1.3 Subconjuntos Estables. 4
1.1.4 Ordenes sobre subconjuntos estables. 5
1.1.5 Ordenes casi–graduados. 6
1.2 Sobre ideales primos. 7
1.2.1 Anillo de fraciones. 8
1.2.2 Extensiones de Ore. 9

2. Algebras de tipo Poincaré–Birkoff-Witt 11
2.1 Definición y primeros ejemplos. 11
2.2 Bases de Gröbner. 18
2.3 Algoritmo de la división. 20
2.4 Primeras aplicaciones. 27
2.5 Bases de Gröbner reducidas. 33
2.6 Cálculo de bases de Gröbner. 35

3. Módulos sobre álgebras de tipo PBW. 47
3.1 Bases de Gröbner para submódulos de R^n. 47
3.2 División y algoritmo de Buchberger para módulos. 50
3.3 Módulo de sicigias. 54
3.4 Aplicaciones del módulo de sicigias. 60
3.4.1 Presentación de módulos. 60
3.4.2 Intersección de submódulos. 62
3.4.3 Cálculo de $\mathrm{Hom}(M, R/I)$ y $\mathrm{Ext}^n(M, R/I)$. 63
3.4.4 Transportadores y anuladores. 75

3.5 Anillo de fracciones. Efectividad. 76

4. Ideales Primos. 81
4.1 Extensión y contracción de ideales primos. 81
4.2 Primalidad en $K[x;\sigma,\delta]$. 85
4.3 Contracción de $Q_{cl}(R)$ a R. 86
4.4 Test de primalidad. 89
4.5 Primos minimales y radical. 94
4.6 Ideales 0–dimensionales. 101
4.7 El radical de un ideal 0–dimensional. 102

5. Dimensiones. 107
5.1 Dimensión de subconjuntos estables. 107
5.2 Función de Hilbert. 109
5.3 Dimensión de Gelfand–Kirillov. 112
5.4 Ordenes casi–graduados. 118

1. PRELIMINARES

1.1 Sobre $\mathbb{N}^p$.

1.1.1 Ordenes admisibles.

[1.1]. Vamos a comenzar estableciendo algunos resultados concernientes al semigrupo $\mathbb{N}^p$ y a ordenes compatibles con la estructura de semigrupo. Recordamos que la estructura de semigrupo natural en $\mathbb{N}^p$ viene dada por la suma componente a componente, es decir,

$$(\alpha_1, \ldots, \alpha_p) + (\beta_1, \ldots, \beta_p) = (\alpha_1 + \beta_1, \ldots, \alpha_p + \beta_p).$$

Consideraremos siempre en $\mathbb{N}$ el orden natural, es decir, para cualesquiera $m, n \in \mathbb{N}$ $n \leq m$ si y sólo si $m - n \in \mathbb{N}$. Los resultados de este capítulo serán utilizados en numerosas ocasiones a lo largo de la memoria sin mención explícita.

[1.2]. Un orden total $\leq$ sobre $(\mathbb{N}^p, +)$ se dice admisible si $\mathbf{0} = (0, \ldots, 0)$ es mínimo para $\leq$ y el orden tiene un buen comportamiento aditivo, es decir, para $\alpha, \beta, \gamma \in \mathbb{N}^p$,

$$\text{si } \alpha < \beta \text{ entonces } \alpha + \gamma < \beta + \gamma,$$

donde $\alpha < \beta$ tiene el significado habitual, $\alpha \leq \beta$ y $\alpha \neq \beta$.

Veamos algunos ejemplos:

[1.3]. Ejemplo. Orden lexicográfico. Definimos el siguiente orden en $\mathbb{N}^p$:

$$\alpha \leq \beta \iff \begin{cases} \alpha = \beta & \text{o} \\ \alpha_i < \beta_i & \text{donde } i \text{ es el primer índice en el que } \alpha_i \neq \beta_i. \end{cases}$$

La admisibilidad de este orden es consecuencia inmediata de la admisibilidad del orden natural en $\mathbb{N}$.

Para definir este orden hemos escogido un orden en los índices $\{1, \ldots, p\}$, el orden natural $1 < \cdots < p$. En este caso se suele llamar orden lexicográfico

directo. Cualquier otro orden en los índices proporciona otro nuevo orden lexicográfico, por ejemplo

$$\alpha \leq \beta \iff \begin{cases} \alpha = \beta & \text{o} \\ \alpha_i < \beta_i & \text{donde } i \text{ es el último índice en el que } \alpha_i \neq \beta_i. \end{cases}$$

En este caso el orden en los índices es $p < \cdots < 1$.

Consideremos los elementos $\epsilon_i = (0, \ldots, \overset{i}{1}, \ldots, 0) \in \mathbb{N}^p$. Dar un orden en los índices equivale a ordenar los elementos $\epsilon_1, \ldots, \epsilon_p$. En el primer caso que hemos visto, $\epsilon_1 > \cdots > \epsilon_p$, mientras que en el segundo se obtiene el orden contrario, $\epsilon_1 < \cdots < \epsilon_p$. Este último será el orden lexicográfico más utilizado a lo largo de esta memoria.

[1.4]. Ejemplo. Para cada $\alpha \in \mathbb{N}^p$, definimos el grado de α como

$$|\alpha| = \alpha_1 + \cdots + \alpha_p.$$

Un orden admisible $\leq$ se dice *graduado* si $\alpha \leq \beta$ implica que $|\alpha| \leq |\beta|$. La importancia de los órdenes graduados se verá en el capítulo 5. Si $\leq$ es un orden admisible sobre $\mathbb{N}^p$, hay una forma natural de definir un orden graduado asociado a $\leq$ y que denotaremos $\leq_g$,

$$\alpha \leq_g \beta \iff \begin{cases} |\alpha| < |\beta| & \text{o} \\ |\alpha| = |\beta| \text{ y } \alpha \leq \beta \end{cases}$$

Como caso particular obtenemos los órdenes lexicográficos graduados.

1.1.2 Monoideales.

[1.5]. Un subconjunto $E \subseteq \mathbb{N}^p$ se llama *monoideal* si es invariante por traslaciones, es decir,

$$E + \mathbb{N}^p = \{\alpha + \beta \mid \alpha \in E, \beta \in \mathbb{N}^p\} = E.$$

En la literatura, dichos subconjuntos suelen recibir el nombre de ideales en lugar de monoideales. Nosotros, sin embargo, vamos a limitar el uso del término ideal a aquellos que lo sean de un anillo.

[1.6]. Vamos a incluir algunos resultados clásicos.

Teorema (Lema de Dickson). *Dado cualquier $A \subseteq \mathbb{N}^p$, existen elementos $\alpha^1, \ldots, \alpha^m \in A$ tales que*

$$A \subseteq \bigcup_{i=1}^{m} (\alpha^i + \mathbb{N}^p).$$

Este teorema garantiza la existencia de sistemas de generadores finitos para todo monoideal de $\mathbb{N}^p$. Dicho sistema de generadores se puede refinar aún más:

Teorema. *Todo monoideal de $\mathbb{N}^p$ tiene un único sistema de generadores minimal respecto a la inclusión.*

Utilizando reiteradamente el siguiente resultado, cuya demostración es inmediata, podemos construir un sistema de generadores minimal a partir de un sistema de generadores finito.

[1.7]. Lema. *Si G es un sistema de generadores de un monoideal $E \subseteq \mathbb{N}^p$ y $\alpha \in G$ satisface la siguiente propiedad,*

$$\alpha \in \bigcup_{\beta \in G \setminus \{\alpha\}} (\beta + \mathbb{N}^p),$$

entonces $G \setminus \{\alpha\}$ es un sistema de generadores para E.

Algunas de las aplicaciones del lema de Dickson son las siguientes:

[1.8]. Proposición. *$\mathbb{N}^p$ satisface la condición de cadena ascendente para monoideales.*

Demostración. Sea $E_0 \subseteq E_1 \subseteq \cdots \subseteq E_i \subseteq \cdots$ una cadena ascendente de monoideales. Entonces $E = \bigcup_{i=1}^{\infty} E_i$ es un monoideal que por el lema de Dickson tiene un conjunto finito de generadores, llamémoslo A. Es claro que existe $n \in \mathbb{N}$ tal que $A \subseteq E_n$ y para dicho natural, $E_n \subseteq E = A + \mathbb{N}^p \subseteq E_n$, lo que prueba que la cadena estaciona a partir de E_n. □

[1.9]. Proposición. *Todo orden admisible $\leq$ sobre $\mathbb{N}^p$ es un buen orden.*

Demostración. Sea $S \subseteq \mathbb{N}^p$. Por el lema de Dickson [1.6] podemos encontrar un subconjunto finito de elementos $\alpha^1, \ldots, \alpha^m \in S$ tales que

$$S \subseteq \bigcup_{i=1}^{m} (\alpha^i + \mathbb{N}^p).$$

Dado que $\leq$ es un orden total, podemos suponer que $\alpha^1 \leq \alpha^2 \leq \cdots \leq \alpha^m$. Vamos a demostrar que α^1 es el mínimo de S. Sea $\beta \in S$. Entonces existen $i \in \{1, \ldots, m\}$ y $\gamma \in \mathbb{N}^p$ tales que $\beta = \alpha^i + \gamma$. Entonces $\alpha^1 \leq \alpha^i \leq \alpha^i + \gamma = \beta$, como queríamos. □

[1.10]. Teorema (Inducción noetheriana.). *Sea $\leq$ un orden admisible sobre $\mathbb{N}^p$. Sea $A \subseteq \mathbb{N}^p$, un subconjunto que satisface las propiedades siguientes:*

(a) $\mathbf{0} \in A$.

(b) Si $M(\alpha) = \{\beta \in \mathbb{N}^p \mid \beta < \alpha\} \subseteq A$ *entonces* $\alpha \in A$.

Entonces $A = \mathbb{N}^p$.

Demostración. Es claro que A es no vacío. Supongamos que $B = \mathbb{N}^p \setminus A$ es no vacío. Por [1.9] existe un mínimo $\beta \in B$. La minimalidad de β implica que $M(\beta) \cap B = \varnothing$, y como $\beta \neq \mathbf{0}$, tenemos que $M(\beta) \neq \varnothing$. Por tanto $M(\beta) \subseteq A$, lo que implica que $\beta \in A$, pero eso es imposible porque $\beta \in B$. Necesariamente $B = \varnothing$. □

1.1.3 Subconjuntos Estables.

Con la vista puesta en no sólo estudiar de manerta efectiva ciertos anillos, sino también sus módulos finitamente generados, necesitamos estudiar ciertos órdenes y subconjuntos sobre $\mathbb{N}^p \times \{1, \ldots, n\} = \mathbb{N}^{p,n}$. Su utilidad se verá en el capítulo 3. Hay una acción natural de $\mathbb{N}^p$ sobre $\mathbb{N}^{p,n}$:

$$\begin{aligned} + : \mathbb{N}^p \times \mathbb{N}^{p,n} &\longrightarrow \mathbb{N}^{p,n} \\ \alpha, (\beta, i) &\longmapsto \alpha + (\beta, i) = (\alpha + \beta, i). \end{aligned}$$

[1.11]. Un subconjunto $E \subseteq \mathbb{N}^{p,n}$ se dice *estable* si $E + \mathbb{N}^p = E$. En el caso $n = 1$ los conjuntos estables coinciden con los monoideales. Decimos que E está generado por G si $E = G + \mathbb{N}^p$. Hay una relación muy estrecha entre monoideales y subconjuntos estables. Dado que todo subconjunto (estable o no) $S \subseteq \mathbb{N}^{p,n}$ se puede escribir como la siguiente unión disjunta,

$$S = \biguplus_{i=1}^{n} \left(S_i + (\mathbf{0}, i)\right), \quad S_i = \{\alpha \in \mathbb{N}^p \mid (\alpha, i) \in S\},$$

obtenemos el siguiente lema:

[1.12]. Lema.

[1.12.1]. *E es estable si y sólo si para cada $1 \leq i \leq n$, E_i es un monoideal o $E_i = \varnothing$.*

[1.12.2]. *G es un conjunto de generadores para E si y sólo si G_i es un conjunto de generadores de E_i para todo $1 \leq i \leq n$.*

Demostración. Inmediata. □

[1.13]. Proposición.

[1.13.1]. *Dado cualquier $S \subseteq \mathbb{N}^{p,n}$, existen $\mathfrak{a}^1, \ldots, \mathfrak{a}^m \in S$ tales que*

$$S \subseteq \bigcup_{i=1}^{m} (\mathfrak{a}^i + \mathbb{N}^p).$$

[1.13.2]. *Todo conjunto estable E tiene un único sistema minimal de generadores.*

[1.13.3]. *Si G es un sistema de generadores de un conjunto estable $E \subseteq \mathbb{N}^{p,n}$ y $\mathfrak{a} \in G$ satisface la siguiente propiedad,*

$$\mathfrak{a} \in \bigcup_{\mathfrak{b} \in G \setminus \{\mathfrak{a}\}} (\mathfrak{b} + \mathbb{N}^p),$$

entonces $G \setminus \{\mathfrak{a}\}$ es un sistema de generadores para E.

Demostración. Dado que $S = \biguplus_{i=1}^{n} (S_i + (\mathbf{0}, i))$, el primer apartado es consecuencia inmediata del Lema de Dickson [1.6].

Sea $G_i = \{\alpha_1^i, \ldots, \alpha_{n_i}^i\}$ un conjunto minimal de generadores de E_i (ver [1.6]); se obtiene fácilmente de [1.12] que el conjunto minimal de generadores de E es

$$G = \bigcup_{i=1}^{n} \{(\alpha_1^i, i), \ldots, (\alpha_{n_i}^i, i)\}.$$

□

1.1.4 Ordenes sobre subconjuntos estables.

[1.14]. Un orden *admisible* sobre $\mathbb{N}^{p,n}$ es un orden total $\preceq$ sobre $\mathbb{N}^{p,n}$ tal que

(i) $\mathfrak{a} \prec \alpha + \mathfrak{a}$ para cualesquiera $\mathfrak{a} \in \mathbb{N}^{p,n}$, $\alpha \in \mathbb{N}^p \setminus \{\mathbf{0}\}$.

(ii) Si $\mathfrak{a} \prec \mathfrak{b}$ entonces $\alpha + \mathfrak{a} \prec \alpha + \mathfrak{b}$ para cualesquiera $\mathfrak{a}, \mathfrak{b} \in \mathbb{N}^{p,n}$, $\alpha \in \mathbb{N}^p$.

Esta definición coincide en el caso $n = 1$ con la definición usual de orden admisible. Además, todo orden admisible $\leq$ sobre $\mathbb{N}^p$ proporciona dos ordenes admisibles sobre $\mathbb{N}^{p,n}$ de forma natural:

[1.14.1]. El orden TOP:

$$(\alpha, i) \preceq (\beta, j) \iff \begin{cases} \alpha < \beta \\ \text{o} \\ \alpha = \beta \text{ y } i \leq j \end{cases} \qquad \text{(TOP)}$$

[1.14.2]. El orden POT:

$$(\alpha, i) \preceq (\beta, j) \iff \begin{cases} i < j \\ \text{o} \\ i = j \text{ y } \alpha \leq \beta \end{cases} \qquad \text{(POT)}$$

Es sencillo comprobar que los ordenes anteriores son admisibles.

[1.15]. Proposición. *Todo orden admisible $\preceq$ sobre $\mathbb{N}^{p,n}$ es un buen orden.*

Demostración. La demostración es análoga a [1.9]. Sea $S \subseteq \mathbb{N}^{p,n}$. Por [1.13] podemos encontrar un subconjunto finito de elementos $\mathfrak{a}_1, \ldots, \mathfrak{a}_m \in S$ tales que

$$S \subseteq \bigcup_{i=1}^{m} (\mathfrak{a}_i + \mathbb{N}^p).$$

Dado que $\preceq$ es un orden total, podemos suponer que $\mathfrak{a}_1 \preceq \mathfrak{a}_2 \preceq \cdots \preceq \mathfrak{a}_m$. Vamos a demostrar que $\mathfrak{a}_1$ es el mínimo de S. Sea $\mathfrak{b} \in S$. Entonces existen $i \in \{1, \ldots, m\}$ y $\gamma \in \mathbb{N}^p$ tales que $\mathfrak{b} = \mathfrak{a}_i + \gamma$. Entonces $\mathfrak{a}_1 \preceq \mathfrak{a}_i \preceq \mathfrak{a}_i + \gamma = \mathfrak{b}$, como queríamos. □

[1.16]. Vamos a extender el concepto de orden graduado dado en [1.4]. Dado $\mathfrak{a} = (\alpha, i) \in \mathbb{N}^{p,n}$, definimos el grado de $\mathfrak{a}$ como

$$|\mathfrak{a}| = |\alpha|.$$

Un orden admisible $\preceq$ sobre $\mathbb{N}^{p,n}$ se dice graduado si $\mathfrak{a} \preceq \mathfrak{b}$ implica $|\mathfrak{a}| \leq |\mathfrak{b}|$.

Dado un orden graduado $\leq$ sobre $\mathbb{N}^p$, el orden TOP definido en $\mathbb{N}^{p,n}$ es también graduado, mientras que el orden POT no lo es (salvo que $n = 1$).

1.1.5 Ordenes casi–graduados.

[1.17]. Sea $\omega \in (\mathbb{R}^+)^p$. En nuestras aplicaciones las entradas de ω estarán usualmente en $\mathbb{N}$. Para cada $\alpha \in \mathbb{N}^p$ pondremos

$$\langle \alpha, \omega \rangle = \alpha_1\omega_1 + \cdots + \alpha_p\omega_p.$$

Con esta definición es inmediato que $|\alpha| = \langle \alpha, (1, \ldots, 1) \rangle$. Análogamente, si $\mathfrak{a} = (\alpha, i) \in \mathbb{N}^{p,n}$ entonces

$$\langle \mathfrak{a}, \omega \rangle = \langle \alpha, \omega \rangle.$$

[1.18]. Diremos que un orden admisible $\preceq$ sobre $\mathbb{N}^{p,n}$ es *casi graduado* si existe un $\omega \in (\mathbb{R}^+)^p$ tal que $\mathfrak{a} \preceq \mathfrak{b}$ implica $\langle \mathfrak{a}, \omega \rangle \leq \langle \mathfrak{b}, \omega \rangle$. En la literatura estos órdenes también suelen recibir el nombre de órdenes graduados con pesos o órdenes pesados. Para el caso $n = 1$ obtenemos el concepto para órdenes admisibles sobre $\mathbb{N}^p$. En particular, todos los ordenes graduados son casi graduados. Veamos algunos ejemplos.

[1.19]. **Ejemplo.** Sea $\leq$ un orden lexicográfico sobre $\mathbb{N}^p$ y sea $\omega \in (\mathbb{R}^+)^p$. El orden

$$\alpha \leq_\omega \beta \iff \begin{cases} \langle \alpha, \omega \rangle < \langle \alpha, \omega \rangle & \text{o} \\ \langle \alpha, \omega \rangle = \langle \alpha, \omega \rangle \text{ y } \alpha \leq \beta \end{cases}$$

es casi graduado sobre $\mathbb{N}^p$. Esta construcción nos da en particular los ordenes lexicográficos casi–graduados, tomando como $\leq$ algún orden lexicográfico.

[1.20]. **Ejemplo.** Sea $\leq$ un orden casi graduado sobre $\mathbb{N}^p$. El orden TOP es de nuevo un orden casi graduado sobre $\mathbb{N}^{p,n}$. El orden POT no lo es salvo en el caso $n = 1$.

1.2 Sobre ideales primos.

[1.21]. Vamos a comenzar dando definiciones de distintos conceptos de ideal primo y semiprimo para álgebras no conmutativas.

[1.21.1]. Un ideal bilátero $P \leq R$ se dice *completamente primo* si para cualesquiera $a, b \in R$, si $ab \in P$ entonces $a \in P$ o $b \in P$.

[1.21.2]. Un ideal bilátero $P \leq R$ se dice *primo* si para cualesquiera ideales $I, J \leq R$, si $IJ \subseteq P$ entonces $I \subseteq P$ o $J \subseteq P$.

[1.21.3]. Un ideal bilátero $P \leq R$ se dice *semiprimo* si para cualquier ideal $I \leq R$, si $I^2 \subseteq P$ entonces $I \subseteq P$.

Hay algunas equivalencias clásicas y cuya demostración es inmediata.

Proposición. *$P \leq R$ es primo si y sólo si $aRb \subseteq P$ implica $a \in P$ o $b \in P$ para elementos $a, b \in R$ cualesquiera.*

Proposición. *Un ideal $P \leq R$ es completamente primo si y sólo si R/P es un dominio.*

Un anillo en el que 0 es un ideal primo (resp. semiprimo) se llama anillo primo (resp. semiprimo), por lo que $P \leq R$ es primo (resp. semiprimo) si y sólo si R/P es un anillo primo (resp. semiprimo).

Es inmediato comprobar que todo ideal completamente primo es primo, y que todo ideal primo es semiprimo. En [4.8] hay un ejemplo de un ideal primo que no es completamente primo. Sin embargo, la siguiente lista de álgebras satisface que todo ideal primo es completamente primo:

1. $U(\mathfrak{g})$ donde $\mathfrak{g}$ es un álgebra de Lie resoluble finito–dimensional. La demostración puede verse en [21, Theorem 3.7.2].

2. Extensiones iteradas de Ore. Demostrado por Sigurdsson en [74, 2.7].

3. $\mathcal{O}_q(\Bbbk^p)$, $\mathcal{O}_q(M_n(\Bbbk))$, $\mathcal{O}_q(GL_n(\Bbbk))$ y $\mathcal{O}_q(SL_n(\Bbbk))$, con q genérico. Dado que q es en este caso una matriz de tamaño n sobre $\mathbb{C}$ multiplicativamente antisimétrica, por q genérico entendemos que el subgrupo de $\mathbb{C}^\times$ generado por los elementos de q es libre de torsión. Ver [31, Theorem 2.3 y Theorem 3.2].

4. $U_q^+(\mathfrak{g})$, donde $\mathfrak{g}$ es un álgebra de Lie semisimple finito–dimensional y q de nuevo genérico (al ser aquí $q \in \mathbb{C}^\times$, genérico significs no raíz de la unidad).

1.2.1 Anillo de fracciones.

La última parte de este capítulo la configuran los anillos de fracciones. Para una buena introducción a los anillos de fracciones ver [13, Chapter I] o [77, Chapter II]. Sea R $\Bbbk$–álgebra. Dado un subconjunto multiplicativamente cerrado $C \subseteq R$, se define el anillo de cocientes a izquierda de R respecto de C como un anillo $C^{-1}R$ junto con un morfismo de anillos $\varphi : A \to C^{-1}R$ tales que

F1. $\varphi(c)$ es invertible para todo $c \in C$.

F2. Todo elemento de $C^{-1}R$ tiene la forma $\varphi(c)^{-1}\varphi(r)$ con $c \in C$.

F3. $\varphi(a) = 0$ si y sólo si $ca = 0$ para algún $c \in C$.

Dados $C \subseteq R$, no existe en general el anillo $C^{-1}R$. La siguiente proposición no solo caracteriza la existencia del anillo de fracciones, sino que nos indica como se realizan las operaciones usuales con ellos.

[1.22]. Proposición. *Sea C un subconjunto multiplicativamente cerrado de R. $C^{-1}R$ existe si y sólo si C satisface*

S1. Si $c \in C$ y $r \in R$ existen $d \in C$ and $s \in R$ tales que $dr = sc$.

S2. Si $rc = 0$ con $c \in C$ entonces $dr = 0$ para algún $d \in C$.

Además, cuando $C^{-1}R$ existe tiene la forma

$$C^{-1}R \cong (C \times R)/\sim$$

donde $\sim$ es la relación de equivalencia definida como $(c,r) \sim (d,s)$ si existen $a,b \in R$ tales que $ac = bd \in C$ y $ar = bs$.

Demostración. Ver [77, Chapter II, Proposition 1.4]. □

Si C satisface S1 y S2 recibe el nombre de conjunto de denominadores a izquierda. La suma y producto en $C^{-1}R$ se realizan de la siguiente forma:

$$\begin{aligned} (c,r)+(d,s) &= (u, ar+bs) \quad \text{donde } u = ac = bd \in C, \\ (c,r)\cdot(d,s) &= (uc, as) \quad \text{donde } ur = ad \text{ y } u \in C. \end{aligned} \tag{1.1}$$

[1.23]. Vamos a restringir nuestra atención al conjunto multiplicativo C_{reg} de los elementos regulares de R. En este caso, para que exista $C_{reg}^{-}1R$ es suficiente que se verifique S1, ya que la propiedad S2 es automáticamente satisfecha. En caso de existir, notaremos $C_{reg}^{-1}R = Q_{cl}(R)$, el anillo clásico de fracciones de R. En el caso noetheriano, satisfacer la condición S1 implica la condición S2, [,]. Si R es noetheriano, el teorema de Goldie [77, Chapter II, Theorem 2.2] garantiza la existencia de $Q_{cl}(R)$ cuando R es un anillo semiprimo. En particular, $Q_{cl}(R/P)$ existe si P es primo o completamente primo.

1.2.2 Extensiones de Ore.

[1.24]. Dada una $\Bbbk$–álgebra R y un automorfismo σ sobre R, una σ–derivación es una aplicación $\Bbbk$–lineal $\delta : R \to R$ tal que $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$. Recordemos que una extensión de Ore de una $\Bbbk$–álgebra R es una extensión S de R que satisface las siguientes condiciones:

1. S es un R–módulo libre a la izquierda con base $\{1, x, x^2, \dots\}$ para algún elemento $x \in S$.

2. Existe un automorfismo de $\Bbbk$–álgebras $\sigma : R \to R$ y una σ–derivación $\Bbbk$–lineal $\delta : R \to R$ tales que $xr = \sigma(r)x + \delta(r)$ para cualquier $r \in R$.

Escribiremos $S = R[x; \sigma, \delta]$. La pareja (σ, δ) se suele llamar *derivación torcida.* Si reiteramos el proceso obtenemos las llamadas extensiones iteradas de Ore, que notaremos $R[x_1; \sigma_1, \delta_1] \cdots [x_p; \sigma_p, \delta_p]$.

[1.25]. Los elementos de una extensión de Ore $R[x;\sigma,\delta]$ se escriben como polinomios en x con coeficientes en R, por lo que tiene sentido definir el grado $\deg(f)$ de un elemento $f \in R[x;\sigma,\delta]$ de la forma habitual. Este grado es aditivo, es decir,

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

para cualesquiera $f, g \in R[x;\sigma,\delta]$ no nulos.

Las extensiones de Ore aparecieron por primera vez en [68]. Posteriormente han sido tratadas en multitud de trabajos. Los ideales primos han sido estudiados entre otros en [29] y [45].

2. ÁLGEBRAS DE TIPO POINCARÉ–BIRKOFF-WITT

2.1 Definición y primeros ejemplos.

A lo largo de este capítulo $\Bbbk$ va a ser un dominio noetheriano conmutativo. Una de las características fundamentales del anillo de polinomios sobre $\Bbbk$ con variables $\{x_1, \ldots, x_p\}$ que lo hacen tratable desde el punto de vista efectivo en la presencia de una $\Bbbk$–base indexada en el semigrupo $\mathbb{N}^p$. Es por ello que vamos a comenzar estudiando $\Bbbk$–álgebras con una $\Bbbk$–base de dichas características. Además, el anillo de polinomios es el enillo de semigrupo sobre $\mathbb{N}^p$, por lo que la estructura multiplicativa de $\Bbbk[x_1, \ldots, x_p]$ se recupera a partir de la estructura aditiva de $\mathbb{N}^p$. Recordemos también que los ordenes admisibles sobre $\mathbb{N}^p$ son lo que mantienen una buena relación con la operación en $\mathbb{N}^p$.

[2.1]. Partamos de una $\Bbbk$–álgebra R libre sobre $\Bbbk$ con base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ y un orden admisible sobre $\mathbb{N}^p$. Como $\mathcal{B}$ es una $\Bbbk$–base de R, cada $f \in R$ tiene una representación única

$$f = \sum_{\alpha \in \mathbb{N}^p} c_{\alpha,f} u_\alpha,$$

es decir, $c_{\alpha,f}$ representa el coeficiente de u_α en la expresión de f respecto de $\mathcal{B}$. El *diagrama de Newton* de f va a ser el conjunto

$$\mathcal{N}(f) = \{\alpha \in \mathbb{N}^p \mid c_{\alpha,f} \neq 0\}$$

Como dicho conjunto es finito podemos definir

$$\exp(f) = \max \mathcal{N}(f) \text{ si } f \neq 0, \quad \exp(0) = -\infty,$$

lo que llamamos *exponente* de f. También llamaremos *coeficiente líder* y *monomio líder* a los elementos

$$\mathrm{lc}(f) = c_{\exp(f),f} \qquad \mathrm{lm}(f) = \mathrm{lc}(f) u_{\exp(f)}$$

[2.2]. Lema. *Sea R una $\Bbbk$-álgebra con $\Bbbk$-base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ y sea $\leq$ un orden admisible sobre $\mathbb{N}^p$.*

[2.2.1]. $\mathcal{N}(f+g) \subseteq \mathcal{N}(f) \cup \mathcal{N}(g)$

[2.2.2]. $\exp(f+g) \leq \max\{\exp(f), \exp(g)\}$, *siendo la desigualdad estricta si y sólo si* $\operatorname{lm}(f) = -\operatorname{lm}(g)$.

Demostración. Inmediata. □

Las condiciones equivalentes de la siguiente proposición son satisfechas por el anillo de polinomios $\Bbbk[x_1, \ldots, x_p]$ por ser el anillo de semigrupo en $\mathbb{N}^p$.

[2.3]. Proposición. *Sea R una $\Bbbk$-álgebra con $\Bbbk$-base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ y sea $\leq$ un orden admisible sobre $\mathbb{N}^p$. Las siguientes afirmaciones son equivalentes:*

[a] $\exp(fg) = \exp(f) + \exp(g)$ *para cualesquiera* $f, g \in R$.

[b] $u_\alpha u_\beta = q_{\alpha,\beta} u_{\alpha+\beta} + \sum_{\gamma<\alpha+\beta} c_\gamma u_\gamma$, *donde* $q_{\alpha,\beta} \in \Bbbk^\times$.

Si se da alguna de las afirmaciones anteriores, entonces

$$\operatorname{lc}(fg) = q_{\exp(f),\exp(g)} \operatorname{lc}(f) \operatorname{lc}(g)$$

Demostración. Es claro que (b) es un caso particular de (a). Por otra parte, supongamos que $u_\alpha u_\beta = q_{\alpha,\beta} u_{\alpha+\beta} + \sum_{\gamma<\alpha+\beta} c_\gamma u_\gamma$ y sean $f = c_1 u_{\alpha_1} + \cdots + c_n u_{\alpha_n}$, $g = d_1 u_{\beta_1} + \cdots + d_m u_{\beta_m}$ con $\alpha_1 < \cdots < \alpha_n$ y $\beta_1 < \cdots < \beta_m$. Entonces

$$fg = \sum_{ij} c_i d_j u_{\alpha_i} u_{\beta_j}.$$

Usando la hipótesis, $\exp(u_{\alpha_i} u_{\beta_j}) = \alpha_i + \beta_j$, y por otra parte, $\alpha_i + \beta_j \leq \alpha_n + \beta_m$, dándose la igualdad sólo en el caso $i = n$, $j = m$. Por el lema [2.2], tenemos que $\exp(fg) = \alpha_n + \beta_m = \exp(f) + \exp(g)$. □

[2.4]. Es precisamente un buen comportamiento del exponente la propiedad fundamental para desarrollar primeras técnicas efectivas. En vista de ello vamos a llamar *álgebra de Poincaré–Birkoff–Witt* o *álgebra de tipo PBW* o *PBW álgebra* a una $\Bbbk$–álgebra R que posee una $\Bbbk$–base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ y un orden admisible $\leq$ que satisface las afirmaciones equivalentes de la proposición [2.3]. En este caso, también diremos que el orden $\leq$ es $\mathcal{B}$–admisible.

Estas álgebras fueron introducidas en [39] con el nombre de anillos de polinomios de tipo resoluble cuando $\Bbbk$ es un cuerpo. Veremos ejemplos en [2.14], [2.15], [2.16] y [2.17]

Toda álgebra de tipo PBW está finitamente generada como álgebra si $\Bbbk$ es un cuerpo.

[2.5]. Lema. *u_0 es una unidad de $\Bbbk$.*

Demostración. Para cualquier $\beta \in \mathbb{N}^p$, $\beta = \exp(u_\beta) = \exp(1u_\beta) = \exp(1)+\beta$, de donde $\exp(1) = \mathbf{0}$. Así $1 = c_0 u_0$ con $c_0 \in \Bbbk \setminus \{0\}$, lo que demuestra el resultado. □

Como consecuencia del lemma anterior, un sencillo cambio de base nos permite suponer que $u_0 = 1$.

[2.6]. Proposición. *Si $q_{\alpha,\beta}$ es una unidad de $\Bbbk$ para toda pareja $\alpha, \beta \in \mathbb{N}^p$, entonces R está generada (como $\Bbbk$–álgebra) por los elementos u_{ϵ_i} para $1 \leq i \leq p$, donde $\epsilon_i = (0, \ldots, \overset{(i)}{1}, \ldots, 0)$.*

Demostración. Es suficiente con demostrar que para cada α, u_α está en la subálgebra generada por los elementos de la forma u_{ϵ_i}. Demostramos esto por inducción sobre α. Si $\alpha = \mathbf{0}$, $u_\alpha \in \Bbbk$ que pertenece a la $\Bbbk$–álgebra generada por los elementos u_{ϵ_i} $1 \leq i \leq p$. Supongamos $\alpha > \mathbf{0}$. Existen $i \in \{1, \ldots, p\}$, $\beta \in \mathbb{N}^p$ tales que $\alpha = \epsilon_i + \beta$. Como $\beta < \alpha$ tenemos

$$u_\alpha = u_{\beta+\epsilon_i} = q^{-1}_{\beta,\epsilon_i} u_\beta u_{\epsilon_i} + \sum_{\gamma<\alpha} c_\gamma u_\gamma.$$

Por hipótesis de inducción tanto u_β como los u_γ estan en la subálgebra generada por los u_{ϵ_j} $1 \leq j \leq p$, por lo que u_α también está en dicha álgebra. □

[2.7]. Antes de ver algunos ejemplos vamos a dar un resultado que proporciona condiciones suficientes para que un álgebra finitamente generada sea un álgebra de tipo PBW

Proposición. *Sea R una $\Bbbk$–álgebra finitamente generada por $\{x_1, \ldots, x_p\}$ y denotemos $X^\alpha = x_1^{\alpha_1} \cdots x_p^{\alpha_p}$ para cualquier $\alpha \in \mathbb{N}^p$. Si existe un orden admisible $\leq$ sobre $\mathbb{N}^p$ tal que*

$$x_j x_i = q_{ji} x_i x_j + \sum_{\gamma<\epsilon_i+\epsilon_j} c_\gamma X^\gamma \tag{2.1}$$

entonces

$$X^\alpha X^\beta = q_{\alpha,\beta} X^{\alpha+\beta} + \sum_{\gamma<\alpha+\beta} c_\gamma X^\gamma$$

Demostración. En esta demostración seguimos [39, Lemma 1.4]. Vamos a proceder por inducción noetheriana sobre $\alpha+\beta$. Si $\alpha=\mathbf{0}$ o $\beta=\mathbf{0}$ entonces el resultado es claro. Si existe un índice $i\in\{1,\dots,p\}$ tal que $\alpha_k=0$ cuando $k>i$ y $\beta_k=0$ cuando $k<i$, entonces

$$X^\alpha X^\beta = x_1^{\alpha_1}\cdots x_i^{\alpha_i}x_i^{\beta_i}\cdots x_p^{\beta_p} = x_1^{\alpha_1}\cdots x_i^{\alpha_i+\beta_i}\cdots x_p^{\beta_p} = X^{\alpha+\beta}$$

Podemos por tanto suponer que $X^\alpha = x_h^{\alpha_h}\cdots x_j^{\alpha_j}$ y $X^\beta = x_i^{\beta_i}\cdots x_k^{\beta_k}$, donde h,i son minimales entre los índices tales que $\alpha_h,\beta_i\neq 0$, j,k maximales para $\alpha_j,\beta_k\neq 0$, e $i<j$. Vamos a estudiar tres casos.

Caso 1. Si $h\leq i$ entonces $X^\alpha = x_h X^{\alpha'}$ con $\alpha'<\alpha$. Por inducción,

$$\begin{aligned} X^\alpha X^\beta &= x_h\underline{X^{\alpha'}X^\beta} \\ &= x_h\big(q_{\alpha',\beta}X^{\alpha'+\beta}+\sum_{\gamma<\alpha'+\beta}c_\gamma X^\gamma\big) \\ &= q_{\alpha',\beta}x_hX^{\alpha'+\beta}+\sum_{\gamma<\alpha'+\beta}c_\gamma\underline{x_hX^\gamma} \\ &= q_{\alpha',\beta}X^{\alpha+\beta}+\sum_{\varrho<\alpha+\beta}d_\varrho X^\varrho \end{aligned}$$

Caso 2. Si $j\leq k$ el resultado se obtiene análogamente al Caso 1.

Caso 3. Supongamos por último que $i<h$ y $k<j$. Obtenemos entonces que $X^\alpha = X^{\alpha'}x_j$ y $X^\beta = x_iX^{\beta'}$. Procedemos a operar:

$$\begin{aligned} X^\alpha X^\beta &= X^{\alpha'}x_jx_iX^{\beta'} \\ &= X^{\alpha'}\big(q_{ji}x_ix_j+\sum_{\gamma<\epsilon_i+\epsilon_j}c_\gamma X^\gamma\big)X^{\beta'} \\ &= q_{ji}X^{\alpha'}x_ix_jX^{\beta'}+\sum_{\gamma<\epsilon_i+\epsilon_j}c_\gamma\underline{X^{\alpha'}X^\gamma X^{\beta'}} \end{aligned}$$

A los sumandos subrayados podemos aplicarles la hipótesis de inducción. El sumando restante, dado que $\alpha'+\epsilon_i<\alpha'+\epsilon_i+\epsilon_j=\alpha+\epsilon_i\leq\alpha+\beta$ y $\beta'+\epsilon_j<\beta'+\epsilon_i+\epsilon_j=\beta+\epsilon_j\leq\alpha+\beta$ podemos aplicar de nuevo el principio de inducción,

$$\begin{aligned} X^{\alpha'}x_ix_jX^{\beta'} &= \big(q_{\alpha',\epsilon_i}X^{\alpha'+\epsilon_i}+\sum_{\varrho<\alpha'+\epsilon_i}c_\varrho X^\varrho\big)\big(q_{\epsilon_j,\beta'}X^{\beta'+\epsilon_j}+\sum_{\varphi<\beta'+\epsilon_j}c_\varphi X^\varphi\big) \\ &= q_{\alpha',\epsilon_i}q_{\epsilon_j,\beta'}X^{\epsilon_i+\alpha'}X^{\beta'+\epsilon_j}+\sum_{\varrho<\alpha'+\epsilon_i}d_\varrho\underline{X^\varrho X^{\beta'+\epsilon_j}} \\ &\quad+\sum_{\varphi<\beta'+\epsilon_j}d_\varphi\underline{X^{\alpha'+\epsilon_i}X^\varphi}+\sum_{\substack{\varrho<\alpha'+\epsilon_i\\ \varphi<\beta'+\epsilon_j}}c_\varrho c_\varphi\underline{X^\varrho X^\varphi} \end{aligned}$$

Una vez más los sumandos subrayados se razonan por inducción. El restante,

$$\begin{aligned} X^{\epsilon_i+\alpha'}X^{\beta'+\epsilon_j} &= x_iX^{\alpha'}X^{\beta'}x_j \\ &= x_i\big(q_{\alpha',\beta'}X^{\alpha'+\beta'} + \sum_{\psi<\alpha'+\beta'} c_\psi X^\psi\big)x_j \\ &= q_{\alpha',\beta'}x_iX^{\alpha'+\beta'}x_j + \sum_{\psi<\alpha'+\beta'} c_\psi \underline{x_iX^\psi x_j} \end{aligned}$$

Para los términos subrayados aplicamos de nuevo el principio de inducción. El primer sumando, dado que

$$X^{\alpha'+\beta'} = x_i^{\alpha_i-1+\beta_i}x_{i+1}^{\alpha_{i+1}+\beta_{i+1}}\dots x_{j-1}^{\alpha_{j-1}+\beta_{j-1}}x_j^{\alpha_j+\beta_j-1},$$

entonces

$$x_iX^{\alpha'+\beta'}x_j = X^{\epsilon_i+\alpha'+\beta'+\epsilon_j} = X^{\alpha+\beta}$$

La fórmula anterior completa la demostración. □

[2.8]. Corolario. *En las hipótesis de la proposición anterior, el conjunto* $\{X^\alpha \mid \alpha \in \mathbb{N}^p\}$ *es un sistema de generadores del* $\Bbbk$*–módulo* R.

[2.9]. Corolario. *Sea* R *una* $\Bbbk$*–álgebra generada por* $\{x_1,\dots,x_p\}$ *y supongamos que* $\mathcal{B} = \{X^\alpha \mid \alpha \in \mathbb{N}^p\}$ *es una* $\Bbbk$*–base de* R. *Sea además* $\leq$ *un orden admisible sobre* $\mathbb{N}^p$. *Las siguientes afirmaciones son equivalentes:*

[a] $x_jx_i = q_{ji}x_ix_j + \sum_{\gamma<\epsilon_i+\epsilon_j} c_\gamma X^\gamma$ *donde* $q_{ji} \neq 0$.

[b] $X^\alpha X^\beta = q_{\alpha,\beta}X^{\alpha+\beta} + \sum_{\gamma<\alpha+\beta} c_\gamma X^\gamma$ *donde* $q_{\alpha,\beta} \neq 0$.

[c] R *es una PBW algebra.*

Demostración. Consecuencia directa de [2.3] y [2.7] □

La proposición [2.7] no nos asegura que el conjunto $\{X^\alpha \mid \alpha \in \mathbb{N}^p\}$ es linealmente independiente. De hecho, cualquier $\Bbbk$–álgebra conmutativa de $\Bbbk$–dimensión finita distinta de $\Bbbk$ nos sirve como contraejemplo. En cualquier caso, podemos dar también un ejemplo propio no conmutativo.

[2.10]. Ejemplo. Para un cuerpo $\Bbbk$ de característica distinta de 2, sea R la $\Bbbk$–álgebra generada por x, y, z con relaciones $zy = yz + x$, $zx = -xz - y$, $yx = xy + z$. Entonces

$$\begin{aligned} zyx &= (yz+x)x = yzx + x^2 = y(-xz-y) + x^2 \\ &= -yxz - y^2 + x^2 = -(xy+z)z - y^2 + x^2 = -xyz + x^2 - y^2 - z^2 \end{aligned}$$

$$zyx = z(xy + z) = zxy + z^2 = (-xz - y)y + z^2$$
$$= -xzy - y^2 + z^2 = -x(yz + x) - y^2 + z^2 = -xyz - x^2 - y^2 + z^2$$

de donde $x^2 - z^2 = 0$. Observemos que los generadores están en las condiciones de [2.7] para cualquier orden graduado sobre $\mathbb{N}^3$.

Sin embargo, una vez garantizado que $\{X^\alpha \mid \alpha \in \mathbb{N}^p\}$ es una $\Bbbk$–base nos basta con comprobar la fórmula (2.1) para comprobar que nuestra álgebra es de tipo PBW. Con este fin vamos a introducir el concepto de extensión de Ore.

[2.11]. Supongamos que R es un $\Bbbk$–módulo libre con base $\mathcal{B}$. Dado que $R[x;\sigma,\delta]$ es libre como R–módulo a izquierda, es ciertamente inmediato comprobar que el conjunto $\mathcal{B}' = \{ux^n \mid u \in \mathcal{B}, n \in \mathbb{N}\}$ es una $\Bbbk$–base. En particular, si $R = \Bbbk[x_1;\sigma_1,\delta_1]\cdots[x_p;\sigma_p,\delta_p]$ entonces el conjunto $\mathcal{B} = \{X^\alpha = x_1^{\alpha_1}\cdots x_p^{\alpha_p} \mid \alpha \in \mathbb{N}^p\}$ es una $\Bbbk$–base de R.

[2.12]. Proposición. *Sea $R = \Bbbk[x_1;\sigma_1,\delta_1]\cdots[x_p;\sigma_p,\delta_p]$ una extensión iterada de Ore, $\mathcal{B} = \{X^\alpha = x_1^{\alpha_1}\cdots x_p^{\alpha_p} \mid \alpha \in \mathbb{N}^p\}$ la $\Bbbk$–base anterior y supongamos que para cada pareja $j < i$ tenemos $\sigma_i(x_j) = q_{ji}x_j + \sum_{\gamma<\epsilon_j} c_\gamma X^\gamma$ donde $q_{ji} \neq 0$. Entonces el orden lexicográfico en $\mathbb{N}^p$ con $\epsilon_p > \epsilon_{p-1} > \cdots > \epsilon_1$ es un orden $\mathcal{B}$–admisible. Por tanto R es un álgebra de tipo PBW.*

Demostración. Consecuencia inmediata de [2.7] y [2.11]. □

[2.13]. La proposición [2.12] también es consecuencia de un resultado algo más general. Supongamos que R es una PBW álgebra con respecto a la base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ y al orden $\leq$. Un automorfismo $\sigma : R \to R$ se dice $\mathcal{B}$–compatible si

$$\sigma(u_\alpha) = k_\alpha u_\alpha + \sum_{\gamma<\alpha} c_\gamma u_\gamma$$

con $k_\alpha \neq 0$. Sea $S = R[x;\sigma,\delta]$ una extensión de Ore en la que σ es $\mathcal{B}$–compatible. Recordemos que $\mathcal{B}' = \{u_\alpha x^n \mid \alpha \in \mathbb{N}^p, n \in \mathbb{N}\}$ es una $\Bbbk$–base para $R[x;\sigma,\delta]$. Definimos el orden $\preceq$ en $\mathbb{N}^p \times \mathbb{N}$ mediante

$$(\alpha,n) \preceq (\beta,m) \iff \begin{cases} n < m & \text{o} \\ n = m \text{ y } \alpha \leq \beta \end{cases}$$

Proposición. *El orden $\preceq$ es $\mathcal{B}'$–admisible.*

Demostración. Para empezar, dotamos a S de la filtración $F_nS = \sum_{k<n} Rx^k$. El anillo graduado asociado a S es $G(S) = R[y;\sigma]$, donde $y = x + F_0S$ [58, página 28]. Un sencillo argumento de inducción demuestra que

$$\sigma^n(u_\beta) = k_\beta^n u_\beta + \sum_{\gamma<\beta} d_\gamma u_\gamma.$$

Para cualesquiera $(\alpha, n), (\beta, m) \in \mathbb{N}^{p+1}$, tenemos

$$\begin{aligned} u_\alpha y^n u_\beta y^m &= u_\alpha \sigma^n(u_\beta) y^{n+m} \\ &= k_\beta^n u_\alpha u_\beta y^{n+m} + \sum_{\gamma<\beta} d_\gamma u_\gamma y^{n+m}. \end{aligned}$$

Como la imagen de $u_\alpha x^n u_\beta x^m$ en $G(S)$ es $u_\alpha y^n u_\beta y^m$, tenemos que

$$u_\alpha x^n u_\beta x^m = k_\beta^n u_\alpha u_\beta x^{n+m} + \sum_{\gamma<\beta} d_\gamma u_\gamma x^{n+m} + r,$$

donde $r \in F_{n+m-1}S$. Esta última fórmula demuestra la proposición. □

Vamos a acabar con algunos ejemplos.

[2.14]. Ejemplo. Si $R = \Bbbk[X]$ con $X = \{x_1, \ldots, x_p\}$, cualquier orden admisible convierte a R en un álgebra de tipo PBW. El anillo de coordenadas cuántico del espacio afín n–dimensional sobre $\Bbbk$, $R = \mathcal{O}_q(\Bbbk^p)$, es otro ejemplo en el que podemos considerar cualquier orden admisible. R es el álgebra generada por $\{x_1, \ldots, x_p\}$ y relaciones $x_ix_j = q_{ij}x_jx_i$, donde $q_{ij} = q_{ji}^{-1}$. Podemos dotar a R de estructura de extensión iterada de Ore:

$$R = \Bbbk[x_1][x_2;\sigma_2]\cdots[x_p;\sigma_p],$$

donde $\sigma_i(x_j) = q_{ij}x_j$ para $i > j$.

[2.15]. Ejemplo. Un ejemplo clásico es el álgebra envolvente de un álgebra de Lie finito–dimensional. La base viene dada por el teorema de Poincaré–Birkoff-Witt para álgebras envolventes de álgebras de Lie finitodimensionales, véase por ejemplo [21, Chapter 2]. Cualquier orden graduado convierte a dichas álgebras en álgebras de tipo PBW. Para definición de orden graduado véase [1.4].

[2.16]. Ejemplo. Las álgebras de coordenadas cuánticas $\mathcal{O}_q(M_n(\Bbbk))$ de matrices $n \times n$ sobre un cuerpo $\Bbbk$ son una extensión iterada de Ore, como fue observado en [3]. Podemos aplicarles la proposición [2.12]. De hecho este álgebra es un caso especial del álgebra $H(p, \lambda)$, cuya definición también

aparece en [3]. $H(p,\lambda)$ es una extensión iterada de Ore con generadores $\{u_{i\alpha} \mid 1 \leq i, \alpha \leq p\}$, y relaciones

$$u_{j\beta}u_{i\alpha} = \begin{cases} \frac{p_{ji}}{p_{\beta\alpha}}u_{i\alpha}u_{j\beta} + (\lambda-1)p_{ji}u_{i\beta}u_{j\alpha} & \text{if } j > i,\ \beta > \alpha \\ \lambda\frac{p_{ji}}{p_{\beta\alpha}}u_{i\alpha}u_{j\beta} & \text{if } j > i,\ \alpha \leq \beta \\ \frac{1}{p_{\beta\alpha}}u_{i\alpha}u_{j\beta} & \text{if } j = i,\ \beta > \alpha \end{cases}$$

Ordenando los generadores respecto al orden lexicográfico en $\{1,\ldots,p\} \times \{1,\ldots,p\}$, el orden lexicográfico o el orden lexicográfico graduado sobre $\mathbb{N}^{p^2}$ convierte a $H(p,\lambda)$ en un álgebra de tipo PBW.

[2.17]. Ejemplo. Como último ejemplo vamos a estudiar las álgebras q–envolventes definidas y estudiadas por R. Berger en [5]. Estas álgebras están generadas por p elementos $\{x_1,\ldots,x_p\}$ y tienen por relaciones

$$x_jx_i = q_{ji}x_ix_j + \sum_{\substack{i<k\leq l<j \\ i+j=k+l}} c_{kl}^{ji}x_kx_l + \sum_{k=1}^{p} c_k^{ji}x_k + c$$

Que los monomios ordenados forman una $\Bbbk$–base viene demostrado en dicho trabajo bajo la hipótesis adicional de que los generadores satisfagan la allí llamada condición de Jacobi. Los órdenes lexicográficos graduados con $\epsilon_1 < \cdots < \epsilon_p$ o con $\epsilon_1 > \cdots > \epsilon_p$ convierten a estas álgebras en PBW álgebras. Casos particulares aparecen en [81], [69], [57] y [34].

2.2 Bases de Gröbner.

Recordemos que en el capítulo 1 se encuantran las definiciones concernientes a $\mathbb{N}^p$ y a sus órdenes admisibles.

[2.18]. En esta sección vamos a estudiar la conexión entre un ideal de un álgebra de tipo PBW R y su *exponente*. Dado un subconjunto $F \subseteq R$, definimos su exponente como el conjunto

$$\mathrm{Exp}(F) = \{\exp(f) \mid f \in F, f \neq 0\}.$$

[2.19]. Lema. *Si I es un ideal (a izquierda o derecha) de R entonces* $\mathrm{Exp}(I)$ *es un monoideal.*

Demostración. Vamos a suponer que I es un ideal a izquierda. Dado que sólo tenemos que demostrar la inclusión $\mathrm{Exp}(I) + \mathbb{N}^p \subseteq \mathrm{Exp}(I)$, escojamos $\alpha \in \mathrm{Exp}(I)$ y $\beta \in \mathbb{N}^p$. Existe un elemento $f \in I$ tal que $\exp(f) = \alpha$. Como I es un ideal $u_\beta f \in I$. Por otra parte $\exp(u_\beta f) = \exp(u_\beta) + \exp(f) = \beta + \alpha$, luego $\alpha + \beta \in \mathrm{Exp}(I)$. □

El lema de Dickson proporciona el siguiente corolario.

[2.20]. Corolario. *Dado un ideal (a izquierda o derecha) $I \leq R$, existen $f_1, \ldots, f_m \in I$ tales que*

$$\mathrm{Exp}(I) = \bigcup_{i=1}^{m} \big(\exp(f_i) + \mathbb{N}^p\big).$$

Demostración. Consecuencia inmediata de [2.19] y el Lema de Dickson [1.6]. □

[2.21]. Un subconjunto $G = \{g_1, \ldots, g_m\}$ de $I \leq R$ es una *base de Gröbner* para I si

$$\mathrm{Exp}(I) = \bigcup_{i=1}^{m} \big(\exp(g_i) + \mathbb{N}^p\big).$$

Como consecuencia del corolario anterior tenemos:

Proposición. *Sea R un álgebra de tipo PBW y sea $I \leq R$ un ideal (a izquierda o derecha). Existe una base de Gröbner para I.*

[2.22]. Ejemplo. Consideremos la $\Bbbk$–álgebra $R = \Bbbk_q[x, y]$, con dos generadores y relación $yx = qxy$ para $q \in \mathbb{K}^\times$, conocida por el plano cuántico (ver [2.14]). Consideramos el orden lexicográfico graduado con $\epsilon_2 > \epsilon_1$ sobre $\mathbb{N}^2$. Sea $I = R(y - x)$ el ideal a izquierda generado por $y - x$. Todo elemento de I se escribe de la forma $f(y - x)$ con $f \in R$, y dado que $\exp(f(y - x)) = \exp(f) + \exp(y - x) = \exp(f) + \epsilon_2$, tenemos que $\exp(y - x)$ genera $\mathrm{Exp}(I)$. De hecho esta propiedad es general para todo ideal a izquierda principal como se verá en [2.59]. Si llamamos $J = R(y - x)R$, es ideal biláltero generado por $y - x$, la situación cambia sustancialmente. Si $q \neq 1$ tenemos la siguiente idualdad:

$$x^2 = \frac{q}{1-q}x(y - x) - (y - x)\frac{1}{1-q}x,$$

de donde $x^2 \in J$. Pero $\exp(x^2) = 2\epsilon_1 \notin \epsilon_2 + \mathbb{N}^p$, de donde podemos concluir que $y - x$ no es una base de Gröbner para J. Comprobaremos más adelante que $\{y - x, x^2\}$ es una base de Gröbner para J.

[2.23]. Si $\mathrm{Exp}(G)$ es un sistema de generadores minimal de $\mathrm{Exp}(I)$ entonces G recibe el nombre de *base de Gröbner minimal.* La existencia de bases de Gröbner minimales viene garantizada por los teoremas de [1.6]. Además están caracterizadas porque para todo $g \in G$,

$$\exp(g) \notin \bigcup_{f \in G \setminus \{g\}} \big(\exp(f) + \mathbb{N}^p\big)$$

[2.24]. Ejemplo. Un ideal puede tener más de una base de Gröbner minimal como demuestra el siguiente ejemplo: Sea $R = \Bbbk[x, y]$ e I el ideal generado por x, y. Es fácil comprobar que tanto $\{x, y\}$ como $\{x + y, y\}$ son bases de Gröbner minimales para I, considerando en $\mathbb{N}^2$ el orden lexicográfico con $(1, 0) > (0, 1)$.

Para conseguir la unicidad en las bases de Gröbner es necesario tener un control más preciso de sus elementos, y no sólo de sus exponentes. Véase la proposición [2.53].

2.3 Algoritmo de la división.

El siguiente algoritmo de la división extiende el algoritmo de la división usual sobre un anillo de polinimios.

[2.25]. Sea $F = \{f_1, \ldots, f_m\}$ un conjunto finito de elementos de R. Si consideramos el orden en que hemos escrito sus elementos obtenemos una upla (ordenada) $[F] = [f_1, \ldots, f_m]$ de elementos no nulos de R. Asociada a esta upla definimos una partición $\boldsymbol{\Delta}^{[F]}$ en $\mathbb{N}^p$:

$$\begin{aligned}
&\Delta_1 = \exp(f_1) + \mathbb{N}^p \\
&\vdots \\
&\Delta_i = \big(\exp(f_i) + \mathbb{N}^p\big) \setminus \big(\Delta_1 \cup \cdots \cup \Delta_{i-1}\big) \qquad (2.2) \\
&\vdots \\
&\overline{\Delta} = \mathbb{N}^p \setminus \big(\Delta_1 \cup \cdots \cup \Delta_m\big).
\end{aligned}$$

Observemos que $\Delta_1 \cup \cdots \cup \Delta_m = \operatorname{Exp}(F) + \mathbb{N}^p$, el monoideal generado por $\{\exp(f_1), \ldots, \exp(f_m)\}$. Si $\leq$ es un orden admisible sobre $\mathbb{N}^p$, diremos que una $\Bbbk$–álgebra R con base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ tiene *división a izquierda fuerte* por la upla $[F]$ si para todo $f \in R$, existen $q_1, \ldots, q_m, r \in R$ tales que

1. $f = \sum_{i=1}^{m} q_i f_i + r$.
2. O bien $r = 0$, o bien $\mathcal{N}(r) \subseteq \overline{\Delta}$ y $\exp(r) \leq \exp(f)$.
3. $\exp(f_i) + \mathcal{N}(q_i) \subseteq \Delta_i$ y $\exp(q_i f_i) \leq \exp(f)$.

Estas condiciones nos dicen, en particular, que

$$\exp(f) = \max\{\exp(r), \exp(q_1 f_1), \ldots, \exp(q_m f_m)\}.$$

Dado que $\exp(r) \in \overline{\Delta}$, $\exp(q_i f_i) \in \Delta_i$ para cada i y $\Delta_1, \ldots, \Delta_m, \overline{\Delta}$ forman una partición, tenemos que $\exp(f) = \exp(r)$ o existe un único i_0 tal que

$\exp(f) = \exp(q_{i_0} f_{i_0})$. El primer caso es equivalente a que $\exp(f) \in \overline{\Delta}$, y el segundo a que $\exp(f) \in \Delta_{i_0}$, es decir, $\exp(f) = \exp(r)$ si y sólo si $\exp(f) \in \overline{\Delta}$ y $\exp(q_i f_i) = \exp(f)$ si y sólo si $\exp(f) \in \Delta_i$.

[2.26]. Lema. *Si $f = q_1 f_1 + \ldots q_m f_m + r$ y $f = q_1' f_1 + \ldots q_m' f_m + r'$ son divisiones a izquierda fuerte de f entre $[f_1, \ldots f_m]$ entonces $q_i = q_i'$ para todo i y $r = r'$.*

Demostración. Supongamos que existen dos descomposiciones, es decir,

$$f = \sum_{i=1}^{m} q_i f_i + r = \sum_{i=1}^{m} q_i' f_i + r'$$

Entonces

$$0 = \sum_{i=1}^{m} (q_i - q_i') f_i + (r - r').$$

Si $r - r' \neq 0$, $\exp(r - r') \in \mathcal{N}(r - r') \subseteq \mathcal{N}(r) \cup \mathcal{N}(r') \subseteq \overline{\Delta}$. Por otra parte, $\mathcal{N}(q_i) + \exp(f_i) \subseteq \Delta_i$ y $\mathcal{N}(q_i') + \exp(f_i) \subseteq \Delta_i$, de donde

$$\begin{aligned} \exp\left((q_i - q_i')f_i\right) = \exp(q_i - q_i') + \exp(f_i) &\in \mathcal{N}(q_i - q_i') + \exp(f_i) \\ &\subseteq (\mathcal{N}(q_i) \cup \mathcal{N}(q_i')) + \exp(f_i) \subseteq \Delta_i. \end{aligned}$$

Los conjuntos Δ_i satisfacen $\Delta_i \cap \Delta_j = \varnothing$ cuando $i \neq j$, de donde

$$\exp\Big(\sum_{i=1}^{m} (q_i - q_i')f_i\Big) = \max\big\{\exp\left((q_i - q_i')f_i\right) \mid 1 \leq i \leq m\big\}.$$

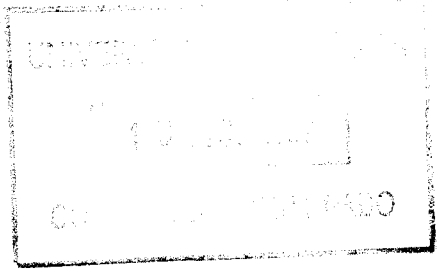
Se impone por tanto la necesidad de que exista un índice i_0 tal que

$$\exp(r - r') = \exp\Big(\sum_{i=1}^{m} (q_i - q_i')f_i\Big) \in \Delta_{i_0},$$

lo que es imposible, dado que $\Delta_{i_0} \cap \overline{\Delta} = \varnothing$. Con esto demostramos que $r = r'$.

Análogamente, si $q_1 \neq q_1'$, entonces

$$(q_1' - q_1) f_1 = \sum_{i=2}^{m} (q_i - q_i') f_i.$$



Por una parte, $\exp\big((q_i' - q_1)f_1\big) \in \Delta_1$, y por otra parte podemos garantizar la existencia de un índice $i_0 \in \{2, \ldots, m\}$ tal que

$$\exp\big(\sum_{i=2}^{m}(q_i - q_i')f_i\big) \in \Delta_{i_0},$$

lo que contradice el hecho de que $\Delta_1 \cap \Delta_{i_0} = \varnothing$. Tenemos pues que $q_1 = q_1'$. Repitiendo el proceso llegamos a que $q_i = q_i'$ para todo $i \in \{1, \ldots, m\}$. □

La unicidad es consecuencia de haber adoptado un orden en los elementos de la lista. Llamaremos cocientes a los elementos q_i y resto al elemento r. Al resto de dividir f por la upla $[F]$ lo notaremos $\mathrm{lres}(f, [F])$ o $\mathrm{lres}(f, F)$ abusando del lenguaje.

Si existe división a izquierda fuerte por cualquier upla $[F]$, diremos que R tiene un *algoritmo de la división a izquierda fuerte.*

[2.27]. Lema. *Si f es divisible a izquierda fuertemente por $[F]$ entonces* $\mathrm{lres}(f, [F])$ *es divisible a izquierda fuertemente por $[F]$ y*

$$\mathrm{lres}(\mathrm{lres}(f, [F]), [F]) = \mathrm{lres}(f, [F]).$$

Demostración. Dado que $\mathcal{N}(\mathrm{lres}(f, [F])) \subseteq \overline{\Delta}$ es inmediato que

$$\mathrm{lres}(f, [F]) = \sum_{i=1}^{m} 0 \cdot f_i + \mathrm{lres}(f, [F])$$

es una división a izquierda fuerte. □

[2.28]. Podemos dar también el *algoritmo de la división a izquierda débil.* R tiene un algoritmo débil si para cualesquiera $f, f_1, \ldots, f_m \in R$, con $f_i \neq 0$, existen $q_1, \ldots, q_m, r \in R$ tales que

1. $f = \sum_{i=1}^{m} q_i f_i + r$,
2. $\mathcal{N}(r) \cap \Big(\bigcup_{i=1}^{m}\big(\exp(f_i) + \mathbb{N}^p\big)\Big) = \varnothing$ y $\exp(r) \leq \exp(f)$,
3. $\exp(q_i f_i) \leq \exp(f)$.

Utilizaremos la misma convención que en el caso del algoritmo fuerte para hablar de división débil por $F = \{f_1, \ldots, f_m\}$. Dado que no hay unicidad ni en cocientes ni en restos vamos a llamar $\mathrm{LRes}(f, F)$ al conjunto de todos los restos que se obtienen al dividir débilmente f por F.

Consecuencia directa de las definiciones es que la existencia de un algoritmo fuerte implica la existencia de un algoritmo débil, y que $\mathrm{lres}(f, F) \in \mathrm{LRes}(f, F)$.

Análogamente se define la división a derecha, donde usaremos la notación $\mathrm{rres}(f, [F])$, $\mathrm{RRes}(f, F)$ como en el caso anterior.

[2.29]. Lema. *Sea* $F = \{f_1, \ldots, f_m\}$. *Si* $\exp(f) \notin \operatorname{Exp}(F) + \mathbb{N}^p$ *y* $r \in \operatorname{LRes}(f, F)$ *entonces* $\exp(f) = \exp(r)$.

Demostración. Sabemos que $\exp(r) \leq \exp(f)$ y que $f = \sum_{i=1}^{m} q_i f_i + r$. Por tanto

$$\exp(f) = \exp\left(\sum_{i=1}^{m} q_i f_i + r\right)$$
$$\leq \max\{exp(r), \exp(q_i f_i) \mid 1 \leq i \leq m\} \leq \exp(f).$$

Dado que las desigualdades deben ser igualdades tenemos que $\exp(f) = \exp(q_{i_0} f_{i_0})$ para algún i_0 o $\exp(f) = \exp(r)$. La primera posibilidad es imposible debido a que $\exp(f) \notin \operatorname{Exp}(F) + \mathbb{N}^p$. □

[2.30]. Teorema. *Sea* R *un álgebra de tipo PBW en la que los elementos* $q_{\alpha,\beta}$ *son unidades de* $\Bbbk$. *Si* $\operatorname{lc}(f_i)$ *es una unidad de* $\Bbbk$ *para cualquier* i, *entonces* R *tiene división a izquierda fuerte por* $[F]$.

Demostración. Veamos la existencia de los cocientes y el resto. Primeramente, dado que los coeficientes líderes de cada f_i son unidades, podemos suponer que todos son 1. La demostración la vamos a realizar por inducción en $\exp(f)$. Si $\exp(f) = \mathbf{0}$, $q_{i_0} = f$ para el primer índice i_0 tal que $\exp(f_{i_0}) = \mathbf{0}$, $q_i = 0$ si $i \neq i_0$, y $r = 0$, o $r = f$, $q_i = 0$ si $\exp(f_i) \neq \mathbf{0}$ para todo i. Supongamos por consiquiente que $\exp(f) \neq \mathbf{0}$. Dado que los conjuntos $\Delta_1, \ldots, \Delta_m, \overline{\Delta}$ constituyen una partición de $\mathbb{N}^p$, tenemos que $\exp(f) \in \Delta_{i_0}$ para un único i_0 o $\exp(f) \in \overline{\Delta}$. Si $\exp(f) \in \overline{\Delta}$, llamamos $f' = f - \operatorname{lm}(f)$. Como $\exp(f') < \exp(f)$, por hipótesis de inducción

$$f' = \sum_{i=1}^{m} q_i f_i + r',$$

de donde

$$f = \sum_{i=1}^{m} q_i f_i + \left(\operatorname{lm}(f) + r'\right)$$

satisface las propiedades requeridas. Observemos que en este caso $\exp(f) = \exp(r)$, donde $r = \operatorname{lm}(f) + r'$, y $\exp(q_i f_i) \leq \exp(f') < \exp(f)$. Por otra parte, si $\exp(f) \in \Delta_{i_0}$, entonces $\exp(f) = \beta + \exp(f_{i_0})$ para un cierto $\beta \in \mathbb{N}^p$. Como $\operatorname{lc}(f_{i_0}) = 1$,

$$\operatorname{lc}\left(\frac{\operatorname{lc}(f)}{q_{\beta,\exp(f_{i_0})}} u_\beta f_{i_0}\right) = q_{\beta,\exp(f_{i_0})} \frac{\operatorname{lc}(f)}{q_{\beta,\exp(f_{i_0})}} \operatorname{lc}(f_{i_0}) = \operatorname{lc}(f),$$

de donde $f' = f - \frac{\mathrm{lc}(f)}{q_{\beta,\exp(f_{i_0})}} u_\beta f_{i_0}$ satisface que $\exp(f') < \exp(f)$. Por la hipótesis de inducción,

$$f' = \sum_{i \neq i_0} q_i f_i + q'_{i_0} f_{i_0} + r.$$

Llamemos $q_{i_0} = \frac{\mathrm{lc}(f)}{q_{\beta,\exp(f_{i_0})}} u_\beta + q'_{i_0}$. Es evidente que esta descomposición satisface las propiedades 1 y 2 del teorema y la 3 si $i \neq i_0$. Si $\alpha \in \mathcal{N}(q_{i_0})$ entonces $\alpha \in \mathcal{N}(q'_{i_0})$ o $\alpha = \beta$. En el primer caso $\alpha + \exp(f_{i_0}) \in \Delta_{i_0}$ por hipótesis de inducción, y en el segundo caso $\beta + \exp(f_{i_0}) = \exp(f) \in \Delta_{i_0}$. Además, en vista de que

$$\exp(q'_{i_0} f_{i_0}) \leq \exp(f') < \exp(f) \text{ y } \exp\left(\frac{\mathrm{lc}(f)}{q_{\beta,\exp(f_{i_0})}} u_\beta f_{i_0}\right) = \exp(f),$$

obtenemos la siguiente igualdad:

$$\exp(q_{i_0} f_{i_0}) = \exp(f).$$

Nótese que $\exp(q_i f_i) \leq \exp(f') < \exp(f)$ si $i \neq i_0$, y $\exp(r) \leq \exp(f') < \exp(f)$. □

[2.31]. Corolario. *Sea R un álgebra de tipo PBW en la que los elementos $q_{\alpha,\beta}$ son unidades de $\Bbbk$. Si $\{f_1, \ldots, f_m\}$ es un conjunto tal que $\mathrm{lc}(f_i)$ es una unidad de $\Bbbk$ para cualquier i, entonces R tiene división a izquierda débil por $\{f_1, \ldots, f_m\}$.*

[2.32]. Corolario. *Si $\Bbbk$ es un cuerpo y R es una $\Bbbk$–álgebra de tipo PBW, entonces R tiene algoritmos de la división fuerte y débil.*

[2.33]. Ejemplo. Vamos a dar un ejemplo ilustrativo de como podemos realizar la división fuerte. El procedimiento está implícito en la demostración del teorema [2.30]. Consideremos $R = U(\mathfrak{g})$, donde $\mathfrak{g}$ es el álgebra de Lie de dimensión 2 y corchete $[y, x] = x$. Podemos ver R como el álgebra con dos generadores x, y y relación $yx = xy + x$. Por el teorema de Poincaré–Birkoff–Witt para álgebras envolventes de álgebras de Lie finitodimensional, los monomios ordenados forman una $\Bbbk$–base, y el orden lexicográfico graduado con $\epsilon_2 > \epsilon_1$ convierte a R en una PBW álgebra. Consideremos los elementos

$$\begin{aligned} f &= 2x^2y^2 + 3x^3y + 6y + 5x \\ f_1 &= xy + x \\ f_2 &= y^2 + x^2 + 1 \\ f_3 &= x^3 + y \\ [F] &= [f_1, f_2, f_3]. \end{aligned}$$

Vamos a realizar la división fuerte de f entre $[F]$. Empezamos calculando la partición $\Delta^{[F]}$:

$$\begin{aligned}\Delta_1 &= (1,1) + \mathbb{N}^2\\ \Delta_2 &= \big((0,2) + \mathbb{N}^2\big) \setminus \Delta_1\\ \Delta_3 &= \big((3,0) + \mathbb{N}^2\big) \setminus (\Delta_1 \cup \Delta_2)\\ \overline{\Delta} &= \{(0,0),(1,0),(2,0),(0,1)\}\end{aligned}$$

Tenemos que $\exp(f) = (2,2) \in \Delta_1$, luego la primera reducción debe ser por f_1. Dado que

$$2xyf_1 = 2x^2y^2 + 4x^2y + 2x^2,$$

tenemos que

$$f = \boxed{2xyf_1} + 3x^3y - 4x^2y - 2x^2 + 6y + 5x,$$

Pongamos $f' = 3x^3y - 4x^2y - 2x^2 + 6y + 5x$, con lo que $\exp(f') < \exp(f)$. Repetimos el proceso para f', $\exp(f') = (3,1) \in \Delta_1$ y

$$3x^2f_1 = 3x^3y + 3x^3,$$

de donde

$$f' = \boxed{3x^2f_1} + f'' \qquad f'' = -4x^2y - 3x^3 - 2x^2 + 6y + 5x.$$

Análogamente, $\exp(f'') = (2,1) \in \Delta_1$ y

$$-4xf_1 = -4x^2y - 4x^2,$$

por lo que

$$f'' = \boxed{-4xf_1} - 3x^3 + 2x^2 + 6y + 5x$$

Llamemos $f''' = -3x^3 + 2x^2 + 6y + 5x$, $\exp(f''') = (3,0) \in \Delta_3$. Como $-3f_3 = -3x^3 - 3y$, tenemos que

$$f''' = \boxed{-3f_3} + 2x^2 + 9y + 5x.$$

Si llamamos ahora $f^{IV} = 2x^2 + 9y + 5x$, si observamos que $\mathcal{N}(f^{IV}) \subseteq \overline{\Delta}$, y juntamos todas las descomposiciones previas tenemos que

$$f = (2xy + 3x^2 - 4x)f_1 - 3f_3 + 2x^2 + 9y + 5x,$$

que es la división a izquierda fuerte de f entre $[F]$. Podemos también reescribir f mediante una división débil,

$$f = 2f_1 + (2x^2 - 3)f_2 + (3y - 2x - 9)f_3 + x^2 + 15y + 3x + 3.$$

En particular ebservamos como el resto no es único.

La existencia de estos algoritmos está estrechamente relacionada con el concepto de álgebra de tipo PBW. De hecho, el siguiente teorema caracteriza las álgebras de tipo PBW en términos de la existencia de un algoritmo de la división, en el caso en que $\Bbbk$ es un cuerpo.

[2.34]. Teorema. *Sea $\Bbbk$ un cuerpo. Sea R una $\Bbbk$-álgebra que tiene por $\Bbbk$-base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ y sea $\leq$ un orden admisible sobre $\mathbb{N}^p$. Si R tiene un algoritmo de la división a izquierda débil, entonces $\leq$ es un orden $\mathcal{B}$-admisible.*

Demostración. Tenemos que demostrar alguna de las equivalencias de [2.3], por lo que vamos a demostrar que

$$u_\alpha u_\beta = q_{\alpha,\beta} u_{\alpha+\beta} + \sum_{\gamma<\alpha+\beta} c_\gamma u_\gamma,$$

siendo $q_{\alpha,\beta} \neq 0$, por inducción sobre α. Sea entonces $\alpha = \mathbf{0}$. Llamamos $f = f_1 = u_{\mathbf{0}}$. Por la división débil

$$u_{\mathbf{0}} = q u_{\mathbf{0}} + r,$$

con $\exp(q) + \mathbf{0} = \mathbf{0}$, $\exp(r) \leq \mathbf{0}$ y $\mathcal{N}(r) \cap (\mathbf{0} + \mathbb{N}^p)$. Esto fuerza a que $r = 0$ y $q = c_{\mathbf{0}} u_{\mathbf{0}}$. En consecuencia $u_{\mathbf{0}} \in \Bbbk \setminus \mathbf{0}$ y el resultado es claro. Supongamos ahora que el resultado es cierto para cualquier $\gamma < \alpha$. Llamemos $f = u_{\alpha+\beta}$ y $f_1 = u_\beta$. Por la división, existen $q, r \in R$ tales que

1. $u_{\alpha+\beta} = q u_\beta + r$,
2. $\mathcal{N}(r) \subseteq \mathbb{N}^p \setminus (\beta + \mathbb{N}^p)$ y $\exp(r) \leq \alpha + \beta$,
3. $\exp(q) + \beta \leq \alpha + \beta$.

Dado que $\exp(r) = \alpha + \beta$ implicaría que $\mathcal{N}(r) \cap (\beta + \mathbb{N}^p) \neq \varnothing$, se tiene que $\exp(r) < \alpha + \beta$, por lo que $\exp(q) + \beta = \alpha + \beta$ y $\exp(q) = \alpha$. Podemos deducir que

$$\begin{aligned} u_{\alpha+\beta} &= \left(c_\alpha u_\alpha + \sum_{\gamma<\alpha} c_\gamma u_\gamma \right) u_\beta + \sum_{\delta<\alpha+\beta} d_\delta u_\delta \\ &= c_\alpha u_\alpha u_\beta + \underline{\sum_{\gamma<\alpha} c_\gamma u_\gamma u_\beta} + \sum_{\delta<\alpha+\beta} d_\delta u_\delta \\ &= c_\alpha u_\alpha u_\beta + \underline{\sum_{\rho<\alpha+\beta} k_\rho u_\rho}, \end{aligned}$$

donde la última igualdad se obtiene aplicando la hipótesis de inducción a los términos subrayados. Despejando $u_\alpha u_\beta$ (teniendo en cuenta que $c_\alpha \neq 0$) obtenemos la fórmula deseada. □

Podemos resumir los resultados anteriores en un teorema.

[2.35]. Teorema. *Sea $\Bbbk$ un cuerpo y sea R una $\Bbbk$-álgebra con $\Bbbk$-base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$. Sea $\leq$ un orden admisible sobre $\mathbb{N}^p$. Las siguientes afirmaciones son equivalentes:*

[a] $\exp(fg) = \exp(f) + \exp(g)$.

[b] $u_\alpha u_\beta = q_{\alpha,\beta} u_{\alpha+\beta} + \sum_{\gamma<\alpha+\beta} c_\gamma u_\gamma$, *donde* $q_{\alpha,\beta} \neq 0$.

[c] *R tiene un algoritmo de la división a izquierda fuerte.*

[d] *R tiene un algoritmo de la división a izquierda débil.*

[e] *R tiene un algoritmo de la división a derecha fuerte.*

[f] *R tiene un algoritmo de la división a derecha débil.*

Los dos últimos apartados son por simetría.

2.4 Primeras aplicaciones.

Vamos a profundizar en la conexión entre bases de Gröbner de un ideal y los elementos de dicho ideal. En esta sección R será una $\Bbbk$–álgebra de tipo PBW, con $\Bbbk$ un dominio noetheriano conmutativo, en la que los elementos $q_{\alpha,\beta}$ son unidades de $\Bbbk$.

[2.36]. Proposición. *Si $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner para el ideal a izquierda I en la que $\mathrm{lc}(g_i)$ es una unidad de $\Bbbk$ para todo i, entonces*

$$I = Rg_1 + \cdots + Rg_t.$$

Demostración. Sea $f \in I$, $f \neq 0$. Como G es una base de Gröbner $\mathrm{Exp}(I) = \bigcup_{i=1}^{t} (\exp(g_i) + \mathbb{N}^p)$. Por la división débil a izquierda existen $q_1, \ldots, q_t, r \in R$ tales que

$$f = \sum_{i=1}^{t} q_i g_i + r \qquad r = 0 \text{ o } \mathcal{N}(r) \cap \mathrm{Exp}(I) = \varnothing$$

Dado que $r = f - \sum_{i=1}^{m} q_i g_i \in I$, si $r \neq 0$ entonces $\exp(r) \in \mathrm{Exp}(I)$, con lo que $\mathrm{Exp}(I) \cap \mathcal{N}(r) \neq \varnothing$. Por tanto $r = 0$. □

Usando la división a derecha tenemos el resultado análogo a derecha, es decir, si $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner para el ideal a derecha I entonces

$$I = g_1 R + \cdots + g_t R.$$

[2.37]. Corolario. *Si* $\Bbbk$ *es un cuerpo entonces* R *es noetheriano.*

Demostración. Consecuencia inmediata de [2.20] y [2.36]. □

[2.38]. Corolario. *Si* I *es un ideal bilátero de* R *y* $G = \{g_1, \ldots, g_t\}$ *es una base de Gröbner para* I *en la que* $\mathrm{lc}(g_i)$ *es una unidad de* $\Bbbk$*, entonces*

$$I = Rg_1 + \cdots + Rg_t = g_1R + \cdots + g_tR.$$

El corolario [2.38] nos permite tratar un ideal bilátero como un ideal a izquierda o derecha una vez conocida una base de Gröbner para él. Abordemos ahora el problema de la unicidad del resto en la división débil.

[2.39]. Proposición. *Sean* $G = \{g_1, \ldots, g_t\}$ *y* $G' = \{g'_1, \ldots, g'_s\}$ *dos bases de Gröbner para el ideal a izquierda* I*, y sea* $f \in R$*. Entonces para todo* $r \in \mathrm{LRes}(f, G)$ *y todo* $r' \in \mathrm{LRes}(f, G')$*,* $r = r'$*.*

Demostración. Por la división a izquierda débil

$$f = \sum_{i=1}^{t} q_i g_i + r = \sum_{i=1}^{s} q'_i g'_i + r'.$$

Por tanto $r - r' \in I$ y $\exp(r - r') \in \mathrm{Exp}(I)$ si suponemos que $r - r' \neq 0$. Por otra parte $\exp(r - r') \in \mathcal{N}(r - r') \subseteq \mathcal{N}(r) \cup \mathcal{N}(r') \subseteq \mathbb{N}^p \setminus \mathrm{Exp}(I)$, lo que es imposible. □

[2.40]. En particular, si ponemos $G = G'$ en [2.39], obtenemos que el conjunto $\mathrm{LRes}(f, G)$ es un conjunto unitario, es decir, si G es una base de Gröbner para el ideal a izquierda que genera,

$$\mathrm{LRes}(f, G) = \{\mathrm{lres}(f, [G])\}.$$

Es natural emplear la notación $\mathrm{lres}(f, G)$ cuando G es una base de Gröbner para el ideal I.

[2.41]. Corolario. *Sea* $G = \{g_1, \ldots, g_t\}$ *una base de Gröbner para el ideal a izquierda* I*, y sea* $f \in R$*. Entonces* $f \in I$ *si y sólo si* $\mathrm{lres}(f, G) = 0$*.*

Demostración. Sea $G' = G \cup \{f\}$. Es evidente de la definición que G' también es una base de Gröbner para I, y además $\mathrm{lres}(f, G') = 0$ como la siguiente división a izquierda demuestra:

$$f = \sum_{i=1}^{t} 0 \cdot g_i + 1 \cdot f + 0.$$

Consecuentemente, la proposición [2.39] demuestra el corolario. □

[2.42]. Ejemplo. Consideremos el álgebra del diamante D que aparece en [7, 5.9 Beispiel]. Es el álgebra envolvente del álgebra de Lie de dimensión cuatro con corchete de Lie

$$\begin{aligned} [x,y]=0 \quad [x,t]=0 \quad [x,z]=0 \\ [y,t]=y \quad [y,z]=x \quad [z,t]=-z, \end{aligned}$$

i.e., la $\Bbbk$–álgebra generada por los elementos $\{x,y,z,t\}$ y con relaciones

$$\begin{aligned} yx=xy \qquad tx=xt \qquad zx=xz \\ ty=yt-y \quad zy=yz-x \quad tz=zt+z \end{aligned}$$

La estructura de álgebra de tipo PBW viene dada en [2.15], por lo que consideraremos el orden graduado lexicográfico graduado sobre $\mathbb{N}^4$ con $\epsilon_1 < \epsilon_2 < \epsilon_3 < \epsilon_4$. Llamemos I al ideal a izquierda de D generado por x^3+t^2, z^2+y, y t^3+3t, es decir, $I = D(x^3+t^2)+D(z^2+y)+D(t^3+3t)$. Pretendemos decidir $xyz+z^2t \in I$. Para aplicar [2.41] necesitamos una base de Gröbner para I. Una base de Gröbner para I es $\{y,t,x^2,xz,z^2\}$. Ahora bien, la siguiente igualdad nos da una división débil de resto cero,

$$xyz+z^2t = xz\cdot y + (t-2)\cdot z^2,$$

por lo que podemos asegurar que $xyz+z^2t \in I$.

Los restos nos permiten caracterizar de nuevo a las bases de Gröbner:

[2.43]. Lema. *Sea $F=\{f_1,\dots,f_m\}$ un conjunto tal que $\mathrm{LRes}(g,F)$ tiene un único elemento para cualquier $g \in R$. Si $c \in \Bbbk^\times$, $\alpha \in \mathbb{N}^p$, $f \in R$ y $\{r\} = \mathrm{LRes}(f,F)$ entonces para todo $1 \le i \le m$*

$$\{r\} = \mathrm{LRes}(f - cu_\alpha f_i, F)$$

Demostración. Vamos a estudiar dos casos. Supongamos en primer lugar que $\exp(f-cu_\alpha f_i) = \max\{\exp(f), \exp(cu_\alpha f_i)\}$. Como $r \in \mathrm{LRes}(f,F)$ existen $q_1,\dots,q_m$ tales que

$$f = q_1f_1+\cdots+q_mf_m+r, \quad \exp(q_jf_j) \le \exp(f) \quad \text{y}$$
$$\mathcal{N}(r) \cap \bigcup_{i=1}^{m} \left(\exp(f_i)+\mathbb{N}^p\right) = \varnothing.$$

Ahora,

$$f - cu_\alpha f_i = \sum_{j\neq i} q_jf_j + (q_i - cu_\alpha)f_i + r$$

con

$$\mathcal{N}(r) \cap \bigcup_{i=1}^{m} \big(\exp(f_i) + \mathbb{N}^n \big) = \varnothing,$$

$$\exp(q_j f_j) \leq \exp(f) \leq \max\{\exp(f), \exp(cu_\alpha f_i)\} = \exp(f - cu_\alpha f_i)$$

si $j \neq i$ y

$$\begin{aligned} \exp((q_i - cu_\alpha) f_i) &\leq \max\{\exp(q_i f_i), \exp(cu_\alpha f_i)\} \\ &\leq \max\{\exp(f), \exp(cu_\alpha f_i)\} = \exp(f - cu_\alpha f_i), \end{aligned}$$

luego $r \in \mathrm{LRes}(f - cu_\alpha f_i, F)$ como queríamos.

Supongamos ahora que $\exp(f - cu_\alpha f_i) < \max\{\exp(f), \exp(cu_\alpha f_i)\}$ y sea $\{r\} = \mathrm{LRes}(f, F)$. Entonces $\exp(f - cu_\alpha f_i) < \exp(f) = \exp(cu_\alpha f_i)$. Sea $r_1 \in \mathrm{LRes}(f - cu_\alpha f_i, F)$. Entonces

$$f - cu_\alpha f_i = \sum_{j=1}^{m} q_j f_j + r_1$$

con las propiedades de la división débil. Por consiguiente

$$f = \sum_{j \neq i} q_j f_j + (q_i + cu_\alpha) f_i + r_1$$

donde $exp(q_j f_j) \leq \exp(f - cu_\alpha f_i) < \exp(f)$ si $j \neq i$, y $\exp((q_i + cu_\alpha) f_i) \leq \max\{\exp(q_i f_i), \exp(cu_\alpha f_i)\} \leq \max\{\exp(f), \exp(cu_\alpha f_i)\} = \exp(f)$. Hemos demostrado que $r_1 \in \mathrm{LRes}(f, F)$, luego $r_1 = r$ y $r \in \mathrm{LRes}(f - cu_\alpha f_i, F)$. □

[2.44]. Teorema.

[2.44.1]. *Sea I un ideal a izquierda no nulo de R. $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner para I si y sólo si para cualquier $f \in I$, $0 \in \mathrm{LRes}(f, G)$.*

[2.44.2]. *G es una base de Gröbner para el ideal a izquierda que genera si y sólo si los conjuntos* $\mathrm{LRes}(f, G)$ *son unitarios para todo $f \in R$*

Demostración. Veamos [2.44.1]. Una implicación es clara a partir del corolario [2.41]. Supongamos pues que $f \in I$ y $f \neq 0$. La división débil y la existencia de un resto nulo nos garantiza la existencia de elementos $q_1, \ldots, q_m \in R$ tales que

$$f = q_1 g_1 + \cdots + q_t g_t \qquad \exp(q_i g_i) \leq \exp(f).$$

Como

$$\exp(f) = \exp(q_1 g_1 + \cdots + q_t g_t) \leq \max\{\exp(q_i g_i) \mid 1 \leq i \leq t\} \leq \exp(f),$$

las desigualdades se convierten en igualdades y existe un índice i_0 tal que $\exp(f) = \exp(q_{i_0} g_{i_0}) = \exp(q_{i_0}) + \exp(g_{i_0}) \in \exp(g_{i_0}) + \mathbb{N}^p$. Consecuentemente

$$\mathrm{Exp}(I) = \bigcup_{i=1}^{t} \big(\exp(g_i) + \mathbb{N}^p\big)$$

y G es una base de Gröbner.

Para ver [2.44.2]., si G es una base de Gröbner entonces el resultado está en [2.40]. Si todos los conjuntos $\mathrm{LRes}(f, G)$ son unitarios entonces vamos a utilizar [2.44.1]. para ver que G es una base de Gröbner para el ideal que genera. Supongamos que $G = \{g_1, \dots g_t\}$ y sea $f = \sum c_{\alpha,i} u_\alpha g_i$ (un elemento genérico del ideal generado por G). Sea $r \in \mathrm{LRes}(f, G)$. Aplicando reiteradamente el lema [2.43] tenemos que $r \in \mathrm{LRes}(f - \sum c_{\alpha,i} u_\alpha f_i, G) = \mathrm{LRes}(0, G) \ni 0$. De la hipótesis $r = 0$, luego $0 \in \mathrm{LRes}(f, G)$ para todo f en el ideal a izquierda generado por G. □

Vamos a acabar la sección con dos nuevas aplicaciones, eliminación e intersección efectivas. Debemos tener presentes los resultados [1.24], [2.11], [2.12] y [2.13]. Siguiendo la notación de [2.13] tenemos el siguiente lema:

[2.45]. Lema. *Sea $\preceq$ el orden definido en [2.13] y sea $f \in S$, $f \neq 0$. $f \in R$ si y sólo si* $\exp(f) \in \mathbb{N}^p \times \{0\}$.

Demostración. La implicación hacia la derecha es clara. En el otro sentido, si $(\alpha, n) \in \mathcal{N}(f)$ entonces $(\alpha, n) \preceq (\beta, 0)$ lo que fuerza que $n = 0$. □

[2.46]. Proposición. *Sea $I \leq S = R[x; \sigma, \delta]$ y sea $G = \{g_1, \dots, g_t\}$ una base de Gröbner para I con respecto al orden $\preceq$. Sea $G^c = G \cap R$ y $I^c = I \cap R$. Entonces $G^c \neq \varnothing$ si y sólo si $I^c \neq \{0\}$, en cuyo caso G^c es una base de Gröbner para I^c. En particular G^c es un sistema de generadores para I^c.*

Demostración. Si $G^c \neq \varnothing$ es inmediato que $I^c \neq \{0\}$. Supongamos pues que $I^c \neq \{0\}$ y sea $0 \neq f \in I^c$. Como $f \in I$ y G es una base de Gröbner para I,

$$\exp(f) \in \bigcup_{i=1}^{t} \big(\exp(g_i) + \mathbb{N}^{p+1}\big),$$

por lo que podemos garantizar la existencia de un índice i_0 y un elemento $\gamma \in \mathbb{N}^p$ tales que $\exp(f) = \exp(g_{i_0}) + \gamma$. Por el lemma [2.45] sabemos que $\exp(f) \in \mathbb{N}^p \times \{0\}$, por lo que los elementos $\exp(g_{i_0}), \gamma \in \mathbb{N}^p \times \{0\}$ y $g_{i_0} \in G^c$. El mismo argumento demuestra que G^c es una base de Gröbner para I^c. □

Un ejemplo de aplicación de [2.46] lo encontraremos en [2.49].

En el caso conmutativo, es posible eliminar variables en cualquier orden, ya que cualquier orden admisible convierte a un anillo de polinomios en un álgebra de tipo PBW, y podemos ordenar las variables como deseemos.

La proposición [2.46] nos permite calcular de manera efectiva la intersección de un número finito de ideales a izquierda, reduciendo el problema a una eliminación:

[2.47]. Proposición. *Sea $I, J \leq R$ ideales a izquierda de un álgebra de tipo PBW. Llamemos $H = R[x]Ix + R[x]J(1-x) \leq R[x]$. Entonces $I \cap J = H \cap R$.*

Demostración. Dado que $f = fx + f(1-x)$ la inclusión $I \cap J \subseteq H \cap R$ es inmediata. Recíprocamente, sea $f \in H \cap R$, entonces

$$f = \sum_{i=1}^{m} h_i f_i x + \sum_{j=1}^{n} h'_j f'_j (1-x),$$

donde $h_i, h'_j \in R[x]$, $f_i \in I$ y $f'_j \in J$. Definimos el siguiente morfismo de R–módulos a izquierda:

$$\begin{aligned} \Phi : R[x] &\longrightarrow R \\ x^i &\longmapsto 1. \end{aligned}$$

Como la x no aparece en f tenemos que $\Phi(f) = f$. Por otra parte, como la x es una variable conmutativa $\Phi(f) \in I$, por lo que $f \in I$. Análogamente, definiendo $\Phi(x^i) = 0$ obtenemos que $f \in J$. □

[2.48]. Observación. Un sistema de generadores de H viene dado por

$$\{f_1 x, \ldots, f_m x, h_1(1-x), \ldots, h_n(1-x)\},$$

donde $\{f_1, \ldots f_m\}$ y $\{h_1, \ldots, h_n\}$ son sistemas de generadores de I y J respectivamente.

[2.49]. Ejemplo. Consideremos $R = \Bbbk_q[x, y]$ el plano cuántico. Sean $I = Rx^2 + Ry$, $J = Ry^2 + Rx$. Para calcular $I \cap J$ consideramos el ideal $H = R[z]x^2 z + R[z]yz + R[z]y^2(1-z) + R[z]x(1-z)$. Una base de Gröbner para H es $G = \{x^2, xy, y^2, xz - z, yz\}$. Por [2.46] $G \cap R = \{x^2, xy, y^2\}$ es una base de Gröbner para $H \cap R$, y en particular un sistema de generadores. Por [2.47], $I \cap J = H \cap R = Rx^2 + Rxy + Ry^2$.

2.5 Bases de Gröbner reducidas.

[2.50]. Podemos abordar ya el problema de la unicidad en las bases de Gröbner. Una *base de Gröbner reducida* para el ideal I es una base de Gröbner $G = \{g_1, \ldots, g_t\}$ para I tal que para todo $i = 1, \ldots, t$,

$$\mathrm{lc}(g_i) = 1 \text{ y } \mathcal{N}(g_i) \cap \Big(\bigcup_{i \neq j} \big(\exp(g_j) + \mathbb{N}^p \big) \Big) = \varnothing.$$

[2.51]. Lema. *Toda base de Gröbner reducida es minimal.*

Demostración. Consecuencia inmediata de [2.23]. □

[2.52]. Lema. *Si $G = \{g_1, \ldots, g_s\}$ es una base de Gröbner reducida para I entonces para cualquier $i = 1, \ldots, s$*

$$\mathcal{N}(g_i) \cap \mathrm{Exp}(I) = \{exp(g_i)\}.$$

Demostración. Supongamos que existe $\alpha \in \mathcal{N}(g_i) \cap \mathrm{Exp}(I)$, $\alpha \neq \exp(g_i)$. Entonces $\alpha < \exp(g_i)$ y $\alpha \notin \exp(g_i) + \mathbb{N}^p$. Dado que $\alpha \in \mathrm{Exp}(I) = \bigcup_{j=1}^{s} \big(\exp(g_j) + \mathbb{N}^p \big)$ existe un índice $j \neq i$ tal que $\alpha \in \exp(g_j) + \mathbb{N}^p$, pero entonces

$$\mathcal{N}(g_i) \cap \bigcup_{j \neq i} \big(\exp(g_j) + \mathbb{N}^p \big) \supseteq \{\alpha\},$$

lo que contradice el que G sea una base reducida. □

[2.53]. Teorema. *Si $\Bbbk$ es un cuerpo entonces todo ideal I tiene una única base de Gröbner reducida para I.*

Demostración. La demostración se basa en dar un método constructivo para obtener una base de Gröbner reducida a partir de una base de Gröbner mininmal, la cual se puede construir a partir de una base de Gröbner utilizando [1.7]. La existencia de una base de Gröbner minimal viene garantizada en [2.23], por tanto sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner minimal para I. Para cada $i = 1, \ldots, s$ elegimos $g_i' \in \mathrm{LRes}(g_i, G \setminus \{g_i\})$ (esta elección es efectiva ya que podemos elegir $g_i' = \mathrm{lres}(g_i, [G \setminus \{g_i\}])$). Como $\exp(g_i) \notin \bigcup_{j \neq i} \big(\exp(g_j) + \mathbb{N}^p \big)$ por [2.23], tenemos que $\exp(g_i) = \exp(g_i')$ aplicando [2.29]. Además

$$\mathcal{N}(g_i') \cap \big(\bigcup_{i \neq j} (\exp(g_j') + \mathbb{N}^p) \big) = \mathcal{N}(g_i') \cap \big(\bigcup_{i \neq j} (\exp(g_j) + \mathbb{N}^p) \big) = \varnothing.$$

Multiplicando cada g'_i por $\mathrm{lc}(g'_i)^{-1}$ obtenemos pues una base reducida para I.

Veamos la unicidad. Sean $G = \{g_1, \ldots, g_s\}$ y $G' = \{g'_1, \ldots, g'_t\}$ dos bases de Gröbner reducidas. Por [1.6] y el lema [2.51] tenemos que $s = t$ y $\mathrm{Exp}(G) = \mathrm{Exp}(G')$. Sean pues $g_i \in G$ y $g'_j \in G'$ tales que $\exp(g_i) = \exp(g'_j)$. Por una parte $g_i - g'_j \in I$, luego $\mathrm{lres}(g_i - g'_j, G) = 0$ (ver [2.41]). Por otra parte $\exp(g_i - g'_j) < \exp(g_i)$, luego si $\alpha \in \mathcal{N}(g_i - g'_j) \cap \mathrm{Exp}(I)$ entonces $\alpha \in \mathcal{N}(g_i) \cap \mathrm{Exp}(I)$ o $\alpha \in \mathcal{N}(g'_j) \cap \mathrm{Exp}(I)$ dado que $\mathcal{N}(g_i - g'_j) \subseteq \mathcal{N}(g_i) \cup \mathcal{N}(g'_j)$. Por el lema [2.52] tenemos que $\alpha = \exp(g_i) = \exp(g'_j)$, y como $\alpha \leq \exp(g_i - g'_j)$ llegamos a una contradicción. Hemos demostrado que $\mathcal{N}(g_i - g'_j) \cap \bigcup_{i=1}^{s} \left(\exp(g_i) + \mathbb{N}^p\right) = \varnothing$, por lo que

$$g_i - g'_j = \sum_{i=1}^{s} 0 \cdot g_i + (g_i - g'_j)$$

es una división débil. Por tanto $g_i - g'_j = \mathrm{lres}(g_i - g'_j, G) = 0$. Hemos demostrado que $g_i = g'_j$, con lo que reiterando el proceso $G = G'$. □

[2.54]. Vamos a acabar la sección dando dos resultados de [39] en los que se relacionan bases de Gröbner de ideales a izquierda e ideales a derecha. Vamos a decir que $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner a izquierda (resp. derecha) si G es una base de Gröbner para el ideal a izquierda (resp. a derecha) que genera.

[2.55]. Teorema ([39, Theorem 4.4]). *Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner reducida a izquierda y $H = \{h_1, \ldots, h_s\}$ una base de Gröbner reducida a derecha tales que $Rg_1 + \cdots + Rg_t = h_1R + \cdots + h_sR$. Entonces $G = H$.*

Demostración. Supongamos que $G \neq H$. Entre los elementos del conjunto $(G \setminus H) \cup (H \setminus G)$ escogemos un elemento f de exponente minimal. Una cuestión de simetría nos permite suponer que $f = g_j \in G \setminus H$. Dado que g_j está en el ideal a derecha generado por H y H es una base de Gröbner a derecha tenemos que $\mathrm{rres}(g_j, H) = 0$, por lo que hay $q_1, \ldots, q_s \in R$ y un índice $i \in \{1, \ldots, s\}$ tales que $g_j = h_1q_1 + \cdots + h_sq_s$ y $\exp(g_j) = \exp(h_i) + \exp(q_i)$ utilizando la división a derecha fuerte. En vista de la minimalidad del exponente de g_j, si $\exp(h_i) < \exp(g_j)$ entonces $h_i \in G \cap H$, y como $\exp(g_j) \in \exp(h_i) + \mathbb{N}^p$ llegamos a una contradicción con el hecho de que G es una base de Gröbner minimal (ver [2.51]). Necesariamente $\exp(g_j) = \exp(h_i)$. Vamos por último a comprobar que $f' = g_j - h_i = 0$. Reordenando las bases si fuera preciso es evidente que podemos suponer que los elementos de G y H están ordenados en orden descendente de sus exponentes, es decir,

$\exp(g_1) > \cdots > \exp(g_t)$ y $\exp(h_1) > \cdots > \exp(h_s)$. Si $f' \neq 0$ entonces $\exp(f') < \exp(g_j) = \exp(h_i)$ ya que $\mathrm{lm}(g_j) = \mathrm{lm}(h_i)$. Por la división fuerte tenemos

$$f' = q'_{j+1}g_{j+1} + \cdots + q'_t g_t = h_{i+1}q''_{i+1} + \cdots + h_s q''_s.$$

En vista de que $\exp(f') \in \mathcal{N}(f') \subseteq \mathcal{N}(g_j) \cup \mathcal{N}(h_i)$ tenemos que

$$\mathcal{N}(g_j) \cap \left(\bigcup_{k=j+1}^{t} \left(\exp(g_k) + \mathbb{N}^p \right) \right) \neq \varnothing$$

o

$$\mathcal{N}(h_i) \cap \left(\bigcup_{k=i+1}^{s} \left(\exp(h_k) + \mathbb{N}^p \right) \right) \neq \varnothing,$$

lo que es imposible ya que G y H son reducidas. □

[2.56]. Proposición ([39, Proposition 4.6]). *Si $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner a izquierda tal que $g_1R + \cdots + g_tR \subseteq Rg_1 + \cdots + Rg_t$, entonces G es una base de Gröbner a derecha.*

Demostración. Vamos a emplear [2.44.1]. Supongamos que G no es una base de Gröbner a derecha y sea $f \in g_1R + \cdots + g_tR$ satisfaciendo que $\mathrm{rres}(f, [G]) \neq 0$ y minimal con respecto a esta propiedad. Como $f \in Rg_1 + \cdots + Rg_t$ y G es una base de Gröbner a izquierda tenemos que $\mathrm{lres}(f, [G]) = 0$ y $\exp(f) \notin \bigcup_{i=1}^{t} \left(\exp(g_i) + \mathbb{N}^p \right)$. Necesariamente $\exp(\mathrm{rres}(f, [G])) < \exp(f)$ debido a la división fuerte. Finalmente $\mathrm{rres}(f, [G]) \in g_1R + \cdots + g_tR$ y $\mathrm{rres}(\mathrm{rres}(f, [G]), [G]) = \mathrm{rres}(f, [G]) \neq 0$ (ver el lema [2.27]), lo que contradice la minimalidad de f. □

2.6 Cálculo de bases de Gröbner.

Vamos a terminar el capítulo dando una versión del algoritmo de Buchberger para las álgebras de tipo PBW. En esta sección R será una $\Bbbk$–álgebra de tipo PBW sobre un dominio conmutativo noetheriano $\Bbbk$ en el que supondremos que podemos calcular de manera efectiva las operaciones usuales de un anillo, así como determinar si un elemento es una unidad y calcular su inverso. Supondremos además que los elementos $q_{\alpha,\beta}$ son unidades.

[2.57]. Dados dos elementos $\alpha, \beta \in \mathbb{N}^p$, definimos un nuevo elemento en $\mathbb{N}^p$, al que vamos a llamar $\mathrm{m}(\alpha, \beta)$, mediante la ecuación

$$\mathrm{m}(\alpha, \beta)_i = \max\{\alpha_i, \beta_i\}.$$

Es inmediato comprobar que $\mathrm{m}(\alpha,\beta)+\mathbb{N}^p = (\alpha+\mathbb{N}^p)\cap(\beta+\mathbb{N}^p)$. Dados dos elementos $f,g\in R$ definimos el *S–polinomio a izquierda* de f y g como

$$S^\ell(f,g) = \tfrac{\mathrm{lc}(g)}{q_{\gamma-\alpha,\alpha}}u_{\gamma-\alpha}f - \tfrac{\mathrm{lc}(f)}{q_{\gamma-\beta,\beta}}u_{\gamma-\beta}g,$$

donde $\alpha=\exp(f)$, $\beta=\exp(g)$ y $\gamma=\mathrm{m}(\alpha,\beta)$. Observemos que

$$\exp(S^\ell(f,g)) < \mathrm{m}(\exp(f),\exp(g)).$$

[2.58]. Teorema. *Sea $G=\{f_1,\dots,f_s\}$ un sistema de generadores para el ideal a izquierda $I\leq R$ tal que $\mathrm{lc}(f_i)$ es una unidad para cada i. G es una base de Gröbner para I si y sólo si para cualesquiera $i,j\in\{1,\dots,s\}$, $0\in\mathrm{LRes}(S^\ell(f_i,f_j),G)$.*

Demostración. Seguimos [44]. Una implicación es inmediata a partir de [2.41] dado que $S^\ell(f_i,f_j)\in I$. Para ver la otra implicación es suficiente con ver que $\mathrm{Exp}(I)\subseteq\bigcup_{i=1}^s(\exp(f_i)+\mathbb{N}^p)=\Gamma$. Sea por tanto

$$f=\sum_{i=1}^s g_if_i\in I \tag{2.3}$$

y vamos a introducir alguna notación. Llamamos $\gamma^i=\exp(g_if_i)$ y $\gamma=\max\{\gamma^1,\dots,\gamma^s\}$; sea $\{i_1,\dots,i_t\}$ el conjunto de índices para los cuales $\gamma^{i_j}=\gamma$. La demostración va a consistir en reescribir el elemento f como combinación lineal de los elementos f_i y de manera que γ y t vayan decreciendo, es decir, vamos a realizar inducción sobre γ y t. Si $t=1$ entonces $\exp(f)=\gamma=\exp(g_{i_1})+\exp(f_{i_1})\in\Gamma$, por lo que el teorema está demostrado en el caso $t=1$ (observemos que $\gamma\geq\exp(f)$). Supongamos pues que $t>1$. Llamemos además $\alpha^i=\exp(f_i)$, $\beta^i=\exp(g_i)$ y $\tau=\mathrm{m}(\alpha^{i_1},\alpha^{i_2})$. Consecuencia inmediata de las propiedades descritas en [2.57] es la existencia de un elemento $\delta\in\mathbb{N}^p$ tal que $\alpha^{i_1}+\beta^{i_1}=\gamma=\tau+\delta$, de donde $\beta^{i_1}=\tau-\alpha^{i_1}+\delta$. Sea

$$d_{i_1}=\tfrac{\mathrm{lc}(g_{i_1})}{q_{\tau-\alpha^{i_1},\delta}}u_\delta. \tag{2.4}$$

Utilizando las relaciones que definen R tenemos que

$$d_{i_1}u_{\tau-\alpha^{i_1}} = \mathrm{lm}(g_{i_1})-h_{i_1}, \tag{2.5}$$

donde $\exp(h_{i_1})<\beta^{i_1}$. De la ecuación 2.5 obtenemos

$$\begin{aligned} g_{i_1}f_{i_1} &= \mathrm{lm}(g_{i_1})f_{i_1}+\big(g_{i_1}-\mathrm{lm}(g_{i_1})\big)f_{i_1}\\ &= d_{i_1}u_{\tau-\alpha^{i_1}}f_{i_1}+h_{i_1}f_{i_1}+\big(g_{i_1}-\mathrm{lm}(g_{i_1})\big)f_{i_1}. \end{aligned} \tag{2.6}$$

Por otra parte, dado que $0 \in \mathrm{LRes}(S^\ell(f_{i_1}, f_{i_2}), G)$, podemos escribir

$$S^\ell(f_{i_1}, f_{i_2}) = \sum_{i=1}^{s} s_i f_i \quad \text{con} \quad \exp(s_i f_i) \leq \exp(S^\ell(f_{i_1}, f_{i_2})) < \tau \tag{2.7}$$

empleando división a izquierda. De la definición de S–polinomio podemos afirmar que

$$u_{\tau-\alpha^{i_1}} f_{i_1} = a S^\ell(f_{i_1}, f_{i_2}) + abu_{\tau-\alpha^{i_2}} f_{i_2}, \tag{2.8}$$

donde $a = \frac{q_{\alpha^{i_1}, \tau-\alpha^{i_1}}}{\mathrm{lc}(f_{i_2})}$ y $b = \frac{\mathrm{lc}(f_{i_1})}{q_{\alpha^{i_2}, \tau-\alpha^{i_2}}}$. Mezclando (2.3), (2.6), (2.7) y (2.8) tenemos:

$$\begin{aligned}
f &= g_{i_1} f_{i_1} + \sum_{j \neq i_1} g_j f_j \\
&= d_{i_1} u_{\tau-\alpha^{i_1}} f_{i_1} + h_{i_1} f_{i_1} + (g_{i_1} - \mathrm{lm}(g_{i_1}) f_{i_1} + \sum_{j \neq i_1} g_j f_j \\
&= d_{i_1} a S^\ell(f_{i_1}, f_{i_2}) + d_{i_1} abu_{\tau-\alpha^{i_2}} f_{i_2} \\
&\quad + h_{i_1} f_{i_1} + (g_{i_1} - \mathrm{lm}(g_{i_1})) f_{i_1} + \sum_{j \neq i_1} g_j f_j \\
&= ad_{i_1} \sum_{i=1}^{s} s_i f_i + abd_{i_1} u_{\tau-\alpha^{i_2}} f_{i_2} \\
&\quad + h_{i_1} f_{i_1} + (g_{i_1} - \mathrm{lm}(g_{i_1}) f_{i_1} + \sum_{j \neq i_1} g_j f_j \\
&= \big(ad_{i_1} s_{i_1} + h_{i_1} + (g_{i_1} - \mathrm{lm}(g_{i_1}))\big) f_{i_1} \\
&\quad + \big(abd_{i_1} u_{\tau-\alpha^{i_2}} + ad_{i_1} s_{i_2} + g_{i_1}\big) f_{i_1} \\
&\quad + \sum_{j \neq i_1, i_2} \big(ad_{i_1} s_j + g_j\big) f_j.
\end{aligned} \tag{2.9}$$

De esta manera (2.9) proporciona una nueva expresión para f,

$$f = \sum_{i=1}^{s} g'_i f_i,$$

donde

$$\begin{aligned}
g'_{i_1} &= ad_{i_1} s_{i_1} + h_{i_1} + (g_{i_1} - \mathrm{lm}(g_{i_1})) \\
g'_{i_2} &= abd_{i_1} u_{\tau-\alpha^{i_2}} + ad_{i_1} s_{i_2} + g_{i_1} \\
g'_j &= ad_{i_1} s_j + g_j \quad \text{si } j \neq i_1, i_2
\end{aligned} \tag{2.10}$$

Nos queda para terminar y poder aplicar el principio de inducción comprobar como son los exponentes $\exp(g_i' f_i)$. Observemos primeramente que

$$\begin{gathered}\exp(ad_{i_1} s_{i_1} f_{i_1}) = \delta + \exp(s_{i_1} f_{i_1}) < \delta + \tau = \gamma \\ \exp(h_{i_1} f_{i_1}) < \beta^{i_1} \alpha^{i_1} = \gamma \\ \exp((g_{i_1} - \operatorname{lm}(g_{i_1})) f_{i_1}) < \beta^{i_1} + \alpha^{i_1} = \gamma,\end{gathered}$$

luego

$$\exp(g_{i_1}' f_{i_1}) \leq \max\{\exp(ad_{i_1} s_{i_1} f_{i_1}), \exp(h_{i_1} f_{i_1}), \exp((g_{i_1} - \operatorname{lm}(g_{i_1})) f_{i_1})\} < \gamma. \tag{2.11}$$

Continuemos con i_2,

$$\begin{gathered}\exp(abd_{i_1} u_{\tau - \alpha^{i_2}} f_{i_2}) = \delta + \tau - \alpha^{i_2} + \alpha^{i_2} = \gamma \\ \exp(ad_{i_1} s_{i_1} f_{i_1}) = \delta + \exp(s_{i_1} f_{i_1}) < \delta + \tau = \gamma \\ \exp(g_{i_1} f_{i_1}) = \gamma,\end{gathered}$$

por tanto

$$\exp(g_{i_2}' f_{i_2}) \leq \max\{\exp(abd_{i_1} u_{\tau - \alpha^{i_2}} f_{i_2}), exp(ad_{i_1} s_{i_1} f_{i_1}), \exp(g_{i_1} f_{i_1})\} = \gamma. \tag{2.12}$$

Si $j \neq i_1, i_2$ entonces

$$\begin{gathered}\exp(ad_{i_0} s_j f_j) = \delta + \exp(s_j f_j) < \delta + \tau = \gamma \\ \exp(g_j f_j) = \gamma \quad \text{si } j \in \{i_1, \ldots, i_t\} \\ \exp(g_j f_j) < \gamma \quad \text{si } j \notin \{i_1, \ldots, i_t\},\end{gathered}$$

lo que implica que

$$\exp(g_j' f_j) \leq \max\{\exp(ad_{i_0} s_j f_j), \exp(g_j f_j)\} \begin{cases} = \gamma & \text{si } j \in \{i_1, \ldots, i_t\} \\ < \gamma & \text{si } j \notin \{i_1, \ldots, i_t\} \end{cases} \tag{2.13}$$

Como consecuencia de (2.11), (2.12) y (2.13), tenemos dos posibilidades: o el número de índices en el que se alcanza el máximo exponente de $\exp(g_i' f_i)$ es menor que t o dicho máximo exponente es menor que γ. Podemos por tanto concluir el resultado por inducción en t y γ. □

[2.59]. Corolario. *Si $I = Rf$ entonces $G = \{f\}$ es una base de Gröbner para I.*

De aquí al final del capítulo $\Bbbk$ *va a ser un cuerpo.*

[2.60]. El teorema [2.58] nos permite dar un algoritmo para el cálculo de una base de Gröbner: Sea $F = \{f_1, \ldots, f_s\}$ un sistema de generadores de un ideal I. El algoritmo tiene los siguientes pasos

Paso 1. Llamamos $F_0 = F$, $k = 0$.

Paso 2. Para cada par $f, g \in F_k$ elegimos $r_{f,g} \in \mathrm{LRes}(S^\ell(f,g), F_k)$.

Paso 3. Llamamos $R_k = \{r_{f,g} \mid f, g \in F_k\}$, $F_{k+1} = F_k \cup (R_k \setminus \{0\})$.

Paso 4. Si $F_k = F_{k+1}$ entonces el algoritmo termina y F_k es una base de Gröbner para I.

Paso 5. Si $F_k \neq F_{k+1}$ entonces $k = k + 1$ y volvemos al Paso 2.

En el paso 2 podemos tomar $r_{f,g} = \mathrm{lres}(S^\ell(f,g), [F_h])$. Nos queda justificar que el algoritmo termina y lo hace correctamente. Para ver que termina consideremos la siguiente cadena de subconjuntos de I:

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \cdots$$

Esta cadena nos da una cadena ascendente de monoideales

$$\mathrm{Exp}(F_0) + \mathbb{N}^p \subseteq \mathrm{Exp}(F_1) + \mathbb{N}^p \subseteq \cdots \subseteq \mathrm{Exp}(F_n) + \mathbb{N}^p \subseteq \cdots,$$

Dado que $\mathbb{N}^p$ es noetheriano (resultado equivalente al Lema de Dickson que aparece en [1.6]) existe un natural $h \in \mathbb{N}$ tal que $\mathrm{Exp}(F_h) + \mathbb{N}^p = \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p$.

Lema. *Si* $\mathrm{Exp}(F_h) + \mathbb{N}^p = \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p$ *entonces* $F_h = F_{h+1}$.

Demostración. Supongamos que existe un elemento $r \in F_{h+1} \setminus F_h$, entonces existen $f, g \in F_h$ tales que $r \in \mathrm{LRes}(S^\ell(f,g), F_h)$. Como $r \neq 0$ tenemos que $\mathcal{N}(r) \neq \varnothing$, y como $\mathcal{N}(r) \cap \mathrm{Exp}(F_h) + \mathbb{N}^p = \varnothing$ obtenemos

$$\mathrm{Exp}(F_h) + \mathbb{N}^p \subsetneq \mathrm{Exp}(F_h \cup \{r\}) + \mathbb{N}^p \subseteq \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p = \mathrm{Exp}(F_h) + \mathbb{N}^p,$$

lo que es imposible. Por tanto $F_h = F_{h+1}$. □

El lema y la noetherianidad de $\mathbb{N}^p$ nos garantiza que el algoritmo termina, y que termina correctamente viene demostrado en el siguiente lema

Lema. *Si* $F_h = F_{h+1}$ *entonces* F_h *es un base de Gröbner.*

Demostración. Si $F_h = F_{h+1}$ entonces para cualesquiera $f, g \in F_h$, $0 \in \mathrm{LRes}(S^\ell(f,g), F_h)$, y el resultado es consecuencia del teorema [2.58]. □

[2.61]. Ejemplo. Vamos a ilustrar el algoritmo con un ejemplo. Llamemos $U = U(\mathfrak{sl}(2))$ el álgebra envolvente del álgebra de Lie $\mathfrak{sl}(2)$. Ésta tiene tres generadores $\{x, y, h\}$ y corchete de Lie

$$[x,y] = h, \quad [x,h] = -2x, \quad [y,h] = 2y.$$

El conjunto $\{x^i y^j h^k \mid (i,j,k) \in \mathbb{N}^3\}$ es una $\Bbbk$–base para U. Además, como se ha visto en [2.15], el orden lexicográfico graduado, con $\epsilon_1 < \epsilon_2 < \epsilon_3$, dota a U de estructura de álgebra de tipo PBW. Vamos a cálcular una base de Gröbner para el ideal $I = Ux^2 + Uy^2 + Uh^2$. Siguiendo el agoritmo [2.60], llamamos

$$F_0 = \{x^2, y^2, h^2\}$$

y calculamos los posibles S–polinomios:

$$\begin{aligned} S(x^2, y^2) &= -4xyh + 2h^2 + 2h \\ S(x^2, h^2) &= 8x^2 + 16x^2 \\ S(y^2, h^2) &= -8y^2h + 16y^2. \end{aligned}$$

Como $-4xyh + 2h \in \mathrm{LRes}(S(x^2, y^2), F_0)$, $0 \in \mathrm{LRes}(S(x^2, h^2), F_0)$, y $0 \in \mathrm{LRes}(S(y^2, h^2), F_0)$, tenemos que

$$F_1 = \{x^2, y^2, h^2, 2xyh - h\}$$

Continuamos con el cálculo de F_2. Observemos que no es necesario calcular los elementos $S(f,g)$ si $f, g \in F_0$. Por tanto,

$$\begin{aligned} S(x^2, 2xyh - h) &= -4xh^2 - 18xh + 8x^2y - 16x \\ S(y^2, 2xyh - h) &= -8xy^2 + 2yh^2 - 3yh \\ S(h^2, 2xyh - h) &= h^2 \end{aligned}$$

y los restos que obtenemos son $-2xh \in \mathrm{LRes}(S(x^2, 2xyh - h), F_1)$, $-3yh \in \mathrm{LRes}(S(y^2, 2xyh - h), F_1)$ y $0 \in \mathrm{LRes}(S(h^2, 2xyh - h), F_1)$, de donde

$$F_2 = \{x^2, y^2, h^2, 2xyh - h, xh, yh\}.$$

Pasamos a F_3. Obtenemos los siguientes S–polinomios,

$$\begin{aligned} S(x^2, xh) &= 4x^2 \\ S(x^2, yh) &= -2xh^2 - 10xh + 4x^2y - 8x \\ S(y^2, xh) &= -4xy^2 + 2yh^2 - 2yh \\ S(y^2, yh) &= -4y^2 \\ S(h^2, xh) &= -2xh \\ S(h^2, yh) &= 2yh \\ S(2xyh - h, xh) &= 2h^2 - h \\ S(2xyh - h, yh) &= -h. \end{aligned}$$

En todos los conjuntos de restos aparece el 0 salvo $-h \in \mathrm{LRes}(S(2xyh - h, xh), F_2)$ y $-h \in \mathrm{LRes}(S(2xyh - h, yh), F_2)$, por lo que

$$F_3 = \{x^2, y^2, h^2, 2xyh - h, xh, yh, h\}.$$

Por último, dado que

$$\begin{aligned} S(x^2, h) &= 4x^2 \\ S(y^2, h) &= -4y^2 \\ S(h^2, h) &= 0 \\ S(2xyh - h, h) &= -h \\ S(xh, h) &= 0 \\ S(yh, h) &= 0, \end{aligned}$$

tenemos que 0 es resto para todos los elementos anteriores, por consiguiente $F_4 = F_3$. Necesariamente $G = \{x^2, y^2, h^2, 2xyh - h, xh, yh, h\}$ es una base de Gröbner para I.

[2.62]. Vamos a dar explícitamente dos algoritmos, uno para calcular una base de Gröbner minimal a partir de una base de Gröbner y otro para calcular la base de Gröbner reducida a partir de una minimal. Se basan en los resultados [1.7] y la demostración de [2.53].

El primer algoritmo tiene como entrada una base de Gröbner G de un ideal I, y como salida una base de Gröbner minimal G' para I.

Paso 1. $G_0 = G$, $k = 0$.

Paso 2. Si existe $g \in G_k$ tal que $\exp(g) \in \mathrm{Exp}(G_k \setminus \{g\}) + \mathbb{N}^p$ entonces $G_{k+1} = G_k \setminus \{g\}$, $k = k + 1$ y repetimos el paso 2.

Paso 3. Si no, $G' = G_k$.

El segundo algoritmo tiene como entrada una base de Gröbner minimal G para I y como salida una base de Gröbner reducida G' para I. Supondremos que $\Bbbk$ es un cuerpo.

Paso 1. $G = \{g_1, \ldots, g_m\}$

Paso 2. Para cada $i = 1, \ldots, m$ escogemos $g_i' \in \mathrm{LRes}(g_i, G \setminus \{g_i\})$.

Paso 3. Para cada $i = 1, \ldots, m$ $g_i'' = (\mathrm{lc}(g_i'))^{-1} g_i'$.

Paso 4. $G' = \{g_1'', \ldots, g_m''\}$.

[2.63]. Ejemplo. Vamos a clacular una base de Gröbner reducida para I en el ejemplo [2.61]. Eliminando los elementos sobrantes tenemos que $G = \{x^2, y^2, h\}$ es una base de Gröbner minimal para I que directamente sale reducida.

[2.64]. Vamos a terminar dando un algoritmo para calcular una base de Gröbner de un ideal bilátero I. Antes de comenzar es conveniente observar algunos hechos. Si tenemos un conjunto de generadores de I como ideal a izquierda entonces el algoritmo dado en [2.60] nos proporciona directamente una base de Grobner para I, como veremos en [2.66]. Necesitamos entonces conseguir conjuntos que generen al ideal a un solo lado. De hecho, el corolario [2.38] nos garantiza que una base de Gröbner para I lo genera a izquierda y derecha. Dado un subconjunto $F \subseteq R$, notaremos RF, resp. FR, resp. RFR al ideal a izquierda, resp. derecha, resp. bilátero generado por F.

[2.65]. Lema ([39, Lemma 5.1]). *Sea $F = \{f_1, \ldots, f_s\} \subseteq R$. Las siguientes afirmaciones son equivalentes:*

[a] $FR \subseteq RF$.

[b] $RF = RFR$.

[c] *Para todo $\alpha \in \mathbb{N}^p$ y todo $f_i \in F$, $f_i u_\alpha \in RF$.*

[d] *Para todo $f_i \in F$ y todo $j \in \{1, \ldots, p\}$, $f_i u_{\epsilon_j} \in RF$.*

Demostración. Que [a] implica [d] es inmediato.

La implicación [d] $\Rightarrow$ [c] es análoga a [2.6]: procedemos por inducción sobre α. Si $\alpha = 0$ entonces $u_\alpha = 1$ trivializa el resultado. Supongamos $\alpha > 0$, entonces $\alpha = \beta + \epsilon_j$. Tenemos que

$$u_\alpha = u_{\beta+\epsilon_j} = q_{\beta,\epsilon_j}^{-1} u_\beta u_{\epsilon_j} + \sum_{\gamma<\alpha} c_\gamma u_\gamma,$$

luego

$$f_i u_\alpha = q_{\beta,\epsilon_i}^{-1} f_i u_\beta u_{\epsilon_j} + \sum_{\gamma<\alpha} c_\gamma f_i u_\gamma. \tag{2.14}$$

Por inducción $f_i u_\gamma \in RF$ y $f_i u_\beta \in RF$, luego $f_i u_\beta = \sum_{i=1}^{s} p_i f_i$, con lo que (2.14) se convierte en

$$f_i u_\alpha = q_{\beta,\epsilon_i}^{-1} \sum_{k=1}^{s} p_k f_k u_{\epsilon_j} + \sum_{\gamma<\alpha} c_\gamma f_i u_\gamma.$$

Por hipótesis $f_k u_{\epsilon_j} \in RF$, luego tenemos el resultado.

[c] implica [b] porque si $f \in RFR$ entonces f se puede escribir como $f = \sum r_{i,\alpha} f_i u_\alpha \in RF$.

Por último, como $FR \subseteq RFR$ tenemos que [b] implica [a]. □

Vamos a decir que G es una base de Gröbner bilátera si G es una base de Gröbner para el ideal bilátero que genera.

[2.66]. Proposición. *Sea $G = \{g_1, \ldots, g_t\} \subseteq R$. G es una base de Gröbner bilátera si y sólo si G es una base de Gröbner a izquierda y $RG = RGR$.*

Demostración. Si G es una base de Gröbner bilátera entonces

$$\mathrm{Exp}(RGR) = \bigcup_{i=1}^{t} \left(\exp(g_i) + \mathbb{N}^p\right) \subseteq \mathrm{Exp}(RG) \subseteq \mathrm{Exp}(RGR),$$

por lo que G es una base de Gröbner a izquierda. Además, [2.38] garantiza que $RG = RGR$.

Por otra parte, si G es una base de Gröbner a izquierda y $RG = RGR$ entonces para cualquier $\alpha \in \mathrm{Exp}(RGR)$ existe un elemento $f \in RGR = RG$ tal que $\exp(f) = \alpha$. Como G es base de Gröbner a izquierda tenemos que $\alpha \in \bigcup_{i=1}^{t} \left(\exp(g_i) + \mathbb{N}^p\right)$, como queríamos. □

[2.67]. El lema [2.65] y la proposición [2.66] nos proporcionan un algoritmo para calcular una base de Gröbner de un ideal bilátero a partir de un conjunto de generadores F. La entrada es F y la salida G, una base de Gröbner para RFR.

Paso 1. $F_0 = F$, $k = 0$.

Paso 2. Calcula G_k una base de Gröbner para RF_k utilizando [2.60].

Paso 3. Para cada $g \in G_k$ y cada $j \in \{1, \ldots, p\}$ elige un $r_{g,j} \in \mathrm{LRes}(gu_{\epsilon_j}, G_k)$ (podemos tomar $r_{g,j} = \mathrm{lres}(gu_{\epsilon_j}, [G_k])$).

Paso 4. $F_{k+1} = (G_k \cup \{r_{g,j} \mid g \in G_k, 1 \leq j \leq p\}) \setminus \{0\}$.

Paso 5. Si $F_{k+1} = G_k$ el algoritmo termina y $G = G_k$ es la base de Gröbner buscada.

Paso 6. Si $F_{k+1} \neq G_k$, cambiamos $k = k + 1$ y volvemos al paso 2.

Lema. *Si $F_{k+1} = G_k$ entonces G_k es una base de Gröbner bilátera*

Demostración. Como $F_{k+1} = G_k$, $0 \in \mathrm{LRes}(gu_{\epsilon_j}, G_k)$ para cualesquiera $g \in G_k$ y $j \in \{1, \ldots, p\}$, y por lo tanto $gu_{\epsilon_j} \in RG_k$. Ahora, por [2.65] $RG_k = RG_kR$ y como G_k es una base de Gröbner a izquierda podemos aplicar [2.66]. □

Una vez visto que cuando el algoritmo termina lo hace correctamente, nos queda ver que termina. La siguiente cadena de subconjuntos

$$F = F_0 \subseteq G_0 \subseteq \cdots \subseteq F_k \subseteq G_k \subseteq F_{k+1} \subseteq \cdots$$

Proporciona una cadena de monoideales en $\mathbb{N}^p$

$$\begin{aligned}\mathrm{Exp}(F_0) + \mathbb{N}^p \subseteq \mathrm{Exp}(G_0) + \mathbb{N}^p \subseteq \cdots \\ \subseteq \mathrm{Exp}(F_k) + \mathbb{N}^p \subseteq \mathrm{Exp}(G_k) + \mathbb{N}^p \subseteq \mathrm{Exp}(F_{k+1}) + \mathbb{N}^p \subseteq \cdots\end{aligned}$$

que debe estacionar por ser $\mathbb{N}^p$ noetheriano, luego existe $h \in \mathbb{N}$ tal que $\mathrm{Exp}(G_h) + \mathbb{N}^p = \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p$. Veamos que esta propiedad implica la terminación del algoritmo:

Lema. *Si* $\mathrm{Exp}(G_h) + \mathbb{N}^p = \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p$ *entonces* $G_h = F_{h+1}$.

Demostración. Supongamos por el contrario que existe $r \in F_{h+1} \setminus G_h$, entonces existen $g \in G_k$ y $j \in \{1, \ldots, p\}$ tales que $0 \neq r \in \mathrm{LRes}(gu_{\epsilon_j}, G_h)$. Como $\mathcal{N}(r) \cap \big(\mathrm{Exp}(G_h) + \mathbb{N}^p\big) = \varnothing$ tenemos que $\exp(r) \notin \mathrm{Exp}(G_h) + \mathbb{N}^p = \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p$, pero $r \in F_{h+1}$, lo que es contradictorio. Por consiguiente $G_h = F_{h+1}$. □

[2.68]. Ejemplo. Consuderemos la $\Bbbk$–álgebra R generada por x, y con relacion $yx = qxy + 1$, donde $q \in \Bbbk^\times$, $q \neq 1$. Una $\Bbbk$–base viene dada por $\{x^i y^j \mid (i,j) \in \mathbb{N}^2\}$. El orden lexicográfico graduado con $\epsilon_2 > \epsilon_1$ convierte a R en un álgebra de tipo PBW. Vamos a calcular una base de Gröbner del ideal bilátero generado por $(x-1)$, al que llamamos I. Para empezar, $F_0 = \{x-1\}$ y por tanto $G_0 = \{x-1\}$. Debemos por tanto multiplicar $x-1$ por las dos variables. Para empezar,

$$(x-1)x = x^2 - x = x(x-1),$$

luego su resto de la división por G_0 es cero. Para la variable y,

$$(x-1)y = xy - y = q^{-1}y(x-1) + (q^{-1}-1)y - q^{-1},$$

luego el resto obtenido es $y + \frac{1}{q-1}$. Por tanto, $F_1 = \{x-1, y+\frac{1}{q-1}\}$. Para calcular G_1, debemos calcular un S–polinomio,

$$S(x-1, y+\tfrac{1}{q-1}) = 1 - y - \tfrac{q}{q-1}x = -(y+\tfrac{1}{q-1}) - \tfrac{q}{q-1}(x-1),$$

por lo que $0 \in \mathrm{LRes}(S(x-1, y+\frac{1}{q-1}), F_1)$. Tenemos que $G_1 = F_1$. Multiplicamos de nuevo por las variables. El elemento $x-1$ no es necesario, ya que fue multipicado por x e y al inicio.

$$(y+\tfrac{1}{q-1})y = y^2 + \tfrac{1}{q-1}y = y(y+\tfrac{1}{q-1}),$$

lo que nos proporciona un resto cero. Por otra parte,

$$(y+\tfrac{1}{q-1})x = yx + \tfrac{1}{q-1}x = qx(y+\tfrac{1}{q-1}) - (x-1)$$

que también da cero de resto. Hemos obtenido que $F_2 = G_1$, por lo que $G = \{x-1, y+\frac{1}{q-1}\}$ es una base de Gröbner para I.

3. MÓDULOS SOBRE ÁLGEBRAS DE TIPO PBW.

A lo largo de este capítulo R será un álgabra de tipo PBW sobre un dominio conmutativo noetheriano $\Bbbk$ con base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$, orden '$\leq$' y en la que además los elementos $q_{\alpha,\beta}$ son unidades de $\Bbbk$ para cualesquiera $\alpha, \beta \in \mathbb{N}^p$. El objetivo de este capítulo consiste en desarrollar métodos efectivos para estudiar módulos finitamente generados sobre R. Si no se indica lo contrario, entenderemos que los módulos son a izquierda.

Muchas de las ideas en las que se basa este capítulo provienen del caso conmutativo, más concretamente de las monografías [1, 4]. Ya dentro del caso no conmutativo, en [14] el autor introduce algoritmos de división para módulos sobre álgebras de operadores diferenciales, aplicando sus resultados al cálculo de multiplicidades. También es conveniente citar [24], donde aparece la ideal de utilizar los subconjuntos estables para estudiar submódulos de módulos libres.

3.1 Bases de Gröbner para submódulos de R^n.

Dado que todo módulo finitamente generado sobre R es un cociente de un R–módulo libre finitamente generado vamos a empezar estudiando una representación adecuada para el módulo libre R^n sobre R con base $\mathbf{e}_1, \ldots, \mathbf{e}_n$, es decir,

$$\mathbf{e}_i = [0, \ldots, \overset{(i)}{1}, \ldots, 0] \quad \text{con } i = 1, \ldots, n.$$

Todo elemento de R^n se escribe de manera única como

$$\mathbf{f} = \sum_{i=1}^{n} f_i \mathbf{e}_i.$$

con $f_1, \ldots, f_n \in R$.

[3.1]. Lema. *El conjunto* $\{u_\alpha \mathbf{e}_i \mid \alpha \in \mathbb{N}^p, 1 \leq i \leq n\}$ *es una* $\Bbbk$*–base para* R^n.

Demostración. Inmediata. □

Llamaremos $\mathbf{u}_{(\alpha,i)} = u_\alpha \mathbf{e}_i$.

Para estudiar el álgebra R hemos utilizado de manera esencial el poder indexar una $\Bbbk$–base de R en $\mathbb{N}^p$ y en el estudio de las propiedades aditivas de $\mathbb{N}^p$ con respecto a un cierto orden. En nuestro estudio de módulos libres debemos acometer un estudio similar.

[3.2]. Ya sabemos que el R–módulo libre R^n tiene por $\Bbbk$–base el conjunto $\{\mathbf{u}_\mathfrak{a} \mid \mathfrak{a} \in \mathbb{N}^{p,n}\}$ (véase [3.1]), por lo que todo elemento $\mathbf{f} \in R^n$ tiene una representación única como

$$\mathbf{f} = \sum_{\mathfrak{a} \in \mathbb{N}^{p,n}} c_{\mathfrak{a},\mathbf{f}} \mathbf{u}_\mathfrak{a}.$$

Análogamente a la propia álgebra R, y fijado un orden admisible $\prec$ sobre $\mathbb{N}^{p,n}$, definimos el *diagrama de Newton* de $\mathbf{f}$ como el conjunto

$$\mathcal{N}(\mathbf{f}) = \{\mathfrak{a} \in \mathbb{N}^{p,n} \mid c_{\mathfrak{a},\mathbf{f}} \neq 0\}$$

Como dicho conjunto es finito podemos definir

$$\exp(\mathbf{f}) = \max \mathcal{N}(\mathbf{f}),$$

lo que llamamos *exponente* de $\mathbf{f}$. También llamaremos *coeficiente líder* y *monomio líder* a los elementos

$$\operatorname{lc}(\mathbf{f}) = c_{\exp(\mathbf{f}),\mathbf{f}} \qquad \operatorname{lm}(\mathbf{f}) = \operatorname{lc}(\mathbf{f})\mathbf{u}_{\exp(\mathbf{f})}$$

[3.3]. Lema. *Dados $\mathbf{f}, \mathbf{g} \in R^n$ se verifican las siguientes propiedades:*

[3.3.1]. $\mathcal{N}(\mathbf{f}+\mathbf{g}) \subseteq \mathcal{N}(\mathbf{f}) \cup \mathcal{N}(\mathbf{g})$

[3.3.2]. $\exp(\mathbf{f}+\mathbf{g}) \preceq \max\{\exp(\mathbf{f}), \exp(\mathbf{g})\}$, *siendo la desigualdad estricta si y sólo si* $\operatorname{lm}(\mathbf{f}) = -\operatorname{lm}(\mathbf{g})$.

Demostración. Inmediata. □

[3.4]. Proposición. *Sea $\prec$ el orden TOP o el orden POT sobre $\mathbb{N}^{p,n}$. Dados $f \in R$, $\mathbf{g} \in R^n$ tenemos:*

1. $\exp(f\mathbf{g}) = \exp(f) + \exp(\mathbf{g})$.
2. $\operatorname{lc}(f\mathbf{g}) = q_{\exp(f),\alpha} \operatorname{lc}(f) \operatorname{lc}(\mathbf{g})$, *donde* $\exp(\mathbf{g}) = (\alpha, i)$.

Demostración. A partir de la fórmula

$$\begin{aligned} u_\alpha \mathbf{u}_{(\beta,i)} &= u_\alpha u_\beta \mathbf{e}_i \\ &= q_{\alpha,\beta} u_{\alpha+\beta}\mathbf{e}_i + \sum_{\gamma<\alpha+\beta} c_\gamma u_\gamma \mathbf{e}_i \\ &= q_{\alpha,\beta}\mathbf{u}_{(\alpha+\beta,i)} + \sum_{\gamma<\alpha+\beta} c_\gamma \mathbf{u}_{(\gamma,i)} \end{aligned}$$

y dado que $\gamma < \alpha+\beta$ implica $(\gamma,i) \prec (\alpha+\beta,i)$, el resultado se obtiene fácilmente por inducción sobre $\exp(f)$ y $\exp(\mathbf{g})$. □

Similarmente a los subconjuntos de R, Dado un subconjunto $F \subseteq R^n$, definimos su exponente como el conjunto

$$\mathrm{Exp}(F) = \{\exp(\mathbf{f}) \mid \mathbf{f} \in F, \mathbf{f} \neq 0\}.$$

[3.5]. Lema. *Si K es un submódulo a izquierda de R^n entonces* $\mathrm{Exp}(K)$ *es un subconjunto estable de* $\mathbb{N}^{p,n}$.

Demostración. Tenemos que demostrar la inclusión $\mathrm{Exp}(K)+\mathbb{N}^p \subseteq \mathrm{Exp}(K)$, escojamos $(\alpha,i) \in \mathrm{Exp}(K)$ y $\beta \in \mathbb{N}^p$. Existe un elemento $\mathbf{f} \in K$ tal que $\exp(\mathbf{f}) = (\alpha,i)$. Como K es un submódulo $u_\beta \mathbf{f} \in K$. Por otra parte $\exp(u_\beta \mathbf{f}) = \exp(u_\beta) + \exp(\mathbf{f}) = \beta + (\alpha,i)$, luego $(\alpha+\beta,i) \in \mathrm{Exp}(K)$. □

De manera análoga a [2.20], [1.13] nos proporciona el corolario siguiente:

[3.6]. Corolario. *Dado un submódulo a izquierda $K \subseteq R^n$, existen elementos $\mathbf{f}_1,\ldots,\mathbf{f}_m \in K$ tales que*

$$\mathrm{Exp}(K) = \bigcup_{i=1}^{m} \big(\exp(\mathbf{f}_i) + \mathbb{N}^p\big).$$

[3.7]. Un subconjunto $G = \{\mathbf{g}_1,\ldots,\mathbf{g}_m\}$ de $K \subseteq R^n$ es una *base de Gröbner* para K si

$$\mathrm{Exp}(K) = \bigcup_{i=1}^{m} \big(\exp(\mathbf{g}_i) + \mathbb{N}^p\big).$$

Como consecuencia del corolario anterior tenemos:

Proposición. *Sea R un álgebra de tipo PBW y sea $K \subseteq R^n$ un submódulo a izquierda. Existe una base de Gröbner para K.*

Utilizando sistemas de generadores minimales de conjuntos estables podemos definir el concepto de base de Gröbner minimal para un submódulo de R^n de manera completamente paralela a [2.23].

3.2 División y algoritmo de Buchberger para módulos.

De nuevo R es un álgebra de tipo PBW con orden $\leq$, y $\preceq$ representa a cualquiera de los ordenes POT o TOP sobre $\mathbb{N}^{p,n}$.

[3.8]. Partimos de un conjunto finito $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ de elementos de R^n, o mejor dicho, de una upla (ordenada) $[F] = [\mathbf{f}_1, \ldots, \mathbf{f}_m]$ de elementos no nulos de R^n. Asociada a esta upla definimos una partición $\mathbf{\Delta}^{[F]}$ en $\mathbb{N}^{p,n}$:

$$\begin{aligned} \Delta_1 &= \exp(\mathbf{f}_1) + \mathbb{N}^p \\ &\vdots \\ \Delta_i &= \big(\exp(\mathbf{f}_i) + \mathbb{N}^p\big) \setminus \big(\Delta_1 \cup \cdots \cup \Delta_{i-1}\big) \\ &\vdots \\ \overline{\Delta} &= \mathbb{N}^{p,n} \setminus \big(\Delta_1 \cup \cdots \cup \Delta_m\big). \end{aligned} \tag{3.1}$$

Observemos que $\Delta_1 \cup \cdots \cup \Delta_m$ es un subconjunto estable que viene generado por $\{\exp(\mathbf{f}_1), \ldots, \exp(\mathbf{f}_m)\}$, y que cada cada conjunto Δ_i está en un sólo nivel.

[3.9]. Teorema. *Si $[F]$ es una upla en la que $\mathrm{lc}(\mathbf{f}_i)$ es una unidad de $\Bbbk$ para todo $i = 1, \ldots, m$, y $\mathbf{f} \in R^n$, entonces existen elementos únicos $q_1, \ldots, q_m \in R$, $\mathbf{r} \in R^n$ tales que:*

1. $\mathbf{f} = \sum_{i=1}^m q_i \mathbf{f}_i + \mathbf{r}$.
2. $\mathcal{N}(\mathbf{r}) \subseteq \overline{\Delta}$ *y* $\exp(\mathbf{r}) \preceq \exp(\mathbf{f})$.
3. $\exp(\mathbf{f}_i) + \mathcal{N}(q_i) \subseteq \Delta_i$ *y* $\exp(q_i \mathbf{f}_i) \preceq \exp(\mathbf{f})$.

Además, $\exp(\mathbf{f}) = \exp(\mathbf{r})$ *si y sólo si* $\exp(\mathbf{f}) \in \overline{\Delta}$ *y* $\exp(q_i \mathbf{f}_i) = \exp(\mathbf{f})$ *si y sólo si* $\exp(\mathbf{f}) \in \Delta_i$.

Demostración. Veamos la existencia de los cocientes y el resto. Primeramente, dado que los coeficientes líderes de cada $\mathbf{f}_i$ son unidades, podemos suponer que todos son 1. La demostración la vamos a realizar por inducción sobre $\exp(\mathbf{f})$. Si $\exp(\mathbf{f}) = (\mathbf{0}, 1)$, entonces $\mathbf{f} = k\mathbf{e}_1$, con lo que podemos hacer $q_{i_0} = k$ para el primer índice i_0 tal que $\exp(\mathbf{f}_{i_0}) = (\mathbf{0}, 1)$, $q_i = 0$ si $i \neq i_0$, y $\mathbf{r} = 0$, o $\mathbf{r} = \mathbf{f}$, $q_i = 0$ si $\exp(\mathbf{f}_i) \neq (\mathbf{0}, 1)$ para todo i. Supongamos por consiquiente que $\exp(\mathbf{f}) \succ (\mathbf{0}, 1)$. Dado que los conjuntos $\Delta_1, \ldots, \Delta_m, \overline{\Delta}$ constituyen una partición de $\mathbb{N}^{p,n}$, tenemos que $\exp(\mathbf{f}) \in \Delta_{i_0}$ para un único i_0 o $\exp(\mathbf{f}) \in \overline{\Delta}$. Si $\exp(\mathbf{f}) \in \overline{\Delta}$, llamamos $\mathbf{f}' = \mathbf{f} - \mathrm{lm}(\mathbf{f})$. Como $\exp(\mathbf{f}') \prec \exp(\mathbf{f})$, por hipótesis de inducción

$$\mathbf{f}' = \sum_{i=1}^m q_i \mathbf{f}_i + \mathbf{r}',$$

de donde

$$\mathbf{f} = \sum_{i=1}^{m} q_i \mathbf{f}_i + \big(\operatorname{lm}(\mathbf{f}) + \mathbf{r}'\big)$$

satisface las propiedades requeridas. Observemos que en este caso $\exp(\mathbf{f}) = \exp(\mathbf{r})$, donde $\mathbf{r} = \operatorname{lm}(\mathbf{f}) + \mathbf{r}'$, y $\exp(q_i\mathbf{f}_i) \preceq \exp(\mathbf{f}') \prec \exp(\mathbf{f})$. Por otra parte, si $\exp(\mathbf{f}) \in \Delta_{i_0}$, entonces $\exp(\mathbf{f}) = \beta + \exp(\mathbf{f}_{i_0})$ para un cierto $\beta \in \mathbb{N}^p$. Como $\operatorname{lc}(\mathbf{f}_{i_0}) = 1$,

$$\operatorname{lc}\left(\tfrac{\operatorname{lc}(\mathbf{f})}{q_{\beta,\varphi}} u_\beta \mathbf{f}_{i_0}\right) = q_{\beta,\varphi} \tfrac{\operatorname{lc}(\mathbf{f})}{q_{\beta,\varphi}} \operatorname{lc}(\mathbf{f}_{i_0}) = \operatorname{lc}(\mathbf{f}),$$

con $\exp(\mathbf{f}_{i_0}) = (\varphi, i)$, de donde $\mathbf{f}' = \mathbf{f} - \frac{\operatorname{lc}(\mathbf{f})}{q_{\beta,\varphi}} u_\beta \mathbf{f}_{i_0}$ satisface que $\exp(\mathbf{f}') \prec \exp(\mathbf{f})$. Por la hipótesis de inducción,

$$\mathbf{f}' = \sum_{i \neq i_0} q_i \mathbf{f}_i + q'_{i_0} \mathbf{f}_{i_0} + \mathbf{r}.$$

Llamemos $q_{i_0} = \frac{\operatorname{lc}(\mathbf{f})}{q_{\beta,\varphi}} u_\beta + q'_{i_0}$. Es evidente que esta descomposición satisface las propiedades 1 y 2 del teorema y la 3 si $i \neq i_0$. Si $\alpha \in \mathcal{N}(q_{i_0})$ entonces $\alpha \in \mathcal{N}(q'_{i_0})$ o $\alpha = \beta$. En el primer caso $\alpha + \exp(\mathbf{f}_{i_0}) \in \Delta_{i_0}$ por hipótesis de inducción, y en el segundo caso $\beta + \exp(\mathbf{f}_{i_0}) = \exp(\mathbf{f}) \in \Delta_{i_0}$. Además, en vista de que

$$\exp(q'_{i_0}\mathbf{f}_{i_0}) \preceq \exp(\mathbf{f}') \prec \exp(\mathbf{f}) \text{ y } \exp\left(\tfrac{\operatorname{lc}(\mathbf{f})}{q_{\beta,\varphi}} u_\beta \mathbf{f}_{i_0}\right) = \exp(\mathbf{f}),$$

obtenemos la siguiente igualdad:

$$\exp(q_{i_0}\mathbf{f}_{i_0}) = \exp(\mathbf{f}).$$

Nótese que $\exp(q_i\mathbf{f}_i) \preceq \exp(\mathbf{f}') \prec \exp(\mathbf{f})$ si $i \neq i_0$, y $\exp(\mathbf{r}) \preceq \exp(\mathbf{f}') \prec \exp(\mathbf{f})$.

La unicidad se demuestra de manera idéntica al lema [2.26]. □

Llamaremos cocientes a los elementos q_i y resto al elemento $\mathbf{r}$. Al resto de dividir $\mathbf{f}$ por la upla $[F]$ lo notaremos $\operatorname{lres}(\mathbf{f}, [F])$ o $\operatorname{lres}(\mathbf{f}, F)$ abusando del lenguaje.

[3.10]. El anterior es el algoritmo de la división a izquierda fuerte en R^n. Podemos dar también un algoritmo de la división a izquierda débil, es decir, para cualesquiera $\mathbf{f}, \mathbf{f}_1, \ldots, \mathbf{f}_m \in R$, con $\operatorname{lc}(\mathbf{f}_i)$ una unidad de $\Bbbk$, existen $q_1, \ldots, q_m \in R$, $\mathbf{r} \in R^n$ tales que

1. $\mathbf{f} = \sum_{i=1}^{m} q_i \mathbf{f}_i + \mathbf{r}$,
2. $\mathcal{N}(\mathbf{r}) \cap \left(\bigcup_{i=1}^{m} \left(\exp(\mathbf{f}_i) + \mathbb{N}^p \right) \right) = \varnothing$ y $\exp(\mathbf{r}) \preceq \exp(\mathbf{f})$,
3. $\exp(q_i \mathbf{f}_i) \preceq \exp(\mathbf{f})$.

Dado que no hay unicidad ni en cocientes ni en restos vamos a llamar $\mathrm{LRes}(\mathbf{f}, F)$ al conjunto de todos los restos que se obtienen al dividir débilmente $\mathbf{f}$ por F.

Al igual que en el caso $n = 1$ tenemos que $\mathrm{lres}(\mathbf{f}, F) \in \mathrm{LRes}(\mathbf{f}, F)$.

Para submódulos a derecha podemos desarrollar algoritmos de la división a derecha análogos a los anteriores, donde usaremos la notación $\mathrm{rres}(f, [F])$, $\mathrm{RRes}(f, F)$.

Antes de dar el algoritmo de Buchberger para módulos es conveniente dar versiones de [2.39] y [2.41] para módulos:

[3.11]. Proposición.

[3.11.1]. *Sean* $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ *y* $G' = \{\mathbf{g}'_1, \ldots, \mathbf{g}'_s\}$ *dos bases de Gröbner para el submódulo a izquierda* $K \subseteq R^n$, *y sea* $\mathbf{f} \in R^n$. *Entonces para todo* $\mathbf{r} \in \mathrm{LRes}(\mathbf{f}, G)$ *y todo* $\mathbf{r}' \in \mathrm{LRes}(\mathbf{f}, G')$, $\mathbf{r} = \mathbf{r}'$.

[3.11.2]. *Sea* $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ *una base de Gröbner para el submódulo a izquierda* K, *y sea* $\mathbf{f} \in R^n$. $\mathbf{f} \in K$ *si y sólo si* $\mathrm{lres}(\mathbf{f}, G) = 0$.

Demostración. La demostración es idéntica a [2.39] y [2.41] cambiando elementos de R por elementos de R^n donde sea necesario. □

[3.12]. Vamos a dar una versión de los S–polinomios para elementos de R^n. Sean $\mathbf{f}, \mathbf{g} \in R^n$. Supongamos que $\exp(\mathbf{f}) = (\alpha, i)$ y $\exp(\mathbf{g}) = (\beta, j)$. Sea además $\gamma = \mathrm{m}(\alpha, \beta)$. Se define el *S–vector a izquierda* de $\mathbf{f}$ y $\mathbf{g}$ como

$$S^{\ell}(\mathbf{f}, \mathbf{g}) = \begin{cases} 0 & \text{si } i \neq j \\ \frac{\mathrm{lc}(\mathbf{g})}{q_{\gamma-\alpha,\alpha}} u_{\gamma-\alpha}\mathbf{f} - \frac{\mathrm{lc}(\mathbf{f})}{q_{\gamma-\beta,\beta}} u_{\gamma-\beta}\mathbf{g} & \end{cases}$$

Las constantes han sido escogidas para que $\exp(S^{\ell}(\mathbf{f}, \mathbf{g})) \prec (\gamma, i)$

[3.13]. Teorema. *Sea* $G = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ *un sistema de generadores del* R*–submódulo* $K \subseteq R^n$ *tal que* $\mathrm{lc}(\mathbf{f}_i)$ *es una unidad para cada* i. G *es una base de Gröbner para* K *si y sólo si para cualquier pareja* $i, j \in \{1, \ldots, s\}$, $0 \in \mathrm{LRes}(S^{\ell}(\mathbf{f}_i, \mathbf{f}_j), G)$.

Demostración. Análoga a [2.58]. □

Para cada $\mathbf{g} \in R^n$, si $\exp(\mathbf{g}) = (\alpha, i)$ llamamos $\text{level}(\mathbf{g}) = i$.

[3.14]. Corolario. *Sea* $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$ *un sistema de generadores del* R*-submódulo* $K \subseteq R^n$. *Supongamos que* $\text{level}(\mathbf{g}_i) \neq \text{level}(\mathbf{g}_j)$ *para todo* $i \neq j$. *Entonces* G *es una base de Gröbner para* K.

[3.15]. Si $\Bbbk$ es un cuerpo, el teorema [3.13] nos permite dar un algoritmo para el cálculo de una base de Gröbner de idéntica manera a [2.60]. Sea $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ un sistema de generadores de un submódulo K. El algoritmo tiene los siguientes pasos

Paso 1. Llamamos $F_0 = F$, $k = 0$.

Paso 2. Para cada par $\mathbf{f}, \mathbf{g} \in F_k$ con $\text{level}(\mathbf{f}) = \text{level}(\mathbf{g})$, elegimos $\mathbf{r}_{\mathbf{f},\mathbf{g}} \in \text{LRes}(S^\ell(\mathbf{f}, \mathbf{g}), F_k)$.

Paso 3. Llamamos $R_k = \{\mathbf{r}_{\mathbf{f},\mathbf{g}} \mid \mathbf{f}, \mathbf{g} \in F_k\}$, $F_{k+1} = F_k \cup (R_k \setminus \{0\})$.

Paso 4. Si $F_k = F_{k+1}$ entonces el algoritmo termina y F_k es una base de Gröbner para K.

Paso 5. Si $F_k \neq F_{k+1}$ entonces $k = k + 1$ y volvemos al Paso 2.

En el paso 2 podemos tomar $\mathbf{r}_{\mathbf{f},\mathbf{g}} = \text{lres}(S^\ell(\mathbf{f}, \mathbf{g}), [F_h])$. Dado que $\text{level}(\mathbf{f}) \neq \text{level}(\mathbf{g})$ implica $S^\ell(\mathbf{f}, \mathbf{g}) = 0$ nos es suficiente con seleccionar elementos del mismo nivel en F_k. Que el algoritmo termina y lo hace correctamente se justifica como en [2.60].

Lema. *Si* $F_h = F_{h+1}$ *entonces* F_h *es un base de Gröbner.*

Demostración. Si $F_h = F_{h+1}$ entonces para cualesquiera $\mathbf{f}, \mathbf{g} \in F_h$, $0 \in \text{LRes}(S^\ell(\mathbf{f}, \mathbf{g}), F_h)$, y el resultado es consecuencia del teorema [3.13]. □

La cadena ascendente de subconjuntos estables

$$\text{Exp}(F_0) + \mathbb{N}^p \subseteq \text{Exp}(F_1) + \mathbb{N}^p \subseteq \cdots \subseteq \text{Exp}(F_n) + \mathbb{N}^p \subseteq \cdots,$$

debe estacionar, ya que en caso contrario encontraríamos un subconjunto estable, el conjunto $\bigcup_{i=0}^{\infty} \left(\text{Exp}(F_i) + \mathbb{N}^p\right)$, que no podría ser generado por un conjunto finito. Existe un natural $h \in \mathbb{N}$ tal que $\text{Exp}(F_h) + \mathbb{N}^p = \text{Exp}(F_{h+1}) + \mathbb{N}^p$.

Lema. *Si* $\text{Exp}(F_h) + \mathbb{N}^p = \text{Exp}(F_{h+1}) + \mathbb{N}^p$ *entonces* $F_h = F_{h+1}$.

Demostración. Supongamos que existe un elemento $\mathbf{r} \in F_{h+1} \setminus F_h$, entonces existen $\mathbf{f}, \mathbf{g} \in F_h$ tales que $\mathbf{r} \in \mathrm{LRes}(S^\ell(\mathbf{f}, \mathbf{g}), F_h)$. Como $\mathbf{r} \neq 0$ tenemos que $\mathcal{N}(\mathbf{r}) \neq \varnothing$, y como $\mathcal{N}(\mathbf{r}) \cap \mathrm{Exp}(F_h) + \mathbb{N}^p = \varnothing$ obtenemos

$$\mathrm{Exp}(F_h) + \mathbb{N}^p \subsetneq \mathrm{Exp}(F_h \cup \{\mathbf{r}\}) + \mathbb{N}^p \subseteq \mathrm{Exp}(F_{h+1}) + \mathbb{N}^p = \mathrm{Exp}(F_h) + \mathbb{N}^p,$$

lo que es imposible. Por tanto $F_h = F_{h+1}$. □

En lo que sigue supondremos que $\Bbbk$ es un cuerpo siempre que necesitemos calcular una base Gröbner para un submódulo K.

3.3 Módulo de sicigias.

Sea R un álgebra de tipo PBW sobre un cuerpo $\Bbbk$, con orden $\leq$. Utilizaremos el símbolo $\preceq$ para denotar al orden POT o al orden TOP indistintamente. Todo morfismo de R^m en otro R–módulo a izquierda viene dado por las imágenes de la base canónica $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$, luego para dar un morfismo

$$\phi : R^m \longrightarrow R^n$$

nos basta con conocer m elementos de R^n, es decir, $\phi(\mathbf{e}_i) = \mathbf{f}_i$. Si cada $\mathbf{f}_i = [f_{i1}, \ldots, f_{in}]$ podemos escribir el morfismo con notación matricial. Si $\mathbf{h} = [h_1, \ldots, h_m]$,

$$\varphi(\mathbf{h}) = [h_1, \ldots, h_m] \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = [h_1, \ldots, h_m] \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{m1} & \cdots & f_{mn} \end{bmatrix}$$

[3.16]. Definimos el módulo de sicigias de $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ como el núcleo del morfismo anterior, es decir,

$$\mathrm{Syz}(F) = \{\mathbf{h} \in R^m \mid \mathbf{h} \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = 0\}$$

Nuestro objetivo va a ser calcular un conjunto finito de generadores de $\mathrm{Syz}(F)$ para cualquier subconjunto finito $F \subseteq R^n$. Las dos herramientas fundamentales son los S–vectores y las bases de Gröbner. Los métodos son análogos a los empleados en [39], donde se hace para $n = 1$, y en [4], donde $n = 1$ y R es conmutativo. Podemos ver también, aún dentro del caso conmutativo pero para un n cualquiera, el libro de [1]. Antecedentes en el caso no conmutativo pueden verse en [14].

[3.17]. El cálculo de los generadores de $\mathrm{Syz}(F)$ lo vamos a hacer en dos etapas. Supongamos primero que $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ es una base de Gröbner para el R–submódulo de R^n que genera, es decir,

$$\mathrm{Exp}(R\mathbf{f}_1 + \cdots + R\mathbf{f}_m) = \mathrm{Exp}(F) + \mathbb{N}^p = \bigcup_{i=1}^{m} \big(\exp(\mathbf{f}_i) + \mathbb{N}^p\big).$$

Dado que $\Bbbk$ es un cuerpo no perdemos generalidad en suponer que $\mathrm{lc}(\mathbf{f}_i) = 1$. Para cada $i \in \{1, \ldots, m\}$ notaremos $\exp(\mathbf{f}_i) = \big(\alpha^i, \mathrm{level}(\mathbf{f}_i)\big)$. Si $1 \leq i < j \leq m$ son índices tales que $\mathrm{level}(\mathbf{f}_i) = \mathrm{level}(\mathbf{f}_j)$, notaremos $\gamma^{ij} = \mathrm{m}(\alpha^i, \alpha^j)$, $s_{ij} = q^{-1}_{\gamma^{ij}-\alpha^i,\alpha^i} u_{\gamma^{ij}-\alpha^i}$, $s_{ji} = q^{-1}_{\gamma^{ij}-\alpha^j,\alpha^j} u_{\gamma^{ij}-\alpha^j}$. Para dos índices $i < j$ cualesquiera tenemos entonces

$$\mathbf{p}_{ij} = S^{\ell}(\mathbf{f}_i, \mathbf{f}_j) = \begin{cases} 0 & \text{si } \mathrm{level}(\mathbf{f}_i) \neq \mathrm{level}(\mathbf{f}_j) \\ s_{ij}\mathbf{f}_i - s_{ji}\mathbf{f}_j & \text{si } \mathrm{level}(\mathbf{f}_i) = \mathrm{level}(\mathbf{f}_j), \end{cases} \tag{3.2}$$

por lo que en el caso $\mathrm{level}(\mathbf{f}_i) \neq \mathrm{level}(\mathbf{f}_j)$ pondremos $s_{ij} = s_{ji} = 0$ para escribir, en cualquier caso,

$$\mathbf{p}_{ij} = s_{ij}\mathbf{f}_i - s_{ji}\mathbf{f}_j.$$

Por el teorema [3.13], $\mathrm{lres}(\mathbf{p}_{ij}, F) = 0$, por lo que

$$\mathbf{p}_{ij} = \sum_{k=1}^{m} q_{ijk}\mathbf{f}_k \tag{3.3}$$

$$q_{ijk} \in R, \text{ para todo } 1 \leq k \leq m$$

$$\exp(q_{ijk}\mathbf{f}_k) \preceq \exp(\mathbf{p}_{ij}), \text{ para todo } 1 \leq k \leq m.$$

Sea $\mathbf{r}_{ij} = [q_{ij1}, \ldots, q_{iji} - s_{ij}, \ldots, q_{ijj} + s_{ji}, \ldots, q_{ijm}]$.

[3.18]. Proposición. *El conjunto* $B_F = \{\mathbf{r}_{ij} \mid 1 \leq i < j \leq m\}$ *es un sistema de generadores de* $\mathrm{Syz}(F)$.

Demostración. Juntando (3.2) y (3.3) tenemos que

$$\sum_{k=1}^{m} r_{ijk}\mathbf{f}_k = 0,$$

luego $\mathbf{r}_{ij} \in \mathrm{Syz}(F)$. Sea entonces RB_F el R–submódulo de $\mathrm{Syz}(F)$ generado por B_F. Supongamos que $M = \mathrm{Syz}(F) \setminus RB_F$ es no vacío. Podemos elegir un elemento $[h_1, \ldots, h_m] \in M$ tal que

(i) $\mathrm{t} = \max\{\exp(h_k\mathbf{f}_k) \mid 1 \leq k \leq m\}$ es un elemento minimal en el conjunto

$$\big\{ \max\{\exp(h_k\mathbf{f}_k) \mid 1 \leq k \leq m\} \mid [g_1, \ldots, g_m] \in M \big\} \subseteq \mathbb{N}^{p,n},$$

(ii) El cardinal del conjunto $\Lambda = \{k \mid \exp(h_k\mathbf{f}_k) = \mathrm{t}\}$ es también minimal.

Dado que $[h_1, \ldots, h_m] \in \mathrm{Syz}(F)$, $\sum_{k=1}^{m} h_k\mathbf{f}_k = 0$. El cardinal de Λ debe ser mayor que uno, ya que si Λ tiene un único elemento entonces $\mathrm{t} = \exp(0)$, lo que es imposible. Existen entonces $i < j \in \Lambda$. Tenemos entonces

$$\mathrm{t} = \exp(h_i) + \exp(\mathbf{f}_i) = \exp(h_j) + \exp(\mathbf{f}_j).$$

Para que la igualdad anmterior se produzca es necesario que $\mathrm{level}(\mathbf{f}_i) = \mathrm{level}(\mathbf{f}_j)$. Es fácil ver que $\mathrm{t} = \mu + \big(\gamma^{ij}, \mathrm{level}(\mathbf{f}_i)\big)$. Por otra parte $\exp(q_{ijk}\mathbf{f}_k) \preceq \exp(\mathbf{p}_{ij}) \prec (\gamma^{ij}, \mathrm{level}(\mathbf{f}_i))$. Esto implica que

$$\exp(u_\mu r_{iji}\mathbf{f}_i) = \mu + \exp(r_{iji}\mathbf{f}_i) = \mu + (\gamma^{ij}, \mathrm{level}(\mathbf{f}_i)) = \mathrm{t}.$$

Sea $a_i = \mathrm{lc}(h_i\mathbf{f}_i)q^{-1}_{\mu,\gamma^{ij}}$. Tenemos entonces

$$\begin{aligned}
\mathrm{lc}(a_i u_\mu r_{iji}\mathbf{f}_i) &= \mathrm{lc}(a_i u_\mu (q_{iji} - s_{ij})\mathbf{f}_i) \\
&= a_i q_{\mu,\gamma^{ij}} \,\mathrm{lc}((q_{iji} - s_{ij})\mathbf{f}_i) \\
&= a_i q_{\mu,\gamma^{ij}} (-1) \\
&= -\mathrm{lc}(h_i\mathbf{f}_i),
\end{aligned}$$

por lo que

$$\exp\big((h_i + a_i u_\mu r_{iji})\mathbf{f}_i\big) \prec \exp(h_i\mathbf{f}_i).$$

Llamemos $g_k = h_k + a_i u_\mu r_{ijk}$. Hemos compobado que $\exp(g_i\mathbf{f}_i) \prec \exp(h_i\mathbf{f}_i)$. Además,

$$\exp(a_i u_\mu r_{ijj}\mathbf{f}_j) = \mu + \exp(q_{ijj}\mathbf{f}_j + s_{ji}\mathbf{f}_j) = \mu + \big(\gamma^{ij}, \mathrm{level}(\mathbf{f}_j)\big) = \mathrm{t},$$

lo que implica que $\exp(g_j\mathbf{f}_j) \preceq \mathrm{t}$. Si $k \neq i, j$ entonces

$$\exp(a_i u_\mu r_{ijk}\mathbf{f}_k) = \mu + \exp(r_{ijk}\mathbf{f}_k) \prec \mu + \big(\gamma^{ij}, \mathrm{level}(\mathbf{f}_i)\big) = \mathrm{t}.$$

Consecuentemente $\exp(g_k\mathbf{f}_k) \preceq \mathrm{t}$, siendo la desigualdad estricta siempre que $\exp(h_k\mathbf{f}_k) \prec \mathrm{t}$. Hemos encontrado un elemento $[g_1, \ldots, g_m]$ en el que o $\max\{\exp(g_k\mathbf{f}_k) \mid 1 \leq k \leq m\} \prec \mathrm{t}$ o el cardinal del conjunto $\{k \mid \exp(g_k\mathbf{f}_k) = \mathrm{t}\}$ es menor que el cardinal de Λ. Dado que

$$[g_1, \ldots, g_m] = [h_1, \ldots, h_m] + a_i u_\mu \mathbf{r}_{ij} \tag{3.4}$$

tenemos que $[g_1, \ldots, g_m] \in \mathrm{Syz}(F)$. Por la minimalidad de $[h_1, \ldots, h_m]$, $[g_1, \ldots, g_m] \in RB_F$, y de nuevo (3.4) implica que $[h_1, \ldots, h_m] \in RB_F$ lo que es imposible. □

Una vez establecido el cálculo del sistema de generadores para bases de Gröbner vamos a resolver el caso general. Sea F un sistema de generadores $K \subseteq R^n$. Sea G una base de Gröbner para K obtenida a partir de F usando [3.15]. Supongamos $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ y $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$. Existen matrices $C = [c_{ij}]_{t\times m}$ y $D = [d_{ji}]_{m\times t}$ tales que

$$\begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} = C \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = D \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix}.$$

[3.19]. La matriz D es fácilmente calculable, ya que sus entradas son los cocientes de la división de cada $\mathbf{f}_j$ entre G:

$$\mathbf{f}_j = \sum_{i=1}^{t} d_{ji}\mathbf{g}_i.$$

[3.20]. También es posible calcular la matriz C. Supongamos que $H = \{\mathbf{h}_1, \ldots, \mathbf{h}_s\} \subseteq K$ y $\mathbf{f}, \mathbf{g} \in K$. Supongamos además que conocemos elementos $e_{kj}, a_j, b_j \in R$ tales que

$$\mathbf{h}_k = \sum_{j=1}^{m} e_{kj}\mathbf{f}_j, \quad \mathbf{f} = \sum_{j=1}^{m} a_j\mathbf{f}_j, \quad \mathbf{g} = \sum_{j=1}^{m} b_j\mathbf{f}_j.$$

Si $\mathbf{r} \in \mathrm{LRes}(S^\ell(\mathbf{f}, \mathbf{g}), H)$,

$$\begin{aligned} \mathbf{r} &= S^\ell(\mathbf{f}, \mathbf{g}) - l_1\mathbf{h}_1 - \cdots - l_s\mathbf{h}_s \\ &= p\mathbf{f} - p'\mathbf{g} - \sum_{k=1}^{s} l_k\mathbf{h}_k \\ &= p\sum_{j=1}^{m} a_j\mathbf{f}_j - p'\sum_{j=1}^{m} b_j\mathbf{f}_j - \sum_{k=1}^{s} l_k\sum_{j=1}^{m} e_{kj}\mathbf{f}_j, \end{aligned}$$

donde todos los coeficientes de los $\mathbf{f}_i$ son conocidos. Esto nos permite ir calculando los elementos c_{ij} cada vez que pasamos por el Paso 2 en [3.15].

[3.21]. Las transformaciones anteriores pueden ser compuestas, y obtenemos que

$$\begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} = CD \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = DC \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix}.$$

Consideremos la matriz identidad $m \times m$ I_m. Tenemos la siguiente identidad:

$$\begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = DC \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = I_m \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix}, \tag{3.5}$$

por lo que llamando $A = I_m - DC = [a_{ij}]_{m\times m}$ obtenemos que las filas de A son elementos de $\mathrm{Syz}(F)$, es decir, para todo $j = 1, \ldots, m$, $\mathbf{a}_j = [a_{j1}, \ldots, a_{jm}] \in \mathrm{Syz}(F)$, donde

$$a_{jl} = \delta_{jl} - \sum_{i=1}^{m} d_{ji} c_{il}.$$

[3.22]. Sea $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$ un sistema de generadores de $\mathrm{Syz}(G) \subseteq R^t$ que puede ser calculado mediante [3.18], esto es,

$$\mathbf{b}_i \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} = 0$$

Definimos $B^* = \{\mathbf{b}_1^*, \ldots, \mathbf{b}_r^*\}$ mediante

$$\mathbf{b}_i^* = \mathbf{b}_i C \in R^m.$$

Vamos a demostrar que $B^* \subseteq \mathrm{Syz}(F)$. Para ello,

$$\mathbf{b}_i^* \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = \mathbf{b}_i C \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = \mathbf{b}_i \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} = 0,$$

como deseábamos

[3.23]. Teorema. *El conjunto* $\{\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1^*, \ldots, \mathbf{b}_r^*\}$ *constituye un sistema de generadores de* $\mathrm{Syz}(F)$.

Demostración. Sea $\mathbf{h} = [h_1, \ldots, h_m] \in \mathrm{Syz}(F)$ un elemento cualquiera y definamos

$$\mathbf{h}_* = \mathbf{h}D.$$

Tenemos entonces que

$$\mathbf{h}_* \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} = \mathbf{h}D \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_t \end{bmatrix} = \mathbf{h} \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix} = 0,$$

luego $\mathbf{h}_* \in \mathrm{Syz}(G)$. Como B es un sistema de generadores para $\mathrm{Syz}(G)$, tenemos que

$$\mathbf{h}_* = \sum_{l=1}^{r} p_l \mathbf{b}_l.$$

Definimos $\mathbf{k} = \mathbf{h}_* C$. Entonces $\mathbf{k} = \sum_{l=1}^{r} p_l \mathbf{b}_l C = \sum_{l=1}^{r} p_l \mathbf{b}_l^* \in RB^*$. Además,

$$\mathbf{h} - \mathbf{k} = \mathbf{h} - \mathbf{h}_* C = \mathbf{h} - \mathbf{h}DC = \mathbf{h}A = \sum_{j=1}^{m} h_i \mathbf{a}_i.$$

Podemos concluir que $\mathbf{h} = \mathbf{k} + (\mathbf{h} - \mathbf{k})$ está en el submódulo generado por $\{\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1^*, \ldots, \mathbf{b}_r^*\}$. □

[3.24]. Podemos realizar el cálculo anterior pero con módulos a derecha. Dados $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\} \subseteq R^s$, se define el módulo de sicigias a derecha de R como

$$\mathrm{Syz}^r(F) = \{\mathbf{h} \in R^m \mid [\mathbf{f}_1, \ldots, \mathbf{f}_m]\mathbf{h}^T = 0\},$$

donde ^{T} representa el vector traspuesto, es decir, visto como vector columna. El procedimiento para calcular un sistema de generadores B_F de $\mathrm{Syz}^r(F)$ es totalmente simétrico al anterior para sicigias a izquierda. Comenzamos calculando una base de Gröbner de $\mathbf{f}_1 R + \cdots + \mathbf{f}_m R$ mediante el análogo a derecha de [3.15]. Sea $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ dicha base. Calculamos matrices C y D tales que

$$[\mathbf{g}_1, \ldots, \mathbf{g}_t] = [\mathbf{f}_1, \ldots, \mathbf{f}_m]C$$
$$[\mathbf{f}_1, \ldots, \mathbf{f}_m] = [\mathbf{g}_1, \ldots, \mathbf{g}_t]D.$$

Por lo tanto

$$[\mathbf{f}_1, \ldots, \mathbf{f}_m] = [\mathbf{f}_1, \ldots, \mathbf{f}_m]I_m = [\mathbf{f}_1, \ldots, \mathbf{f}_m]CD,$$

Por lo que las columnas de $I_m - CD$ son elementos de $\mathrm{Syz}^r(F)$. Llamemos $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\} \subseteq R^m$ al conjunto cuyos elementos satisfacen

$$[\mathbf{a}_1^T, \ldots, \mathbf{a}_m^T] = I_m - CD.$$

Un conjunto de generadores B_G de $\mathrm{Syz}^r(G)$ se obtiene de la siguiente manera: para cada pareja $i < j$,

$$S^r(\mathbf{g}_i, \mathbf{g}_j) = \mathbf{g}_i s_{ij} - \mathbf{g}_j s_{ji}$$

para ciertos $s_{ij}, s_{ji} \in R$. Por otra parte,

$$S^r(\mathbf{g}_i, \mathbf{g}_j) = \sum_{k=1}^{t} \mathbf{g}_k q_{ijk},$$

donde $q_{ijk} \in R$, división a derecha fuerte. Los elementos $\mathbf{b}_{ij} = [q_{ij1}, \ldots, q_{iji} - s_{ij}, \ldots, q_{ijj} + s_{ji}, \ldots, q_{ijm}]$ generan a $\mathrm{Syz}^R(G)$. Sea $\{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$ un sistema de generadores de $\mathrm{Syz}^r(G)$. Es fácil comprobar que

$$[\mathbf{f}_1, \ldots, \mathbf{f}_m] C \mathbf{b}_i^T = 0,$$

por lo que los elementos $\mathbf{b}_i^* = (C\mathbf{b}_i^T)^T$ pertenecen a $\mathrm{Syz}^r(F)$. Llamemos $B = \{\mathbf{b}_1^*, \ldots, \mathbf{b}_r^*$. El resultado análogo a [3.23] establece que $\mathrm{Syz}^r(F)$ está generado por $A \cup B$.

3.4 Aplicaciones del módulo de sicigias.

3.4.1 Presentación de módulos.

[3.25]. Sea M un R–módulo finitamente generado y supongamos que el conjunto $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ es un conjunto de generadores de M. Entonces el homomorfismo de R–módulos

$$\begin{aligned} \phi : R^n &\longrightarrow M \\ \mathbf{e}_i &\longmapsto \mathbf{a}_i \end{aligned}$$

es sobreyectivo, lo que implica que $M \cong R^n / \ker(\phi)$. Hemos demostrado

Lema. *Todo R–módulo finitamente generado tiene asociados un natural $n \in \mathbb{N}$ y un subconjunto finito $\{\mathbf{f}_1, \ldots, \mathbf{f}_m\} \subseteq R^n$ tales que*

$$M \cong \frac{R^n}{R\mathbf{f}_1 + \cdots + R\mathbf{f}_m}$$

Podemos por tanto limitarnos a estudiar submódulos y cocientes de módulos libres.

[3.26]. Lema. *El conjunto $B = \{\mathbf{u}_\alpha + K \mid \alpha \in \mathbb{N}^{p,n} \setminus \mathrm{Exp}(K)\}$ es una $\Bbbk$–base para R^n/K.*

Demostración. Sea G una base de Gröbner para K. Si $\mathbf{f} + K \in R^n/K$ entonces $\mathbf{f} + K = \mathrm{lres}(\mathbf{f}, G) + K$ con $\mathcal{N}(\mathrm{lres}(\mathbf{f}, G)) \subseteq \mathbb{N}^{p,n} \setminus \mathrm{Exp}(K)$, por lo que B es un sistema de generadores.

Si $\mathbf{r} = \sum_{\alpha \notin \mathrm{Exp}(K)} c_\alpha u_\alpha \in K$ entonces $\exp(\mathbf{r}) \in \mathrm{Exp}(K)$, pero $\mathcal{N}(\mathbf{r}) \cap \mathrm{Exp}(K) = \varnothing$, lo que implica que $\mathbf{r} = 0$. Esto prueba la independencia lineal. □

Todo submódulo de R^n es finitamente generado, luego tiene una presentación finita:

[3.27]. Teorema. *Sean $N \subseteq M \subseteq R^n$ R–submódulos. Supongamos que N viene generado por $\{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ y M por $\{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$. Llamemos H al conjunto $\{\mathbf{f}_1, \ldots, \mathbf{f}_s, \mathbf{g}_1, \ldots, \mathbf{g}_t\}$ y sea $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\} \subseteq R^{s+t}$ un conjunto de generadores de* $\mathrm{Syz}(H)$. *Notemos para cada $i = 1, \ldots, r$ $\mathbf{h}_i \in R^s$ las s primeras coordenadas de $\mathbf{p}_i$. Entonces*

$$M/N \cong R^s/K \quad \textit{donde } K = R\mathbf{h}_1 + \cdots + R\mathbf{h}_r$$

Demostración. Definamos el morfismo de R–módulos

$$\begin{aligned} \phi : R^s &\longrightarrow M/N \\ \mathbf{e}_i &\longmapsto \mathbf{f}_i + N \end{aligned}$$

para $1 \leq i \leq s$. Es claro que ϕ es sobreyectivo. Sea $K = \ker(\phi)$. Observemos que $\mathbf{h} = [h_1, \ldots, h_s] \in K$ si y sólo si $h_1\mathbf{f}_1 + \cdots + h_s\mathbf{f}_s \in N$, es decir, existen $a_1, \ldots, a_t \in R$ tales que

$$h_1\mathbf{f}_1 + \cdots + h_s\mathbf{f}_s = a_1\mathbf{g}_1 + \cdots + a_t\mathbf{g}_t,$$

luego $[h_1, \ldots, h_s, -a_1, \ldots, -a_t] \in \mathrm{Syz}(H)$. Como todos los elementos de $\mathrm{Syz}(H)$ son combinación R–lineal de $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\}$, los elementos de K deben ser combinación R–lineal de las primeras s coordenadas de cada $\mathbf{p}_i$. □

[3.28]. Corolario. *Sea $L \subseteq R^n$ un R–submódulo. Supongamos que L viene generado por $\{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$, y sean $\mathbf{f}_1, \ldots, \mathbf{f}_s$ elementos de R^n. Sea $H = \{\mathbf{f}_1, \ldots, \mathbf{f}_s, \mathbf{g}_1, \ldots, \mathbf{g}_t\}$ y sea $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\} \subseteq R^{s+t}$ un conjunto de generadores de* $\mathrm{Syz}(H)$. *Notemos para cada $i = 1, \ldots, r$ $\mathbf{h}_i \in R^s$ las s primeras coordenadas de $\mathbf{p}_i$. Entonces $K = R\mathbf{h}_1 + \cdots + R\mathbf{h}_r$ es el núcleo del morfismo*

$$\begin{aligned} f : R^s &\longrightarrow R^n/L \\ \mathbf{e}_i &\longmapsto \mathbf{f}_i + L \end{aligned}$$

Demostración. Basta aplicar el teorema [3.27] a $M = R\mathbf{f}_1 + \cdots + R\mathbf{f}_s$ y $N = L$. □

Las versiones a derecha de [3.27] y [3.28] son simétricas, cambiando Syz por Syz^r.

3.4.2 Intersección de submódulos.

Sea $M \cong R^n/K$ un R–módulo finitamente generado y sean M_1, M_2 submódulos de M. Existen $K \subseteq K_1, K_2 \subseteq R^n$ tales que $M_i = K_i/K$ para $i = 1, 2$. Además $M_1 \cap M_2 = (K_1 \cap K_2)/K$. Es suficiente con estudiar el cálculo de intersecciones de R–submódulos de R^n.

[3.29]. Antes de estudiar la intersección vamos a introducir alguna notación. Dado un conjunto $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\} \subseteq R^n$, un elemento $\mathbf{h} \in \mathrm{Syz}(F)$ satisface $\mathbf{hF} = 0$, donde $\mathbf{F}$ es la matriz

$$\mathbf{F} = \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_m \end{bmatrix}_{m \times n}$$

Si A es una matriz $m \times n$, entenderemos que $\mathrm{Syz}(A)$ es el módulo de sicigias del conjunto formado por las filas de A. Bajo esta óptica $\mathrm{Syz}(F) = \mathrm{Syz}(\mathbf{F})$, por lo que abusaremos de lenguaje y llamaremos F al conjunto y a la matriz.

[3.30]. Sean M y N submódulos de R^n y supongamos que vienen generados por los conjuntos $\{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ y $\{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ respectivamente. Sea H la matriz $(n+s+t) \times (n+n)$

$$H = \left[\begin{array}{c|c} I_n & I_n \\ \hline \mathbf{f}_1 & \\ \vdots & 0 \\ \mathbf{f}_s & \\ \hline & \mathbf{g}_1 \\ 0 & \vdots \\ & \mathbf{g}_t \end{array}\right]$$

Proposición. *Sea $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\}$ es un conjunto de generadores de $\mathrm{Syz}(H)$ y para cada $1 \leq i \leq r$ notemos por $\mathbf{h}_i$ las n primeras coordenadas de $\mathbf{p}_i$, entonces $\{\mathbf{h}_1, \ldots, \mathbf{h}_r\}$ es un sistema de generadores para $M \cap N$*

Demostración. $\mathbf{h} \in M$ si y sólo si existen $a_1, \ldots, a_s \in R$ tales que $\mathbf{h} = a_1\mathbf{f}_1 + \cdots + a_s\mathbf{f}_s$. Análogamente, $\mathbf{h} \in N$ si y sólo si existen $b_1, \ldots, b_t \in R$ tales que $\mathbf{h} = b_1\mathbf{g}_1 + \cdots + b_t\mathbf{g}_t$. Hemos demostrado pues que $\mathbf{h} \in M \cap N$ si

y sólo si existen elementos $a_1, \ldots, a_s, b_1, \ldots, b_t \in R$ tales que

$$[h_1, \ldots, h_n, a_1, \ldots, a_s, b_1, \ldots, b_t] \left[\begin{array}{c|c} I_n & I_n \\ \hline \mathbf{f}_1 & \\ \vdots & 0 \\ \mathbf{f}_s & \\ \hline & \mathbf{g}_1 \\ 0 & \vdots \\ & \mathbf{g}_t \end{array}\right] = 0,$$

es decir, $[h_1, \ldots, h_n, a_1, \ldots, a_s, b_1, \ldots, b_t] \in \mathrm{Syz}(H)$. Como $\mathrm{Syz}(H)$ está generado por $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\}$, las primeras n coordenadas de cualquier elemento de $\mathrm{Syz}(H)$ están generadas por las primeras n coordenadas de los elementos $\mathbf{p}_i$, lo que demuestra la proposición. □

3.4.3 Cálculo de $\mathrm{Hom}(M, R/I)$ y $\mathrm{Ext}^n(M, R/I)$.

En [1, Section 3.9] se proporciona un método de cálculo de $\mathrm{Hom}_A(M, N)$ cuando A es un anillo de polinomios conmutativo sobre un cuerpo $\Bbbk$. Igualmente se calculan resoluciones libres y consecuentemente $\mathrm{Ext}^n_A(M, N)$. Lamentablemente, para el caso no conmutativo nos encontramos con que siendo M y N dos R–módulos a izquierda cualesquiera, $\mathrm{Hom}(M, N)$ es un grupo abeliano y no un R–módulo. Podemos plantearnos dar una presentación de $\mathrm{Hom}(M, N)$ en el caso en que M o N sea un R–R–bimódulo, ya que $\mathrm{Hom}(M, N)$ adquiere de manera natural estructura de R–módulo a izquierda o derecha (ver [72, Theorem 1.15]). Vamos a dar una presentación de $\mathrm{Hom}(M, R/I)$ cuando I sea un ideal bilátero, por lo que R/I es un R–bimódulo. Recordemos que la estructura de R–módulo a derecha de $\mathrm{Hom}(M, R/I)$ viene dada por $(fr)(x) = f(x) \cdot r$. Las mismas ideal se pueden aplicar cuando el bimódulo aparezca a la izquierda del funtor. Debemos observar que en [25, Section 3] se comete el error de afirmar que $\mathrm{Hom}(M, N)$ tiene estructura natural de R–módulo cuando N es finitamente generado cuando R es el álgebra de Weyl.

[3.31]. Podemos suponer que $M \cong R^s/L$, donde L es el R–submódulo de R^s generado por $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$, es decir, la sucesión

$$0 \to L \to R^s \to M \to 0$$

es exacta.

Lema. *La sucesión*

$$R^n \xrightarrow{\Gamma} R^s \longrightarrow M \longrightarrow 0 \tag{3.6}$$

donde $\Gamma(\mathbf{h}) = \mathbf{h}\begin{bmatrix}\mathbf{f}_1\\ \vdots \\ \mathbf{f}_m\end{bmatrix}$, *es exacta.*

Demostración. Inmediato, ya que $\mathrm{im}(\Gamma) = L$. □

[3.32]. Es bien sabido que existe un isomorfismo de R–módulos a derecha entre las matrices $\mathcal{M}_{m\times n}(R)$ y $\mathrm{Hom}(R^m, R^n)$ (morfismos a izquierda). De hecho, dado $\phi \in \mathrm{Hom}(R^m, R^n)$, definimos la matriz

$$\Delta_\phi = \begin{bmatrix}\phi(\mathbf{e}_1)\\ \vdots \\ \phi(\mathbf{e}_m)\end{bmatrix}.$$

Es fácil comprobar que $\phi([x_1, \ldots, x_m]) = [x_1, \ldots, x_m]\Delta_\phi$. Análogamente, dada la matriz Δ podemos definir $\phi_\Delta([x_1, \ldots, x_m]) = [x_1, \ldots, x_m]\Delta$. Es mecánico comprobar que estas asignaciones definen isomorfismos inversos de R–módulos a derecha.

Utilizaremos la misma letra Γ para notar la matriz $\Gamma = \begin{bmatrix}\mathbf{f}_1\\ \vdots \\ \mathbf{f}_m\end{bmatrix}$ y el morfismo Γ.

[3.33]. Vamos a aplicar el funtor $\mathrm{Hom}(-, R/I)$ a la sucesión (3.6). La exactitud a izquierda de $\mathrm{Hom}(-, R/I)$ aplicada a (3.6), proporciona la siguiente sucesión exacta de R–módulos a derecha:

$$0 \to \mathrm{Hom}(M, R/I) \to \mathrm{Hom}(R^s, R/I) \xrightarrow{\Gamma_*} \mathrm{Hom}(R^n, R/I) \tag{3.7}$$

donde $\Gamma_*(f) = \varphi \circ \Gamma$, i.e., $\Gamma_*(f)(\mathbf{x}) = f(\mathbf{x}\Gamma)$.. Por tanto

$$\mathrm{Hom}(M, R/I) \cong \ker(\Gamma_*) \tag{3.8}$$

Para poder aplicar [3.28] necesitamos dar una presentación de $\mathrm{Hom}(R^s, R/I)$ y describir el morfismo Γ_* a partir de dicha presentación.

[3.34]. Lema. *Sea* $\{g_1, \ldots, g_r\}$ *un conjunto de generadores del ideal bilátero* I *como ideal a derecha. Sea* $I^s \subseteq R^s$ *el* R*–submódulo a derecha generado por los elementos* $\mathbf{g}_{ij} = [0, \ldots, \overset{i}{g_j}, \ldots, 0]$. *Entonces*

$$\mathrm{Hom}(R^s, R/I) \cong R^s/I^s$$

Demostración. Consideremos el siguiente morfismo de R–módulos a derecha:

$$\varphi : R^s \longrightarrow \mathrm{Hom}(R^s, R/I)$$
$$\mathbf{a} = [a_1, \ldots, a_s] \longmapsto \varphi(\mathbf{a}) : R^s \to R/I; [x_1, \ldots, x_s] \mapsto (x_1a_1 + \cdots + x_sa_s) + I$$

Vamos a ver que φ es sobreyectiva y a calcular su núcleo. En primer lugar, si $f : R^s \to R/I$ es un morfismo de R–módulos a derecha, existe $\mathbf{b} = [b_1, \ldots, b_s]$ tal que $f(\mathbf{e}_i) = b_i + I$. Es sencillo comprobar que $f = \varphi(\mathbf{b})$. Nos queda por tanto comprobar que el núcleo es I^s. Si $\mathbf{a} \in I^s$, entonces $\mathbf{a} = \sum_{ij} \mathbf{g}_{ij}c_{ij}$ para ciertos $c_{ij} \in R$. La construcción de los elementos $\mathbf{g}_{ij}$ nos proporciona que para $k = 1, \ldots, s$, $a_k = \sum_j g_jc_{kj} \in I$. Como I es bilátero, $\varphi(\mathbf{a})([x_1, \ldots, x_s]) = 0 + I$. Hemos demostrado que $I^s \subseteq \ker(\varphi)$. Recíprocamente, si $[a_1, \ldots, a_s] \in \ker(\varphi)$, entonces $a_k \in I$ para todo $k = 1, \ldots, s$. Entonces $a_k = \sum_j g_jc_{kj}$, de donde $\mathbf{a} = \sum_{ij} \mathbf{g}_{ij}c_{ij} \in I^s$. □

[3.35]. Observación. Una base de Gröbner para I es un conjunto de generadores como el requerido en [3.34].

[3.36]. Lema. *Sea $\gamma : R^s/I^s \to R^n/I^n$ el morfismo inducido por Γ_* en 3.7 vía el isomorfismo de [3.34]. Entonces,*

$$\gamma(\mathbf{a} + I^s) = (\Gamma\mathbf{a}^T)^T + I^n.$$

Demostración. Sea $\mathbf{a}+I^s \in R^s/I^s$. Le asociamos su morfismo correspondiente $\varphi(\mathbf{a}) : R^s \to R/I$ definido por $\varphi(\mathbf{a})(\mathbf{x}) = \mathbf{x}\mathbf{a}^T + I$. Ahora, $\Gamma_*(\varphi(\mathbf{a}))(\mathbf{y}) = \varphi(\mathbf{a}) \circ \Gamma(\mathbf{y}) = \varphi(\mathbf{a})(\mathbf{y}\Gamma) = \mathbf{y}\Gamma\mathbf{a}^T + I$, y tenemos que $\Gamma_*(\varphi(\mathbf{a}))$ está asociado con el elemento $(\Gamma\mathbf{a}^T)^T + I^n \in R^n/I^n$. □

[3.37]. Observación. Si $f : R^s/L_1 \to R^n/L_2$ es un morfismo de R–módulos a izquierda, entonces $\ker(f) = \ker(f \circ \pi)/L_1$, donde π es la proyección canónica de R^s a R^s/L_1.

[3.38]. Proposición. *Podemos dar una presentación de* $\mathrm{Hom}(M, R/I)$ *como R–módulo a derecha.*

Demostración. Por 3.7, [3.34] y [3.36], tenemos que

$$\mathrm{Hom}(M, R/I) \cong \ker(\gamma).$$

Por otra parte, si $\gamma' : R^s \to R^n/I^n$ se define mediante $\gamma'(\mathbf{e}_i) = \mathbf{f}'_i + I^n$ donde $\mathbf{f}'_i = (\Gamma\mathbf{e}_i^T)^T$, es decir, la i–ésima columna de Γ escrita como fila, entonces $\gamma' = \gamma \circ \pi$, siendo π la proyección canónica de R^s en R^s/I^s; gracias a [3.37] podemos aplicar [3.28] a los generadores de I^n y los elementos $\mathbf{f}'_1, \ldots, \mathbf{f}'_s$. □

[3.39]. Para acabar las cuestiones concernientes al cálculo de $\mathrm{Hom}(M, R/I)$ vamos a describir el procedimiento de cálculo. Los datos de entrada son una presentación de M, i.e., un natural s y un conjunto de elementos $\mathbf{f}_1, \ldots, \mathbf{f}_n \in R^s$ tales que $M \cong R^s/(R\mathbf{f}_1 + \cdots + R\mathbf{f}_n)$, y un conjunto de generadores de I como ideal a derecha, $\{g_1, \ldots, g_t\}$, que podemos suponer una base de Gröbner para I.

Paso 1. Ponemos para $1 \leq i \leq s$, $1 \leq j \leq t$, $\mathbf{g^s}_{ij} = [0, \ldots, \overset{i}{g_j}, \ldots, 0]$ y para $1 \leq i \leq n$, $1 \leq j \leq t$, $\mathbf{g^n}_{ij} = [0, \ldots, \overset{i}{g_j}, \ldots, 0]$.

Paso 2. Para cada $i = 1, \ldots, s$, llamamos $\mathbf{f'}_i = ([\mathbf{f}_1, \ldots, \mathbf{f}_n]\mathbf{e}_i^T)^T$. Llamamos además $H = \{\mathbf{f'}_1, \ldots, \mathbf{f'}_s, \mathbf{g^n}_{11}, \ldots, \mathbf{g^n}_{nt}\}$.

Paso 3. Sea $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\}$ un sistema de generadores de $\mathrm{Syz}^r(H)$, sicigias a derecha, y para cada $i = 1, \ldots, r$, $\mathbf{h}_i$ las primeras s coordenadas de $\mathbf{p}_i$. Por [3.28], [3.37] y [3.38] $\sum_{i=1}^r \mathbf{h}_i R / \sum_{ij} \mathbf{g^s}_{ij} \cong \mathrm{Hom}(M, R/I)$.

Paso 4. Aplicamos [3.27]. Sea $H' = \{\mathbf{h}_1, \ldots, \mathbf{h}_r, \mathbf{g^s}_{11}, \ldots, \mathbf{g^s}_{st}\}$. Calculamos un sistema de generadores de $\mathrm{Syz}^r(H')$ sicigias a derecha, pongamos $\{\mathbf{p'}_1, \ldots, \mathbf{p'}_u\}$. Si llamamos $\mathbf{h'}_1, \ldots, \mathbf{h'}_u$ a las primeras r coordenadas de cada $\mathbf{p'}_i$, tenemos que $\mathrm{Hom}(M, R/I) \cong R^r/(\mathbf{h'}_1 R + \cdots + \mathbf{h'}_u R)$.

[3.40]. Ejemplo. Sea R el álgebra envolvente del álgebra de Lie de dimensión 3 con generadores x, y, z y corchete $[y, x] = 0$, $[z, x] = 0$ y $[z, y] = x$, es decir, R tiene las relaciones

$$yx = xy, \quad zx = xz \quad \text{y} \quad zy = yz + x.$$

Una $\Bbbk$–base para R es $\{x^i y^j z^k \mid (i, j, k) \in \mathbb{N}^3\}$. Consederamos el orden lexicográfico graduado con $\epsilon_1 < \epsilon_2 < \epsilon_3$. Usaremos el orden TOP en cada R–módulo libre R^n. Dado que x es central, el elemento $x-1$ está en el centro de R, por lo que el ideal $R(x-1)$ es bilátero. Llamemos $I = R(x-1) = (x-1)R$. Por otra parte, sean $\mathbf{f}_1 = [y-1, x^2, y-1]$ y $\mathbf{f}_2 = [0, z-1, z-1]$ elementos en R^3. Sea además $M = \frac{R^3}{R\mathbf{f}_1 + R\mathbf{f}_2}$. Nuestro propósito es calcular una presentación de $\mathrm{Hom}(M, R/I)$. Aplicamos el algoritmo en [3.39]. Comenzamos con los elementos $\mathbf{g^s}_{ij}$, $\mathbf{g^n}_{ij}$ y $\mathbf{f}'_i$:

$$\mathbf{g^3}_{11} = [x-1, 0, 0] \qquad \mathbf{g^3}_{21} = [0, x-1, 0] \qquad \mathbf{g^3}_{31} = [0, 0, x-1]$$
$$\mathbf{g^2}_{11} = [x-1, 0] \qquad \mathbf{g^2}_{21} = [0, x-1]$$
$$\mathbf{f}'_1 = [y-1, 0] \qquad \mathbf{f}'_2 = [x^2, z-1] \qquad \mathbf{f}'_3 = [y-1, z-1].$$

Sea $H = \{\mathbf{f}'_1, \mathbf{f}'_2, \mathbf{f}'_3, \mathbf{g^2}_{11}, \mathbf{g^2}_{21}\}$. Para calcular $\mathrm{Syz}^r(H)$, el siguiente paso de nuestro algoritmo, vamos a aplicar [3.24]. Para ello debemos comenzar calculando una base de Gröbner para el módulo a derecha generado por H.

Escribimos una lista de los S–vectores subrayando los restos cuando sean no nulos:

$$
\begin{aligned}
&S([y-1,0],[x^2,z-1]) = \\
&= [y-1,0]x^2 + [x^2,z-1](-y) \\
&= [y-1,z-1](-y+1) + [y-1,0](y-1) + [x^2,z-1](-1) \\
&S([y-1,0],[y-1,z-1]) = \\
&= 0 \\
&S([y-1,0],[x-1,0]) = \\
&= [y-1,0]x + [x-1,0]y \\
&= [y-1,0] + [x-1,0](-1) \\
&S([y-1,0],[0.x-1]) = \\
&= 0 \\
&S([x^2,z-1],[y-1,z-1]) = \\
&= 0 \\
&S([x^2,z-1],[x-1,0]) = \\
&= [x^2,z-1] + [x-1,0](-x) \\
&= [y-1,z-1] + [y-1,0] + [x-1,0] + \underline{[1,0]}
\end{aligned}
$$

$$
\begin{aligned}
&S([x^2, z-1], [0, x-1]) = \\
&= 0 \\
&S([y-1, z-1], [x-1, 0]) = \\
&= 0 \\
&S([y-1, z-1], [0, x-1]) = \\
&= [y-1, z-1]x + [0, x-1](-z) \\
&= [y-1, 0](x-1) + [y-1, z-1] + [0, x-1](-1) \\
&S([x-1, 0], [0, x-1]) = \\
&= 0
\end{aligned}
$$

Llegamos a un conjunto $H_1 = \{[y-1,0], [x^2, z-1], [y-1, z-1], [x-1, 0], [0, x-1], [1, 0]\}$. Este conjunto es ya una base de Gröbner como los siguientes S-vectores demuestran:

$$
\begin{aligned}
&S([y-1, 0], [1-0]) = \\
&= [y-1, 0] + [1, 0](-y) \\
&= [1, 0](-1) \\
&S([x^2, z-1], [1, 0]) = \\
&= [x^2, z-1] + [1, 0](-x^2) \\
&= [y-1, z-1] + [y-1, 0](-1) \\
&S([y-1, z-1], [1, 0]) = \\
&= 0 \\
&S([x-1, 0], [1, 0]) = \\
&= [x-1, 0] + [1, 0](-x) \\
&= [1, 0](-1) \\
&S([0, x-1], [1, 0]) = \\
&= 0
\end{aligned}
$$

Necesitamos calcular las matrices C y D que transformat H en H' y viceversa. Dado que

$$[1, 0] = [y-1, 0] + [x^2, z-1] + [y-1, z-1](-1) + [x-1, 0](-x-1)$$

tenemos

$$
C = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & -1 \\
0 & 0 & 0 & 1 & 0 & -x-1 \\
0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}
\qquad
D = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

De las matrices es claro que $CD = I_5$, por lo que el primer conjunto de generadores A es en este caso vacío, ya que $\mathbf{a}_j = 0$ para cualquier $j = 1, \ldots, 5$. De hecho, esto ocurre porque $H \subseteq H_1$. Podemos dar un lema de demostración directa:

Lema. *Sea $F \subseteq G \subseteq R^n$ tales que $RF = RG$. Existen C y D matrices de cambio de F a G y G a F respectivamente tales que $CD = I_m$, donde m es el número de elementos de F.*

Siguiendo con el algoritmo, un conjunto de generadores de $\mathrm{Syz}^r(H_1)$ es

$$\begin{aligned}
\mathbf{b}_1 &= [x^2 - y + 1, -y + 1, y - 1, 0, 0, 0] \\
\mathbf{b}_2 &= [x - 1, 0, 0, -y + 1, 0, 0] \\
\mathbf{b}_3 &= [1, 1, -1, -x - 1, 0, -1] \\
\mathbf{b}_4 &= [x - 1, 0, -x + 1, 0, z - 1, 0] \\
\mathbf{b}_5 &= [-1, 0, 0, 0, 0, y - 1] \\
\mathbf{b}_6 &= [-1, -1, 1, 0, 0, x^2] \\
\mathbf{b}_7 &= [0, 0, 0, -1, 0, x - 1]
\end{aligned}$$

Componiendo adecuadamente con C tenemos los generadores de $\mathrm{Syz}^r(H)$:

$$\begin{aligned}
\mathbf{b}_1^* &= [x^2 - y + 1, -y + 1, y - 1, 0, 0] \\
\mathbf{b}_2^* &= [x - 1, 0, 0, -y + 1, 0] \\
\mathbf{b}_3^* &= [0, 0, 0, 0, 0] \\
\mathbf{b}_4^* &= [x - 1, 0, -x + 1, 0, z - 1] \\
\mathbf{b}_5^* &= [y - 2, y - 1, -y + 1, -xy - y + x - 1, 0] \\
\mathbf{b}_6^* &= [x^2 - 1, x^2 - 1, -x^2 + 1, -x^3 - x^2, 0] \\
\mathbf{b}_7^* &= [x - 1, x - 1, -x + 1, -x^2, 0]
\end{aligned}$$

El conjunto H' está formado por las 3 primeras coordenadas de cada uno de los $\mathbf{b}_i^*$ y los elementos $\mathbf{g^3}_{ij}$, es decir,

$$\begin{aligned}
H' = \{&[x^2 - y + 1, -y + 1, y - 1], [x - 1, 0, 0], [x - 1, 0, -x + 1], \\
&[y - 2, y - 1, -y + 1], [x^2 - 1, x^2 - 1, -x^2 + 1], [x - 1, x - 1, -x + 1], \\
&[x - 1, 0, 0], [0, x - 1, 0], [0, 0, x - 1]\}
\end{aligned}$$

Nos resta por último calcular un conjunto de generadores de $\mathrm{Syz}^r(H')$. Empezamos demostrando que H' es una base de Gröbner para el R–módulo a

derecha que genera.

$$
\begin{aligned}
&S([x^2-y+1,-y+1,y-1],[x-1,0,0]) = \\
&= [x^2-y+1,-y+1,y-1] + [x-1,0,0](-x) \\
&= [y-2,y-1,-y+1](-1) + [x-1,0,0] \\
&S([x^2-y+1,-y+1,y-1],[x-1,0,-x+1]) = \\
&= 0 \\
&S([x^2-y+1,-y+1,y-1],[y-2,y-1,-y+1]) = \\
&= 0 \\
&S([x^2-y+1,-y+1,y-1],[x^2-1,x^2-1,-x^2+1]) = \\
&= 0 \\
&S([x^2-y+1,-y+1,y-1],[x-1,x-1,-x+1]) = \\
&= 0 \\
&S([x^2-y+1,-y+1,y-1],[x-1,0,0]) = \\
&= [x^2-y+1,-y+1,y-1] + [x-1,0,0](-x) \\
&= [y-2,y-1,-y+1](-1) + [x-1,0,0] \\
&S([x^2-y+1,-y+1,y-1],[0,x-1,0]) = \\
&= 0 \\
&S([x^2-y+1,-y+1,y-1],[0,0,x-1]) = \\
&= 0 \\
&S([x-1,0,0],[x-1,0,-x+1]) = \\
&= 0 \\
&S([x-1,0,0],[y-2,y-1,-y+1]) = \\
&= 0 \\
&S([x-1,0,0],[x^2-1,x^2-1,-x^2+1]) = \\
&= 0 \\
&S([x-1,0,0],[x-1,x-1,-x+1]) = \\
&= 0 \\
&S([x-1,0,0],[x-1,0,0]) = \\
&= [x-1,0,0] + [x-1,0,0](-1) \\
&= 0 \\
&S([x-1,0,0],[0,x-1,0]) = \\
&= 0
\end{aligned}
$$

$$S([x-1,0,0],[0,0,x-1]) =$$
$$= 0$$
$$S([x-1,0,-x+1],[y-2,y-1,-y+1]) =$$
$$= [x-1,0,-x+1]y + [y-2,y-1,-y+1](-x)$$
$$= [x-1,0,0] + [x-1,0,-x+1]$$
$$+ [y-2,y-1,-y+1](-1) + [0,x-1,0](-y+1)$$
$$S([x-1,0,-x+1],[x^2-1,x^2-1,-x^2+1]) =$$
$$= [x-1,0,-x+1]x + [x^2-1,x^2-1,-x^2+1](-1)$$
$$= [x-1,0,-x+1](-1) + [0,x-1,0](-x-1)$$
$$S([x-1,0,-x+1],[x-1,x-1,-x+1]) =$$
$$= [x-1,0,-x+1] + [x-1,x-1,-x+1](-1)$$
$$= [0,x-1,0](-1)$$
$$S([x-1,0,-x+1],[x-1,0,0]) =$$
$$= 0$$
$$S([x-1,0,-x+1],[0,x-1,0]) =$$
$$= 0$$
$$S([x-1,0,-x+1],[0,0,x-1]) =$$
$$= [x-1,0,-x+1] + [0,0,x-1]$$
$$= [x-1,0,0]$$
$$S([y-2,y-1,-y+1],[x^2-1,x^2-1,-x^2+1]) =$$
$$= [y-2,y-1,-y+1]x^2 + [x^2-1,x^2-1,-x^2+1](-y)$$
$$= [x^2-y+1,-y+1,y-1](-1) + [x-1,0,-x+1](-x-1)$$
$$+ [0,x-1,0](-x-1)$$
$$S([y-2,y-1,-y+1],[x-1,x-1,-x+1]) =$$
$$= [y-2,y-1,-y+1]x + [x-1,x-1,-x+1](-y)$$
$$= [x-1,0,0](-1) + [x-1,0,-x+1](-1)$$
$$+ [y-2,y-1,-y+1] + [0,x-1,0](-1)$$
$$S([y-2,y-1,-y+1],[x-1,0,0]) =$$
$$= 0$$
$$S([y-2,y-1,-y+1],[0,x-1,0]) =$$
$$= 0$$

$$
\begin{aligned}
&S([y-2,y-1,-y+1],[0,0,x-1]) = \\
&= [y-2,y-1,-y+1]x + [0,0,x-1]y \\
&= [x-1,0,0](y-1) + [x-1,0,-x+1](-1) \\
&\quad + [y-2,y-1,-y+1] + [0,x-1,0](y-1) \\
&S([x^2-1,x^2-1,-x^2+1],[x-1,x-1,-x+1]) = \\
&= [x^2-1,x^2-1,-x^2+1] + [x-1,x-1,-x+1](-x) \\
&= [x-1,0,-x+1] + [0,x-1,0] \\
&S([x^2-1,x^2-1,-x^2+1],[x-1,0,0]) = \\
&= 0 \\
&S([x^2-1,x^2-1,-x^2+1],[0,x-1,0]) = \\
&= 0 \\
&S([x^2-1,x^2-1,-x^2+1],[0,0,x-1]) = \\
&= [x^2-1,x^2-1,-x^2+1] + [0,0,x-1]x \\
&= [x^2-y+1,-y+1,y-1] + [x-1,0,0](-1) + [x-1,0,-x+1] \\
&\quad + [y-2,y-1,-y+1] + [0,x-1,0](x+1) \\
&S([x-1,x-1,-x+1],[x-1,0,0]) = \\
&= 0 \\
&S([x-1,x-1,-x+1],[0,x-1,0]) = \\
&= 0 \\
&S([x-1,x-1,-x+1],[0,0,x-1]) = \\
&= [x-1,x-1,-x+1] + [0,0,x-1] \\
&= [x-1,0,0] + [0,x-1,0] \\
&S([x-1,0,0],[0,x-1,0]) = \\
&= 0 \\
&S([x-1,0,0],[0,0,x-1]) = \\
&= 0 \\
&S([0,x-1,0],[0,0,x-1]) =
\end{aligned}
$$

De los S–vectores anteriores podemos obtener los generadores de $\mathrm{Syz}^r(H')$,

$$
\begin{aligned}
\mathbf{p}_1 &= [-1,x-1,0,-1,0,0,0,0,0] \\
\mathbf{p}_2 &= [-1,x-1,0,-1,0,0,0,0,0] \\
\mathbf{p}_3 &= [1,0,0,0,0,0,-1,0,0] \\
\mathbf{p}_4 &= [0,1,-y+1,x-1,0,0,0,-y+1,0]
\end{aligned}
$$

$$\begin{aligned}
\mathbf{p}_5 &= [0,0,-x-1,0,1,0,0,-x-1,0]\\
\mathbf{p}_6 &= [0,0,-1,0,0,1,0,-1,0]\\
\mathbf{p}_7 &= [0,1,-1,0,0,0,0,0,-1]\\
\mathbf{p}_8 &= [-1,0,-x-1,-x^2,y,0,0,-x-1,0]\\
\mathbf{p}_9 &= [0,-1,-1,-x+1,0,y,0,-1,-1]\\
\mathbf{p}_{10} &= [0,y-1,-1,-x+1,0,0,0,y-1,y]\\
\mathbf{p}_{11} &= [0,0,1,0,-1,x,0,1,0]\\
\mathbf{p}_{12} &= [1,-1,1,1,-1,0,0,x+1,-x]\\
\mathbf{p}_{13} &= [0,1,0,0,0,-1,0,1,-1].
\end{aligned}$$

Tomamos las seis primeras coordenadas de cada $\mathbf{p}_i$,

$$\begin{aligned}
\mathbf{h}'_1 &= [-1,x-1,0,-1,0,0]\\
\mathbf{h}'_2 &= [-1,x-1,0,-1,0,0]\\
\mathbf{h}'_3 &= [1,0,0,0,0,0]\\
\mathbf{h}'_4 &= [0,1,-y+1,x-1,0,0]\\
\mathbf{h}'_5 &= [0,0,-x-1,0,1,0]\\
\mathbf{h}'_6 &= [0,0,-1,0,0,1]\\
\mathbf{h}'_7 &= [0,1,-1,0,0,0]\\
\mathbf{h}'_8 &= [-1,0,-x-1,-x^2,y,0]\\
\mathbf{h}'_9 &= [0,-1,-1,-x+1,0,y]\\
\mathbf{h}'_{10} &= [0,y-1,-1,-x+1,0,0]\\
\mathbf{h}'_{11} &= [0,0,1,0,-1,x]\\
\mathbf{h}'_{12} &= [1,-1,1,1,-1,0]\\
\mathbf{h}'_{13} &= [0,1,0,0,0,-1].
\end{aligned}$$

El algoritmo nos dice que

$$\mathrm{Hom}(M,R/I) \cong \frac{R^6}{\sum_{i=1}^{13} \mathbf{h}'_i R}.$$

[3.41]. Vamos a calcular ahora $\mathrm{Ext}^n(M,R/I)$, donde M es un R–módulo a izquierda e I un ideal bilátero. Recordemos la definición. Dado M, consideremos una resolución proyectiva de M,

$$\cdots \overset{d_{n+1}}{\to} P_n \overset{d_n}{\to} \cdots \overset{d_3}{\to} P_2 \overset{d_2}{\to} P_1 \overset{d_1}{\to} P_0 \overset{d_0}{\to} M \to 0. \tag{3.9}$$

Si aplicamos $\mathrm{Hom}(-,N)$ a (3.9), obtenemos la siguiente sucesión:

$$0 \to \mathrm{Hom}(M,N) \overset{d_{0*}}{\to} \mathrm{Hom}(P_0,N) \overset{d_{1*}}{\to} \mathrm{Hom}(P_1,N) \overset{d_{2*}}{\to} \cdots \overset{d_{n*}}{\to} \mathrm{Hom}(P_n,N) \overset{d_{n+1*}}{\to} \cdots$$

Se define $\mathrm{Ext}^n(M,N) = \frac{\ker(d_{n+1*})}{\mathrm{im}(d_{n*})}$. Como le ocurre a $\mathrm{Hom}(M,N)$, es un grupo abeliano y solo si M o N es un bimódulo, se le puede dotar de estructura de módulo de forma natural. En particular $\mathrm{Ext}^n(M,R/I)$ es un R–módulo a derecha.

[3.42]. Lema. *Sea $f : R^m/K \to R^n/L$ el morfismo dado por $f(\mathbf{x}+K) = (\Gamma\mathbf{x}^T)^T + L$. Entonces $\mathrm{im}(f) = L'/L$ donde L' está generado por los elementos traspuestos de columnas de Γ.*

Demostración. Inmediata. □

[3.43]. Lema. *Dada una presentación del R–módulo a izquierda M, podemos calcular una resolución libre de M hasta la longitud deseada.*

Demostración. Tenemos que $M \cong R^{s_0}/K_0$ y conocemos un conjunto de generadores de K_0, llámese $\{\mathbf{f}_0,\ldots,\mathbf{f}_{s_1}\}$. Por [3.27] podemos dar una presentación de K_0, luego tenemos las sucesiones exactas

$$0 \longrightarrow K_0 \longrightarrow R^{s_0} \longrightarrow M \longrightarrow 0 \tag{3.10}$$
$$0 \longrightarrow K_1 \longrightarrow R^{s_1} \longrightarrow K_0 \longrightarrow 0 \tag{3.11}$$

Pegando (3.10) con (3.11) obtenemos

$$0 \to K_1 \longrightarrow R^{s_1} \overset{d_1}{\longrightarrow} R^{s_0} \longrightarrow M \longrightarrow 0 \tag{3.12}$$

donde d_1 viene dada por la matriz cuyas filas son los generadores de K_0 (ver [3.31]). Repitiendo el proceso podemos llegar a la longitud deseada. □

[3.44]. Teorema. *Dado un R–módulo M podemos calcular una presentación del R–módulo a derecha $\mathrm{Ext}^n(M,R/I)$ para todo $n \in \mathbb{N}$.*

Demostración. Como $\mathrm{Ext}^0(M,N) = \mathrm{Hom}(M,N)$, podemos suponer que $n > 0$. Dado que todo módulo libre es proyectivo, calculamos una resolución libre de M hasta una longitud $n+1$ mediante [3.43], llámese

$$R^{s_{n+1}} \overset{d_{n+1}}{\longrightarrow} R^{s_n} \overset{d_n}{\longrightarrow} R^{s_{n-1}} \longrightarrow \cdots \longrightarrow R^0 \longrightarrow M \longrightarrow 0.$$

Aplicamos $\mathrm{Hom}(-, R/I)$ a la sucesión anterior y nos quedamos con la parte necesaria para el cálculo de $\mathrm{Ext}^n(M, R/I)$,

$$\mathrm{Hom}(R^{s_{n-1}}, R/I) \xrightarrow{d_n^*} \mathrm{Hom}(R^{s_n}, R/I) \xrightarrow{d_{n+1}^*} \mathrm{Hom}(R^{s_{n+1}}, R/I).$$

Sea Γ_i la matriz asociada a cada morfismo d_i. Por [3.34] y [3.36], la sucesión anterior se convierte en

$$R^{s_{n-1}}/I^{s_{n-1}} \xrightarrow{\gamma_n} R^{s_n}/I^{s_n} \xrightarrow{\gamma_{n+1}} R^{s_{n+1}}/I^{s_{n+1}}$$

donde $\gamma_i(\mathbf{x} + I^{s_{i-1}}) = (\Gamma_i \mathbf{x}^T)^T + I^{s_i}$. El núcleo de γ_{n+1} se calcula mediante [3.28] de manera análoga a $\ker(\gamma)$ en [3.38]. Por otra parte, $\mathrm{im}(\gamma_n)$ se calcula mediante [3.42]. Obtenemos entonces generadores de $L \subseteq K \subseteq R^{s_n}$ donde $\mathrm{im}(\gamma_n) = L/I^{s_n}$ y $\ker(\gamma_{n+1}) = K/I^{s_n}$. Aplicando [3.27] obtenemos una presentación de $\mathrm{Ext}^n(M, R/I)$. □

[3.45]. Observación. En el caso $I = 0$, los módulos I^s y I^n son también nulos, por lo que los álgoritmos se simplifican en algunos pasos.

3.4.4 Transportadores y anuladores.

[3.46]. Sea M un R–módulo a izquierda y sean $A, B \subseteq M$. Se define el transportador cd A por B como el conjunto

$$(A : B) = \{r \in R \mid rB \subseteq A\}.$$

Es fácil comprobar que si A es un R–submódulo de M entonces $(A : B)$ es un ideal a izquierda de R, y si B es R–submódulo de M, $(A : B)$ es un ideal a derecha. Por tanto, si tanto A como B son R–submódulos entonces $(A : B)$ es un ideal bilátero.

Si R es un álgebra de tipo PBW, vamos a poder dar un conjunto de generadores de $(A : B)$ cuando A es un R–módulo finitamente generado y B es un conjunto finito.

[3.47]. Lema. *Supongamos que $M = R^s/L$, $A = A_1/L$ y $B = B_1/L$. Entonces $(A : B) = (A_1 : B_1)$.*

Podemos reducirnos a estudiar submódulos de R^s.

[3.48]. Lema. *Dados $A, B \subseteq M$, $(A : B) = \bigcap_{b \in B}(A : b)$.*

[3.49]. Proposición. *Supongamos que $A \subseteq R^s$ es el R–submódulo generado por $\{\mathbf{f}_1, \ldots, \mathbf{f}_t\}$ y $\mathbf{g} \in R^s$. Sea $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\}$ un sistema de generadores de $\mathrm{Syz}(\mathbf{g}, \mathbf{f}_1, \ldots, \mathbf{f}_t)$ y sea h_i la primera coordenada de $\mathbf{p}_i$ para $i = 1, \ldots, r$. Entonces $(A : \mathbf{g})$ está generado por $\{h_1, \ldots, h_r\}$.*

Demostración. Un elemento $f \in (A : \mathbf{g})$ si y sólo si existen $a_1, \ldots, a_t \in R$ tales que $f\mathbf{g} = a_1\mathbf{f}_1 + \cdots + a_t\mathbf{f}_t$. El resto se razona análogamente a [3.27] y [3.30]. □

[3.50]. Corolario. *Si A es un R–módulo finitamente generado y B es un conjunto finito entonces podemos calcular un conjunto de generadores de $(A : B)$.*

Demostración. Consecuencia inmediata de [3.49], [3.48] y [2.47] (o [3.30]). □

En general, si B es un R–módulo (aún finitamente generado), no podemos dar un conjunto de generadores de $(A : B)$. Sin embargo, si partimos de ideales biláteros entonces sí podemos decir algo más:

[3.51]. Proposición. *Sean $I, J \leq R$ ideales biláteros y supongamos que $J = g_1R + \cdots + g_sR$ entonces*

$$(I : J) = \bigcap_{i=1}^{s} (I : g_i).$$

Demostración. La inclusión $(I : J) \subseteq \bigcap_{i=1}^{s}(I : g_i)$ es inmediata. Supongamos estonces que $rg_i \in I$ para todo I. Un elemento cualquiera de J tiene la forma $g_1r_1 + \cdots + g_sr_s$, luego $r(g_1r_1 + \ldots g_sr_s) = rg_1r_1 + \cdots + rg_sr_s \in I$, lo que nos proporciona la otra inclusión. □

[3.52]. Corolario. *Si $I, J \leq R$ son ideales biláteros entonces podemos calcular un sistema de generadores de $(I : J)$.*

Demostración. Una vez calculada una base de Gröbner de J $G = \{g_1, \ldots, g_s\}$ (para lo cual empleamos el algoritmo [2.67]), el corolario [2.38] nos garantiza que $J = g_1R + \cdots + g_sR$, y el resultado se sigue de [3.49] y [3.51]. □

3.5 Anillo de fracciones. Efectividad.

[3.53]. Vamos a decir que un anillo es computable R si dados elementos $a, b \in R$ existen procedimientos efectivos que nos permiten

(a) decidir si $a = b$,

(b) calcular $a + b$ y $-a$,

(c) calcular ab,

Si K es un anillo de fracciones, es decir, un anillo en el que todo elemento regular tiene inverso, diremos que K es un anillo de fracciones efectivo si K es un anillo efectivo y para cualquier $a \in K$ existen procedimientos finitos para

(d) decidir si a es regular,

(e) calcular a^{-1} si a es regular.

[3.54]. Ejemplos.

[3.54.1]. Los anillos y cuerpos conmutativos computables definidos en [4] son computables en nuestro sentido.

[3.54.2]. Si R es computable, $\mathcal{M}_n(R)$ es computable.

[3.54.3]. Si R es computable y $I \leq R$ es un ideal bilátero, entonces R/I es computable si y sólo si podemos decidir la pertenencia a I de un elemento cualquiera de R.

[3.54.4]. Si R es un dominio conmutativo computable entonces Q_R, el cuerpo de fracciones de R es un cuerpo computable (ver [4, Example 4.82]

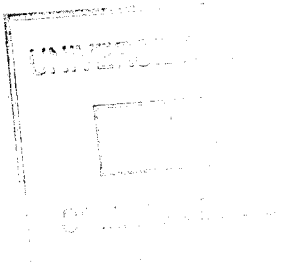
[3.54.5]. Si R es una $\Bbbk$–álgebra de tipo PBW, R es computable si y sólo si $\Bbbk$ es computable.

Vamos a dar un análogo no conmutativo de [3.54.4]. cuando R es el cociente de un álgebra de tipo PBW computable por un ideal semiprimo. En [1.23] se garantiza la existencia del anillo clásico de cocientes en dicho caso. Sea entonces R una $\Bbbk$–álgebra de tipo PBW e $I \leq R$ un ideal semiprimo. Empecemos dando un procedimiento para determinar si un elemento de R/I es regular.

[3.55]. Lema. *Sea $I \leq R$ un ideal bilátero (no necesariamente semiprimo) y sea $r + I \in R/I$. Sea $F = \{f_1, \ldots, f_m\} \subseteq I$ tal que $I = Rf_1 + \cdots + Rf_m$. Sea $\{\mathbf{p}_1, \ldots, \mathbf{p}_s\}$ un sistema de generadores del R–módulo $\mathrm{Syz}(r, f_1, \ldots, f_m)$ y llamemos h_i a la primera coordenada de $\mathbf{p}_i$ con $i = 1, \ldots, s$. Entonces $r+I$ es regular a izquierda si y sólo si $h_1, \ldots, h_s \in I$.*

Demostración. Recordemos que $r + I$ es regular a izquierda si y sólo si $(a + I)(r + I) = 0$ implica $a + I = 0$, o equivalentemente, $ar \in I$ implica $a \in I$. Supongamos pues que $r + I$ es regular. Pongamos $\mathbf{p}_i = [h_i, a_{i1}, \ldots, a_{im}]$. Como $h_i r = -a_{i1} f_1 - \cdots - a_{im} f_m \in I$, por hipótesis $h_i \in I$ para $i = 1, \ldots, s$.

Recíprocamente, supongamos que $h_1, \ldots, h_s \in I$ y que $ar \in I$. Entonces existen $a_1, \ldots, a_m$ tales que $ar = a_1 f_1 + \cdots + a_m f_m$. Como $[a, -a_1, \ldots, -a_m] \in \mathrm{Syz}(r, f_1, \ldots f_m)$ tenemos que $[a, -a_1, \ldots, -a_m]$ es combinación lineal de los



generadores $\{\mathbf{p}_1, \ldots, \mathbf{p}_s\}$, y en consecuencia a es combinación lineal de las primeras coordenadas $\{h_1, \ldots, h_s\}$. Como cada $h_i \in I$ concluimos que $a \in I$. □

Una base de Gröbner para I nos sirve como conjunto F en [3.55]. Ver al efecto [2.38]. Análogamente se comprueba si un elemento es regular a derecha (y por tanto regular).

[3.56]. Proposición. *Sea $I \leq R$ un ideal completamente primo con $I = Rf_1 + \cdots + Rf_m$. Sean $s, a \in R$, con $s + I$ regular, y sea B un conjunto de generadores de* $\mathrm{Syz}(s, a, f_1, \ldots, f_m)$. *Existe un elemento $[b, t, r_1, \ldots, r_m] \in B$ tal que $t + I$ es regular.*

Demostración. Como R/I es un dominio, tenemos que $s + I$ es regular si y sólo si $s \notin I$. Supongamos entonces que para todo elemento $[b, t, r_1, \ldots, r_m] \in B$, $t + I$ no es regular, i.e., $t \in I$. Entonces todo elemento del módulo $\mathrm{Syz}(s, a, f_1, \ldots, f_m)$ tiene su segunda coordenada en I ya ésta es combinación lineal de las segundas coordenadas de los elementos de B. Pero en vista de que R/I es un dominio (y en particular semiprimo), [1.23] garantiza que existen $b + I$ y $t + I$, con $t + I$ regular, tales que $bs + I = ta + I$, es decir, $[-b, t, p_1, \ldots, p_m] \in \mathrm{Syz}(s, a, f_1, \ldots, f_m)$ para algunos $p_1, \ldots, p_m \in R$ y con $t + I$ regular, lo que contradice el hecho de que $t \in I$. □

[3.57]. A partir de un ideal $I \leq R$ completamente primo, la proposición [3.56] nos proporciona un método para calcular los elementos cuya existencia garantiza S1, de manera efectiva en R/I. La entrada son elementos $f, g \in R$ con $f \notin I$ y un subconjunto finito $F \subseteq I$ tal que $I = RFR$.

Paso 1. Utilizamos [2.67] para calcular $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. Por [2.38] $I = Rg_1 + \cdots + Rg_t$. (Si $I = 0$ entonces $G = \varnothing$).

Paso 2. El teorema [3.23], nos dice como calcular un conjunto B que genere $\mathrm{Syz}(f, g, g_1, \ldots, g_t)$.

Paso 3. La proposición [3.56] nos asegura que las segundas coordenadas de cada elemento de B, alguna debe no estar en I. El corolario [2.41] nos permite comprobar la pertenencia a I.

[3.58]. Teorema. *Si $I \leq R$ es un ideal completamente primo, entonces $Q_{cl}(R/I)$ es un anillo de división computable.*

Demostración. Sabemos que R/I es computable (ver [3.54.3].). Sean (s, a) y (t, b) elementos en $Q_{cl}(R/I)$. Por [3.57] podemos calcular elementos no nulos $p, q \in R/I$ tales que $ps = qt$. Entonces $(s, a) = (t, b)$ si y sólo si

$pa = qb \in R/I$. La suma producto se comprueban de forma similar utilizando (1.1): si (s, a) y (t, b) son elementos de $Q_{cl}(R/I)$, entonces podemos calcular elementos $p, q, p', q' \in R/I$ p, q, p' no nulos tales que $ps = qt$ y $p'a = q't$; la suma y producto quedan

$$(s, a) + (t, b) = (ps, pa + qb) \qquad (s, a) \cdot (t, b) = (p's, q'b)$$

Por último, (s, a) es regular si y sólo si $a \neq 0$, y su inverso en este caso es (a, s). □

[3.59]. Si identificamos cada elemento $a \in R/I$ con $(1, a) \in Q_{cl}(R/I)$, entonces para todo $(s, a) \in Q_{cl}(R/I)$ tenemos que $(1, s) \cdot (s, a) = (1, a) \in R/I$. Utilizando el módulo de sicigias a derecha, podemos calcular de manera análoga a [3.57] elementos $p, q \neq 0$ en R/I tales que $sp = aq$. Por tanto,

$$(s, a) \cdot (1, q) = (s, a) \cdot (a, aq) = (s, aq) = (s, sp) = (1, p) \in R/I.$$

Hemos demostrado el siguiente resultado que será de utilidad en [4.19],

Corolario. *Si $I \leq R$ es un ideal completamente primo, para todo $q \in Q_{cl}(R/I)$ podemos calcular elementos no nulos $a_1, a_2 \in R/I$ tales que $a_1 q \in R/I$ y $qa_2 \in R/I$.*

4. IDEALES PRIMOS.

En este capítulo, $\Bbbk$ será un cuerpo conmutativo. El objetivo de este capítulo es abordar por una parte un test que nos sirva para determinar si un determinado ideal en un álgebra de tipo PBW sobre un cuerpo es primo o no. El precedente inmediato hay que buscarlo en el test de primalidad de Gianni, Trager y Zacharias [26] para un anillo de polinomios conmutativo $\Bbbk[x_1, \ldots, x_p]$. Una vez ordenadas las variables, para ver si un ideal I es primo dicho test se basa en estudiar la primalidad de $I \cap \Bbbk[x_1, \ldots, x_i]$ basándose en la primalidad de $I \cap \Bbbk[x_1, \ldots, x_{i-1}]$. Esto se realiza mediante resultados clásicos que podemos encontrar en [83]. Dichos resultados estudian la extensión y contracción de ideales primos con respecto a la introducción de variables y a los anillos de fracciones. En el caso conmutativo, el estudio de los ideales de un anillo se puede realizar mediante los ideales primos. La terminología proviene de los números ideales de Dedekind. En el caso no conmutativo, tomar como definición ideal primo aquellos cuyo cociente es un dominio resulta demasiado restrictivo. Es por ello que se distingue entre los conceptos de ideal primo e ideal completamente primo. La idea para la definición de ideal primo en términos de ideales fue propuesta en 1928 por Krull. La conexión entre ideales primos y elementos nilpotentes es más débil en el caso no conmutativo.

4.1 Extensión y contracción de ideales primos.

Partiendo de las ideas del test de Gianni, Trager y Zacharias, debemos estudiar el comportamiento de los ideales primos con respecto a extensiones de Ore. Las principales propiedades se pueden encontrar en trabajos como [29], [32], [31], [45] y [46] En esta sección R será un anillo noetheriano, y $R[x; \sigma, \delta]$ una extensión de Ore. Recordemos que la definición aparece en [1.24].

[4.1]. Un ideal (bilátero) $I \leq R$ se llama *σ–ideal* si $\sigma(I) \subseteq I$, y *(σ, δ)–ideal* si I es un σ–ideal y $\delta(I) \subseteq I$.

[4.2]. Lema. *Sea $I \leq R[x; \sigma, \delta]$ un ideal bilátero. Si $I \cap R$ es un σ–ideal entonces $I \cap R$ es un (σ, δ)–ideal.*

Demostración. Sea $r \in I \cap R$. Entonces $\delta(r) = xr - \sigma(r)x$. Como $r \in I \cap R$, $\sigma(r) \in I \cap R$ y $\delta(r) \in I$. Dado que $\delta(r) \in R$, se sigue el resultado. □

[4.3]. Dados $I \leq R$ y una derivación torcida (σ, δ), podemos definir el subconjunto $I[x;\sigma,\delta] \subseteq R[x;\sigma,\delta]$ mediante $I[x;\sigma,\delta] = \{\sum r_n x^n \mid r_n \in I\}$. En general $I[x;\sigma,\delta] \subseteq I^e = R[x;\sigma,\delta]IR[x;\sigma,\delta]$, el ideal bilátero de $R[x;\sigma,\delta]$ generado por I.

Proposición. *I es un (σ,δ)-ideal si y sólo si $I[x;\sigma,\delta] = I^e$.*

Demostración. Supongamos que $I[x;\sigma,\delta] = I^e$. Entonces si $r \in I$ tenemos que $xr \in I^e = I[x;\sigma,\delta]$, pero $xr = \sigma(r)x + \delta(r)$, luego $\sigma(r), \delta(r) \in I$.

Recíprocamente, si I es un (σ,δ)–ideal vamos a demostrar que $I^e \subseteq I[x;\sigma,\delta]$. Es suficiente con demostrar que $x^n r \in I[x;\sigma,\delta]$ para todo $r \in I$, lo que hacemos por inducción sobre n. Si $n = 1$ entonces $xr = \sigma(r)x + \delta(r) \in I[x;\sigma,\delta]$ por ser I un (σ,δ)–ideal. Si $n > 1$ entonces

$$\begin{aligned} x^n r &= x x^{n-1} r \\ &= x \sum_i r_i x^i \end{aligned}$$

con $r_i \in I$ por hipótesis de inducción,

$$\begin{aligned} &= \sum_i x r_i x^i \\ &= \sum_i (\sigma(r_i)x + \delta(r_i))x^i \in I[x;\sigma,\delta]. \end{aligned}$$

□

[4.4]. Sea I un ideal bilátero de R tal que I es un (σ,δ)–ideal. Dado que I es invariante por σ y δ, la derivación torcida (σ,δ) induce una nueva derivación torcida, que denotaremos igualmente (σ,δ), definida por $\sigma(r+I) = \sigma(r) + I$ y $\delta(r+I) = \delta(r) + I$. Esto nos permite definir el siguiente morfismo de álgebras:

$$\begin{aligned} \pi : R[x;\sigma,\delta] &\longrightarrow \tfrac{R}{I}[x;\sigma,\delta] \\ r x^n &\longmapsto \overline{r} x^n \qquad \text{donde } \overline{r} = r + I. \end{aligned}$$

Si $I \leq R$ es un (σ,δ)–ideal, entonces $I = R \cap I[x;\sigma,\delta]$. Todo (σ,δ)–ideal de R proviene de un ideal en $R[x;\sigma,\delta]$.

Lema. *Sea $I \leq R$ un (σ,δ)-ideal. Entonces* $\ker(\pi) = I[x;\sigma,\delta]$. *Como consecuencia,*

$$\tfrac{R}{J}[x;\sigma,\delta] \cong \tfrac{R[x;\sigma,\delta]}{J[x;\sigma,\delta]}.$$

[4.5]. Lema. *Sea I un ideal bilátero de $R[x;\sigma,\delta]$ tal que $I \cap R$ es σ-ideal, y sea π el morfismo definido en [4.4] para $I \cap R \leq R$. Entonces $f \in I$ si y sólo si $\pi(f) \in \pi(I)$.*

Demostración. Observemos primero que $I \cap R$ es (σ,δ)-ideal por [4.2]. Una implicación es obvia. Si $\sum \overline{s_n}x^n \in \pi(I)$ entonces existe $\sum r_n x^n \in I$ tal que $\sum \overline{s_n}x^n = \sum \overline{r_n}x^n$. Tenemos entonces que $\sum(\overline{s_n} - \overline{r_n})x^n = 0$, y en vista de que $\frac{R}{R\cap I}[x;\sigma,\delta]$ es libre sobre las potencias de x, tenemos que para todo n $\overline{s_n} - \overline{r_n} = 0$, es decir, $s_n - r_n \in I \cap R$. Por tanto $\sum(s_n - r_n)x^n \in I$ y $\sum s_n x^n = \sum(s_n - r_n)x^n + \sum r_n x^n \in I$. □

[4.6]. Proposición. *Con la notación anterior, I es completamente primo si y sólo si $\pi(I)$ es completamente primo, en cuyo caso $I \cap R$ es completamente primo.*

Demostración. Supongamos que I es completamente primo y que $\pi(r)\pi(s) \in \pi(I)$. Como $\pi(rs) \in \pi(I)$, el lema [4.5] garantiza que $rs \in I$. Necesariamente $r \in I$ o $s \in I$, por lo que $\pi(r) \in \pi(I)$ o $\pi(s) \in \pi(I)$.

Recíprocamente, si $rs \in I$ entonces $\pi(r)\pi(s) \in \pi(I)$, de donde $\pi(r) \in \pi(I)$ o $\pi(s) \in \pi(I)$. El resultado se concluye usando nuevamente [4.5].

Es claro que en dicho caso $I \cap R$ es completamente primo. □

[4.7]. Observación. Consecuencia inmediata de [4.5] es el hecho de que I está generado como ideal a izquierda (resp. derecha, resp. bilátero) por un subconjunto F si y sólo si $\pi(I)$ está generado como ideal a izquierda (resp. derecha, resp. bilátero) por $\pi(F)$.

[4.8]. Ejemplo. La proposición [4.6] no es cierta para ideales primos. Consideremos $\mathbb{C}_{-1}[X,Y]$ el plano cuántico complejo en -1. Esta $\mathbb{C}$-álgebra es la siguientre extensión de Ore:

$$\mathbb{C}_{-1}[X,Y] = \mathbb{C}[X][Y;\sigma] \quad \text{donde } \sigma(X) = -X.$$

El ideal $P = \mathbb{C}_{-1}[X,Y](X^2-1) + \mathbb{C}_{-1}[X,Y](Y^2+1)$ es un ideal primo bilátero, pero $P \cap \mathbb{C}[X] = \mathbb{C}[X](X^2-1)$ no es ni siquiera primario.

[4.9]. La proposición [4.6] permite reducirnos al caso en que $I \cap R = \{0\}$, ya que $\pi(I) \cap \frac{R}{I\cap R} = \{0\}$. De hecho, supongamos que $\pi(f) \in \pi(I) \cap \frac{R}{I\cap R}$. Por una parte, dado que $\pi(f) \in \frac{R}{I\cap R}$ tenemos que $f = f_0 + \sum_{n\geq 1} f_n x^n$ con

$f_n \in I \cap R$ para todo $n \geq 1$. Luego $\pi(f - f_0) = 0$, i.e., $\pi(f_0) = \pi(f) \in \pi(I)$. Por el lema [4.5], $f_0 \in I$, pero $f_0 \in R$, lo que implica que $\pi(f_0) = 0$, i.e., $\pi(f) = 0$.

[4.10]. Vamos a conectar las extensiones de Ore con los anillos de fracciones. Sea R una $\Bbbk$–álgebra noetheriana, (σ, δ) una derivación torcida sobre R y C un conjunto de denominadores a izquierda tal que $C \subseteq C_{reg}$ y $\sigma(C) \subseteq C$. Recordemos que (σ, δ) es una derivación torcida si y sólo si la aplicación $\phi : R \to \mathcal{M}_2(R)$ definida por

$$\phi(r) = \begin{bmatrix} \sigma(r) & \delta(r) \\ 0 & r \end{bmatrix}$$

es un homomorfismo de anillos. La comprobación es sencilla, pero se puede ver al efecto [17, pp. 66-67].

Lema. *La derivación torcida (σ, δ) se extiende de manera única a $C^{-1}R$. La extensión viene dada por la fórmula*

$$\begin{aligned} \sigma'(c^{-1}r) &= \sigma(c)^{-1}\sigma(r) \\ \delta'(c^{-1}r) &= \sigma(c)^{-1}\delta(r) - \sigma(c)^{-1}\delta(c)c^{-1}r \end{aligned} \tag{4.1}$$

Demostración. Véase [29, Lemma 1.3]. □

Vamos a emplear la misma nomenclatura para ambas derivaciones torcidas, (σ, δ). Vamos a llamar $T = R[x; \sigma, \delta]$, $K = C^{-1}R$ y $Q = K[x; \sigma, \delta]$. Es conocido que $Q \cong C^{-1}T$ (ver [29, Lemma 1.4]). Además, si $I \leq T$ es un ideal bilátero tal que $I \cap C = \varnothing$ entonces la noetherianidad de Q nos dice que $QIQ = QI$, como se puede ver en [58, 2.2.26.vi]. Por otra parte es sencillo comprobar que $QI = C^{-1}I$.

[4.11]. Lema. *Con la notación anterior, I es completamente primo si y sólo si QI es completamente primo y $QI \cap T = I$.*

Demostración. Si QI es completamente primo y $QI \cap T = I$, es claro que I es también completamente primo. Supongamos pues que I es completamente primo y $(c^{-1}r)(d^{-1}s) \in QI$. Vamos a utilizar exhaustivamente S1, S2 y (1.1). Existen $a \in C$, $b \in T$ tales que $ar = bd$ y $(c^{-1}r)(d^{-1}s) = (ac)^{-1}(bs) \in QI$. Ya que $QI = C^{-1}I$ tenemos que existen $e \in C$, $v \in I$ tales que $(ac)^{-1}(bs) = e^{-1}v$. La igualdad anterior nos garantiza la existencia de $f, g \in T$ tales que $fac = ge \in C$, $fbs = gv \in I$. Como I es comletamente primo tenemos que $f \in I$, o $b \in I$ o $s \in I$. Si $f \in I$ entonces $fac \in I$ y $\varnothing = I \cap C \supseteq \{fac\}$, lo que es imposible, luego $s \in I$ o $b \in I$. En el primer caso $d^{-1}s \in QI$, y en el segundo caso $ar = bd \in I$. Como $a \in C$ necesariamente $r \in I$ y $c^{-1}r \in QI$. Hemos demostrado que QI es completamente primo. La igualdad $QI \cap T = I$ se obtiene de [58, 2.1.16.vii], ya que QI es primo. □

El siguiente teorema es una de las piezas principales para el test de primalidad [4.22].

[4.12]. Teorema. *Sea I un ideal bilátero de $R[x;\sigma,\delta]$ tal que $I \cap R$ es un (σ,δ)-ideal. Las siguientes afirmaciones son equivalentes*

[a] *I es completamente primo.*

[b] *$I \cap R$ es completamente primo, $K[x;\sigma,\delta]J$ es completamente primo y $J = K[x;\sigma,\delta]J \cap S[x;\sigma,\delta]$, donde $S = \frac{R}{I\cap R}$ (un dominio), $K = Q_{cl}(S)$ y $J = \pi(I)$ (π es el morfismo definido en [4.4]).*

Demostración. Consecuencia inmediata de [4.6], [4.9] y [4.11]. □

4.2 Primalidad en $K[x;\sigma,\delta]$.

En el teorema [4.12], una de las propiedades necesarias para comprobar que I es completamente primo es estudiar si QI lo es, donde $Q = K[x;\sigma,\delta]$. En esta sección vamos a investigar dicho problema cuando $K = Q_{cl}(S)$ con S un dominio, es decir, cuando K es un anillo de división. El algoritmo de la división de Euclides garantiza que $Q = K[x;\sigma,\delta]$ es un dominio de ideales principales. Todo ideal $J \leq Q$ está generado por cualquier elemento de J no nulo de grado en x mínimo. Recordemos estos resultados.

[4.13]. Proposición (Algoritmo de Euclides). *Si $p, q \in Q$ son elementos tales que $\deg_x(p) \geq \deg_x(q)$, existen únicos $q, r \in Q$ tales que*

$$p = qd + r \qquad (resp. \quad p = dq + r)$$
$$r = 0 \quad o \quad \deg_x(r) < \deg_x(d)$$

si además $d \neq 0$, entonces

$$\deg_x(q) + \deg_x(d) = \deg_x(p).$$

[4.14]. Corolario. *Sea $J \leq Q$ un ideal a izquerda (resp. derecha) y sea $f \in J \setminus \{0\}$ un elemento tal que $\deg_x(f) \leq \deg_x(g)$ para todo $g \in J \setminus \{0\}$. Entonces $J = Qf$ (resp. $J = fQ$).*

[4.15]. Observación. Observemos que si $J \leq Q$ es un ideal bilátero, y f es un elemento de grado minimal, entonces $J = Qf = fQ = QfQ$.

[4.16]. Lema. *Sea $J \leq Q$ un ideal bilátero. J es completamente primo si y sólo si J es un ideal a izquierda maximal.*

Demostración. Supongamos que J es maximal a izquierda. Sean $ab \in J$ con $a \notin J$. Como J es maximal a izquierda existen $r \in Q$ y $s \in J$ tales que $1 = ra + s$. Multiplicando por b a la derecha obtenemos $b = rab + sb \in J$, luego J es completamente primo. Recíprocamente, supongamos que $J = Qf$ es completamente primo. Si $J \subsetneq Qg \leq Q$, $g \notin J$. Dado que $f \in Qg$, tenemos que $J \ni f = qg$, de donde $q \in J$ por ser J completamnte primo. Como f tiene grado mínimo,

$$\deg_x(q) \geq \deg_x(f) = \deg_x(q) + \deg_x(g).$$

Necesariamente $\deg_x(g) = 0$, de donde $Qg = Q$. □

[4.17]. Lema. *El ideal a izquierda $J = Qf$ es maximal si y sólo si f es irreducible.*

Demostración. Supongamos que $f = gh$ con g, h no unidades de Q. Entonces $J \subsetneq Qh \lneq Q$ y J maximal implica f irreducible. Recíprocamente, si $Qf \subseteq Qg$ entonces $f = hg$, pero dado que f es irreducible tenemos que h o g es una unidad. Si h es unidad entonces $Qf = Qg$ y si g es unidad entonces $Qg = Q$, por tanto Qf es maximal. □

[4.18]. Proposición. *Sea $J \leq Q$ un ideal bilátero y sea $f \in J$ tal que $J = Qf$. J es completamente primo si y sólo si f es irreducible.*

Demostración. Basta con juntar [4.16] y [4.17]. □

4.3 Contracción de $Q_{cl}(R)$ a R.

En el teorema [4.12] una de las cuestiones a comprobar es que $QI \cap T = I$. Es en esta parte donde las técnicas no conmutativas difieren más profundamente de las conmutativas. Vamos a resolver dicho problema calculando un conjunto de generadores de $J \cap T$ para cualquier $J \leq Q$. Partimos por tanto de S, un dominio noetheriano, (σ, δ), una derivación torcida, $T = S[x; \sigma, \delta]$, $K = Q_{cl}(S) = C^{-1}S$ donde $C = S \setminus \{0\}$, $Q = K[x; \sigma, \delta] = C^{-1}T$.

[4.19]. Sea $J \leq Q$ y sea $g \in J$ de grado mínimo. Podemos tomar $g \in T$. Por sea g de grado mínimo, podemos asegurar que $J = Qg = gQ$ (ver [4.14]). Sea $r \in S$ tal que $r = qa$ con $a \in S$, $q \in K$ y

$$\mathrm{lc}(g)g = gq.$$

El cálculo de r viene garantizado por [3.59] cuando $S = R/I$ con R un álgebra de tipo PBW e I un ideal completamente primo. Sea $H = T[y]gT[y] + T[y](1 - ry) \leq T[y]$.

[4.20]. Proposición. *En las condiciones anteriores* $H \cap T = J \cap T$.

Demostración. Veamos primero que $J \cap T \subseteq H \cap T$. Para ello consideramos $f \in J \cap T$ y procedemos por inducción sobre $\deg_x(f)$. Si $\deg_x(f)$ es mínimo en J entonces $\deg_x(f) = \deg_x(g)$, y por [4.13]

$$f = q_{i_0} g \in T \quad \text{con } q_{i_0} \in K.$$

Tenemos entonces que $q_{i_0} \operatorname{lc}_x(g) \in S$. Por tanto

$$fr = q_{i_0} gr = q_{i_0} gqa = q_{i_0} \operatorname{lc}_x(g) ga.$$

Multiplicando por y, $fry = q_{i_0} \operatorname{lc}_x(g) gay \in H$. Por consiguiente

$$f = fry + f(1 - ry) \in H$$

Supongamos ahora que $\deg_x(f)$ es mayor que el grado mínimo. Tenemos de nuevo

$$f = q_{i_0} g \in T \quad \text{con } q_{i_0} \in Q$$

por [4.13]. Es claro que $\operatorname{lc}_x(f) = \operatorname{lc}_x(q_{i_0}) \sigma^n(\operatorname{lc}_x(g)) \in S$ donde $n = \deg_x(q_{i_0})$. Consecuentemente

$$\begin{aligned}
fr &= \operatorname{lc}_x(q_{i_0}) x^n gr + (q_{i_0} - \operatorname{lc}_x(q_{i_0}) x^n) gr \\
&= \operatorname{lc}_x(q_{i_0}) x^n gqa + (q_{i_0} - \operatorname{lc}_x(q_{i_0}) x^n) gr \\
&= \operatorname{lc}_x(q_{i_0}) x^n \operatorname{lc}_x(g) ga + (q_{i_0} - \operatorname{lc}_x(q_{i_0}) x^n) gr \\
&= \operatorname{lc}_x(q_{i_0}) (\sigma^n(\operatorname{lc}_x(g)) x^n + p) ga + (q_{i_0} - \operatorname{lc}_x(q_{i_0}) x^n) gr \quad (\text{with } \deg_x(p) < n) \\
&= \operatorname{lc}_x(q_{i_0}) \sigma^n(\operatorname{lc}_x(g)) x^n ga + f' \quad (\text{con } \deg_x(f') < \deg_x(f).)
\end{aligned}$$

Dado que $\operatorname{lc}_x(q_{i_0}) \sigma^n(\operatorname{lc}_x(g)) \in S$ tenemos $\operatorname{lc}_x(q_{i_0}) \sigma^n(\operatorname{lc}_x(g)) x^n \in T$ y

$$\operatorname{lc}_x(q_{i_0}) \sigma^n(\operatorname{lc}_x(g)) x^n ga \in J \cap T,$$

lo que implica que $f' \in J \cap T$. Por hipótesis de inducción $f' \in H \cap T$ y entonces

$$fry = f'y + \operatorname{lc}_x(q_{i_0}) \sigma^n(\operatorname{lc}_x(g)) x^n gay \in H,$$

por tanto $f = fry + f(1 - ry) \in H$ como deseábamos.

Para acabar veamos la otra inclusión $J \cap T \supseteq H \cap T$. Si $f \in H \cap T$ entonces

$$f = \sum_{i=1}^{t} p_i g p_i' + s(1 - ry)$$

Podemos ver f en $Q[y]$. Como y conmuta, f puede ser escrito de la siguiente forma:

$$f = \sum_{i=1}^{t} \sum_{j+k=0}^{m} p_{ij} g p'_{ik} y^{j+k} + \sum_{j=0}^{k} s_j y^j - \sum_{j=0}^{k} s_j r y^{j+1}$$

con $p_{ij}, p'_{ik}, s_j \in T$. $Q[y]$ es un Q–módulo libre sobre $\{1, y, y^2, \dots\}$ y $r \in S \setminus \{0\}$, por tanto podemos definir el siguiente morfismo de Q–módulos

$$\begin{aligned} \Phi : Q[y] &\longrightarrow Q \\ y^n &\longmapsto r^{-n} \end{aligned}$$

Dado que $\deg_y(f) = 0$ obtenemos

$$f = \Phi(f) = \Phi\Big(\sum_{i=1}^{t} \sum_{j+k=0}^{m} p_{ij} g p'_{ik} y^{j+k} + \sum_{j=0}^{k} s_j y^j - \sum_{j=0}^{k} s_j r y^{j+1} \Big)$$

$$= \sum_{i=1}^{t} \sum_{j+k=0}^{m} p_{ij} g p'_{ik} r^{-j-k} + \sum_{j=0}^{k} s_j r^{-j} - \sum_{j=0}^{k} s_j r r^{-j-1} = \sum_{i=1}^{t} \sum_{j+k=0}^{m} p_{ij} g p'_{ik} r^{-j-k}.$$

Por consiguiente $f \in J$. □

[4.21]. Proposición. *Sea R una $\Bbbk$–álgebra noetheriana, $P \leq R$ un (σ, δ)-ideal completamente primo, $S = R/P$ y*

$$\begin{aligned} \pi : R[x; \sigma, \delta] &\longrightarrow S[x; \sigma, \delta] \\ rx^n &\longmapsto \overline{r} x^n \qquad \text{donde } \overline{r} = r + P. \end{aligned}$$

Sea H el ideal bilátero generado por $\{\pi(r_1), \dots, \pi(r_s)\}$ y L el generado por $\{r_1, \dots, r_s\}$ y P. Entonces

$$H \cap S = \pi(L \cap R) = \frac{L \cap R}{P}$$

Demostración. [$\supseteq$] Sea $f \in L \cap R$. Entonces $f = a + \sum m_i r_i n_i$ con $a \in R[x; \sigma, \delta] P R[x; \sigma, \delta]$, y usando [4.3], $\pi(f) = \sum \pi(m_i)\pi(r_i)\pi(n_i) \in H$. Por otra parte, $\pi(f) \in S$, luego $\pi(L \cap R) \subseteq H \cap S$.

[$\subseteq$] Sea $f \in H \cap S$. $f = \sum \pi(m_i)\pi(r_i)\pi(n_i)$, luego $f = \pi(g)$ donde $g = \sum m_i r_i n_i \in L$. Como $\pi(g) \in S$, $g = \sum_{i \geq 1} p_i x^i + a_0$ con $p_i \in P$, $a_0 \in R$. Pero $\pi(g) = \pi(a_0)$ y $g - a_0 = \sum_{i \geq 1} p_i x^i \in \langle\langle P \rangle\rangle \subseteq L$, luego $a_0 \in L$, i.e., $H \cap S \subseteq \pi(L \cap R)$. □

4.4 Test de primalidad.

Hemos reunido ya los elementos necesarios para escribir un test de primalidad en extensiones iteradas de Ore. En esta sección,

$$R = \Bbbk[x_1][x_2; \sigma_2, \delta_2] \cdots [x_p; \sigma_p, \delta_p],$$

con $\Bbbk$ un cuerpo. Para que R sea una $\Bbbk$–álgebra de tipo PBW exigiremos que los automorfismos sean del tipo descrito en [2.12].

[4.22]. (Test de Primalidad). La entrada del test es

- $R = \Bbbk[x_1][x_2; \sigma_2, \delta_2] \cdots [x_p; \sigma_p, \delta_p]$.
- Un conjunto de generadores de $I \leq R$, un ideal bilátero.

La salida es

(a) Si cada $I \cap \Bbbk[x_1] \cdots [x_i; \sigma_i, \delta_i]$ es un $(\sigma_{i+1}, \delta_{i+1})$–ideal, el test dice si I es completamente primo o no.

(b) En otro caso, se indica que el test no se puede aplicar.

Vamos a dar una descripción del test.

Paso 1. $k = 1$, $R_1 = \Bbbk[x_1]$, $I_1 = I \cap R_1$.

Paso 2. Si I_k no es completamente primo, I no es completamente primo (FIN).

Paso 3. Si $\sigma_{k+1}(I_k) \not\subseteq I_k$ el algoritmo no se puede aplicar (FIN).

Paso 4. $R_{k+1} = R_k[x_{k+1}; \sigma_{k+1}, \delta_{k+1}]$, $I_{k+1} = I \cap R_{k+1}$, $S_k = \frac{R_k}{I_k}$, $J_{k+1} = \pi(I_{k+1})$, $K_k = Q_{cl}(S_k)$ y $Q_{k+1} = K_k[x_{k+1}; \sigma_{k+1}, \delta_{k+1}]$.

Paso 5. Si $Q_{k+1}J_{k+1}$ no es completamente primo entonces I no es completamente primo (FIN).

Paso 6. Si $Q_{k+1}J_{k+1} \cap S_k[x_{k+1}; \sigma_{k+1}, \delta_{k+1}] \neq J_{k+1}$ entonces I no es completamente primo (FIN).

Paso 7. Si $k+1 = p$ entonces I es completamente primo (FIN), si no $k = k+1$ y volvemos al paso 3

Vamos a comprobar que el test proporciona la salida correcta. En primer lugar, si llegamos al paso 7, dado que partimos de que I_k es completamente primo entonces I_{k+1} también lo es en vista de [4.12]. Dado que $I = I_p$, la salida es correcta. Observemos que basta con que uno de los I_i no sea completamente primo para que I no lo sea. Nos queda comprobar que todos los pasos del test son efectivos.

[4.23]. Los pasos 1 y 4, son meras definiciones. El paso 2 es un paso conmutativo, que tendrá solución cuando $\Bbbk$ sea un cuerpo adecuado. Ver [26]. Por otra parte, podemos conocer un conjunto de generadores (una base de Gröbner) de I_k para cada k utilizando [2.46]. Si llamamos G_k a dichos conjuntos de generadores, comprobar que $\sigma_{k+1}(I_k) \subseteq I_k$ se realiza viendo que $\sigma_{k+1}(g) \in I_k$ para todo $g \in G_k$. Recordemos que la pertenencia se comprueba mediante [2.41], y el paso 3 también es efectivo. Dado que el paso 7 es claramente verificable, nos quedan los pasos 5 y 6. Vamos a ver un lemma que usaremos en ambos.

[4.24]. Sea R una $\Bbbk$–álgebra de tipo PBW. Sea $I \leq R[x;\sigma,\delta]$ un ideal bilátero tal que $I \cap R$ es un (σ,δ)–ideal completamente primo. Sea $S = \frac{R}{I\cap R}$, $T = S[x;\sigma,\delta]$, $J = \pi(I)$, $K = Q_{cl}(S)$ y $Q = K[x;\sigma,\delta]$. Recordemos que π se define en [4.4]. Notamos mediante $\deg_x$ y lc_x el grado y el coeficiente líder respecto de x.

Sea $G = \{h_1,\ldots,h_s,f_1,\ldots,f_t\}$ una base de Gröbner para I tal que $G \cap R = \{h_1,\ldots,h_s\}$, una base de Gröbner para $I\cap R$ (ver [2.46]). Como se indica en [4.7], sabemos que J está geberado por las proyecciones de los elementos de G, es decir, $\{\pi(h_1),\ldots,\pi(h_s),\pi(f_1),\ldots,\pi(f_t)\}$. Dado que $\pi(h_i) = 0$, si llamamos $g_i = \pi(f_i)$ tenemos que J está generado por $\{g_1,\ldots,g_t\}$. Además, $\deg_x(g_i) \geq 1$. El ideal $QJ \leq Q$ está geberado como ideal a izquierda (o derecha) por $\{g_1,\ldots,g_t\}$. Observemos que $J \cap S = \{0\}$ como se demuestra en [4.9], de donde $QJ \neq Q$.

Lema. *Existe un índice $i_0 \in \{1,\ldots,t\}$ tal que $\deg_x(g_{i_0})$ es mínimo entre los elementos no nulos de QJ.*

Demostración. Supongamos que existe un elemento no nulo $g \in QJ$ tal que $\deg_x(g) < \deg_x(g_i)$ para todo i. Es imposible que $\deg_x(g) = 0$, ya que $QJ \neq Q$, por lo que $\deg_x(g) = n \geq 1$. Como $g \in QJ$ tenemos que

$$g = q_1g_1 + \cdots + q_tg_t.$$

Podemos escribir $q_1 = c_1^{-1}t_1$ con $c_1 \in S \setminus \{0\}$ y $t_1 \in T$, por tanto

$$c_1g = t_1g_1 + c_1q_2g_2 + \ldots c_1q_tg_t.$$

Nuevamente $c_1 q_2 \in Q$, luego $c_1 q_2 = c_2^{-1} t_2$ y

$$c_2 c_1 g = c_2 t_1 g_1 + t_2 g_2 + \cdots + c_2 c_1 q_t g_t.$$

Repitiendo el proceso obtenemos un nuevo elemento

$$g' = s_1 g_1 + \ldots s_t g_t$$

tal que $s_i \in T$ y $\deg_x(g') = \deg_x(g)$. Además $g' \in J$, luego existe un $f \in I$ tal que $\pi(f) = g'$ (ver [4.5]). Es fácil observar que podemos suponer que $\deg_x(f) = \deg_x(g') = n$. Podemos escribir f como

$$f = \mathrm{lc}_x(f) x^n + q \quad \text{con } \deg_x(q) < n \text{ y } \mathrm{lc}_x(f) \in R \setminus (I \cap R).$$

La división débil por $\{h_1, \ldots, h_s\}$ nos garantiza la existencia de elementos $h \in I \cap R$ y $r \in R$ tales que $\mathrm{lc}_x(f) = h + r$ y $\mathcal{N}(r) \cap \mathrm{Exp}(I \cap R) = \varnothing$. Llamando $f' = r x^n + q$, tenemos que $\pi(f - f') = \pi(h x^n) = 0$, luego $\pi(f') = g'$. Como $g' \in J$ tenemos que $f' \in I$ y $\exp(f') = (\exp(r), n)$. Dado que $\exp(r) \notin \mathrm{Exp}(I \cap R)$ y que $\exp(h_i) = (\alpha^i, 0)$ donde $\{\alpha^1, \ldots, \alpha^s\}$ generan $\mathrm{Exp}(I \cap R)$, tenemos que

$$\exp(f') \notin \bigcup_{i=1}^{s} \big(\exp(h_i) + \mathbb{N}^{p+1}\big). \tag{4.2}$$

Además,

$$\deg_x(f') = \deg_x(f) = \deg_x(g') = \deg_x(g) < \deg_x(g_i) \leq \deg_x(f_i)$$

para todo i, luego

$$\exp(f') \notin \bigcup_{i=1}^{t} \big(\exp(f_i) + \mathbb{N}^{p+1}\big). \tag{4.3}$$

Como G es una base de Gröbner para I tenemos juntando (4.2) y (4.3) que $\exp(f') \notin \mathrm{Exp}(I)$, lo que es imposible ya que $f' \in I$. □

Por [4.14], $QJ = Q g_{i_0}$.

[4.25]. Vamos a justificar ahora la efectividad del paso 5 en [4.22]. Por el lema [4.24] y la proposición [4.18], $Q_{k+1} J_{k+1}$ es completamente primo si y sólo si el elemento obtenido en [4.24] es irreducible.

[4.26]. Por último, para ver que $Q_{k+1}J_{k+1} \cap S_k[x_{k+1}; \sigma_{k+1}, \delta_{k+1}] = J_{k+1}$ podemos utilizar las proposiciones [4.20] y [4.21]. Para ello debemos garantizar que podemos encontrar el elemento $r = qa$ descrito en [4.20]. Observemos que el generador de grado mínimo obtenido en [4.24] ya verifica que es un elemento de T, el elemento q se obtiene por [4.13] y r aplicando [3.59]. El paso 6 en [4.22] también es efectivo.

[4.27]. Observación. En el caso en que σ_i sea la identidad para cada $i = 1, \ldots, p$, entonces todos los ideales I_i van a ser invariantes bajo σ_{i+1}, por lo que el test se puede aplicar a todos los ideales. En particular el test se aplica sobre todos los ideales en casos como $U(\mathfrak{g})$, donde $\mathfrak{g}$ es un álgebra de Lie resoluble de dimensión finita.

Terminamos con algunos ejemplos de aplicación del test.

[4.28]. Ejemplo. Sea $\mathcal{O}_q(M_2(\Bbbk))$ el anillo de coordenadas cuántico de las matrices 2×2 sobre un cuerpo $\Bbbk$, donde $q \neq 0$. Esta $\Bbbk$–álgebra viene generada por los elementos a, b, c, d y las relaciones

$$ba = qab, ca = qac, dc = qcd, db = qbd, cb = bc, da - ad = (q - q^{-1})bc$$

El llamado determinante cuántico $\mathbf{D}_q = ad - q^{-1}bc$ es un elemento cental sobre $\mathcal{O}_q(M_2(\Bbbk))$, por lo que $I = \mathcal{O}_q(M_2(\Bbbk))(\mathbf{D}_q - 1)$ es un ideal bilátero. Si llamamos $A = \Bbbk[c, b]$ el anillo de polinomios conmutativo con variables b, c, $R = A[d; \sigma_1]$, donde $\sigma_1(c) = qc$ y $\sigma_1(b) = qb$. Finalmente $\mathcal{O}_q(M_2(\Bbbk)) = R[a; \sigma, \delta]$, donde $\sigma(b) = qb$, $\sigma(c) = qc$, $\sigma(d) = d$ y $\delta(b) = \delta(c) = 0$, $\delta(d) = (q - q^{-1})bc$. Como $\mathbf{D}_q - 1$ es central, él mismo es una base de Gröbner para I. Esto nos dice que $I \cap R = \{0\}$, usando [2.46]. Pongamos $D = (R \setminus \{0\})^{-1}R$ y $Q = D[a; \sigma, \delta]$. Fijémonos en que QI viene generado como ideal a izquierda por $\mathbf{D}_q - 1$. Además, $QI \cap R[a; \sigma, \delta] = I$ y $\mathbf{D}_q - 1$ es un elemento irreducible (lineal en a). Por tanto QI es completamente primo y, por tanto I es completamente primo. Nuestro algoritmo da por tanto una demostración de un hecho conocido, que $\mathcal{O}_q(SL_2(\Bbbk)) = \mathcal{O}_q(M_2(\Bbbk))/I$ es un dominio.

[4.29]. Ejemplo. Consideremos el plano cuántico $\Bbbk_q[X, Y]$ ($q \in \Bbbk^\times$ $q \neq 1$). Es una $\Bbbk$–álgebra con dos generadores $\{X, Y\}$ y la relación $YX = qXY$. Este álgebra es una extensión iterada de Ore,

$$\Bbbk_q[X, Y] = \Bbbk[X][Y; \sigma] \qquad \sigma(X) = qX$$

(véase por ejemplo [76]). Sea I el ideal bilátero generado por $Y - X$. Deseamos saber si I es completamente primo o no. Con la idea de calcular $I \cap \Bbbk[X]$

necesitamos una base de Gröbner para I. El conjunto $G = \{Y - X, X^2\}$ es una base de Gröbner para I, por tanto $I_1 = I \cap \Bbbk[X]$ es el ideal generado por X^2. Como $\sigma(X^2) = q^2X^2 \in I_1$, I_1 es un σ–ideal. Además, I_1 no es completamente primo, por tanto I no es completamente primo.

[4.30]. Ejemplo. Vamos a aplicar nuestro test al "álgebra del diamante" D que aparece en [7, 5.9 Beispiel]. Ésta es el álgebra envolvente universal del álgebra de Lie de dimensión cuatro con corchete de Lie

$$\begin{aligned} [x,y] &= 0 \quad [y,z] = x \\ [x,z] &= 0 \quad [y,t] = y \\ [x,t] &= 0 \quad [z,t] = -z, \end{aligned}$$

i.e., la $\Bbbk$–álgebra generada por cuatro elementos $\{x, y, z, t\}$ y relaciones

$$\begin{aligned} yx &= xy \quad zy = yz - x \\ zx &= xz \quad ty = yt - y \\ tx &= xt \quad tz = zt + z \end{aligned}$$

Consecuentemente, D es una extensión iterada de Ore

$$D = \Bbbk[x][y][z;\delta][t;\theta]$$

donde δ y θ son derivaciones tales que $\delta(x) = 0$, $\delta(y) = -x$, $\theta(x) = 0$, $\theta(y) = -y$ y $\theta(z) = z$. Sea I el ideal bilátero generado por $xt - yz - z$. Deseamos saber si I es completamente primo. Como los automorfismos son la identidad podemos aplicar el test. En primer lugar calculamos una base de Gröbner para I, $G = \{x, z\}$. Por tanto $I = Dx + Dz$. $I_1 = I \cap \Bbbk[x] = \langle x \rangle$, que es primo. I_2 es el ideal de $\Bbbk[x][y]$ generado por x, $S_1 = \Bbbk[x]/I_1$, $K_1 = Q_{cl}(S_1)$, $J_2 = \pi(I_2) = 0$ y por tanto $K_1[y]J_2 = 0$ es (completamente) primo y

$$K_1[y]J_2 \cap S_1[y] = 0 = J_2$$

Tenemos que I_2 es completamente primo. Vayamos ahora a I_3, que viene generado por $\{x, z\}$. $S_2 = \Bbbk[x][y]/I_2$ y $J_3 = \pi(I_3)$ es el ideal de $S_2[z;\delta]$ generado por z. Por tanto $K_2[z;\delta]J_3$ también viene generado por z, y como z es irreducible, $K_2[z;\delta]J_3$ es completamente primo. Nos queda comprobar la igualdad

$$K_2[z;\delta]J_3 \cap S_2[z;\delta] = J_3$$

Es suficiente con comprobar que $H \cap S_2[z;\delta] = J_3$ donde H es el ideal de $S_2[z;\delta][u]$ generado por $\{z, 1 - u\}$. Pero $H \cap S_2[z;\delta] = \pi(L \cap \Bbbk[x][y][z;\delta])$

donde L es el ideal de $\Bbbk[x][y][z;\delta][u]$ generado por $\{z, 1-u\}$. Dado que $1-u$ es central, $\{z, 1-u\}$ es una base de Gröbner, y $L \cap \Bbbk[x][y][z;\delta]$ es el ideal bilátero generado por z (eliminación). En consecuencia, $J_3 = H \cap S_2[z;\delta]$ como queríamos. Tenemos que I_3 es completamente primo. Finalmente, $I_4 = I$, $S_3 = \Bbbk[x][y][z;\delta]/I_3$, y $J_4 = \pi(I_4) = 0$. Análogamente a I_2 tenemos que $I = I_4$ es completamente primo.

4.5 Primos minimales y radical.

En esta sección vamos a dar un procedimiento de cálculo de los primos minimales sobre un ideal dado en un álgebra de operadores diferenciales. Los antecedentes conmutativos del tema los podemos encontrar el los algoritmos para la descomposición primaria que aparecen en [26]. Las herramientas no conmutativas empleadas se encuentran en algunos de los tratados más recurridos en la literatura, como [58] y [33]. Debemos mencionar también la monografía de Jategaonkar [35] sobre localización en ideales primos no conmutativos. Vamos a comenzar con algunos prolegómenos necesarios.

[4.31]. Sea R un anillo. Todos los módulos son R–módulos. Recordemos que un submódulo $N \leq M$ se dice esencial si para cualquier otro submódulo no nulo $A \leq M$, $A \cap N \neq 0$. Se suele notar $N \leq_e M$. A cada módulo se asocia un módulo inyectivo $E(M)$ definido por dos propiedades, es el menor inyectivo que contiene a M, es el mayor módulo sobre el que M es esencial. Un módulo es uniforme si todo submódulo suyo no nulo es esencial. Todas estás definiciones y las propiedades básical entre ellas son ampliamente conocidas en la literatura. Vamos a destacar alguna de ellas.

[4.31.1]. Si R es noetheriano y M es un R–módulo finitamente generado, entonces $E(M)$ es la suma directa de n submódulos uniformes. Notamos $\operatorname{rank}(M) = n$. Este número es conocido como la dimensión uniforme, el rango uniforme, dimensión de Goldie, rango de Goldie o simplemente dimensión.

[4.31.2]. $\operatorname{rank}(M_1 \oplus \cdots \oplus M_n) = \operatorname{rank}(M_1) + \cdots + \operatorname{rank}(M_n)$.

Dichas propiedades pueden verse en [33, Chapter 4].

[4.32]. Recordemos que el radical de un ideal $I \leq R$ se define como la intersección de los ideales primos que contienen a I, es decir,

$$\operatorname{rad}(I) = \bigcap_{\substack{P \supseteq I \\ P \text{ primo}}} P.$$

Es inmediato ver que $\operatorname{rad}(I)$ es la intersección de los primos minimales sobre I. En el caso conmutativo se suele definir el radical a través de los elementos

nilpotentes, es decir, como el conjunto

$$N(I) = \{x \in R \mid \exists k \in \mathbb{N}, x^k \in I\}.$$

En un ambiente no conmutativo $N(I)$ ni siquiera es un ideal en general. Se tiene la siguiente inclusión:

[4.33]. Lema. $\mathrm{rad}(I) \subseteq N(I)$.

Demostración. Supongamos que $x \notin N(I)$, entonces $x^n \notin I$ para cualquier $n \in \mathbb{N}$. Sea

$$\Sigma = \{J \leq R \mid x^n \notin J, \forall n \in \mathbb{N}\}$$

Como $I \in \Sigma$, $\Sigma \neq \varnothing$. Si consideramos Σ ordenado por inclusión, el Lema de Zorn nos garantiza la existencia de un elemento maximal $P \in \Sigma$ que contiene a I. Veamos que P es un ideal primo. Supongamos que $y, z \notin P$. Como P es maximal en Σ tenemos que $P + RyR, P + RzR \notin \Sigma$. Por tanto existen $n_1, n_2 \in \mathbb{N}$ tales que $x^{n_1} \in P + RyR$ y $x^{n_2} \in P + RzR$. Como consecuencia existen $a, b \in P$ tales que

$$x^{n_1} = a + \sum \lambda_1 y \lambda_2 \qquad x^{n_2} = b + \sum \mu_1 z \mu_2.$$

Entonces

$$x^{n_1}x^{n_2} = \underbrace{ab + a\sum \lambda_1 y \lambda_2 + \sum \mu_1 z \mu_2 b}_{} + \sum \lambda_1 y \lambda_2 \mu_1 z \mu_2$$

Como $x^{n_1}x^{n_2} = x^{n_1+n_2} \notin P$ y la parte subrayada s pertenece a P, tenemos que existe un sumando en $\sum \lambda_1 y \lambda_2 \mu_1 z \mu_2$ que no pertenece a P, i.e., existen $\lambda_1, \lambda_2, \mu_1, \mu_2$ tales que

$$\lambda_1 y \lambda_2 \mu_1 z \mu_2 \notin P.$$

Al ser P bilátero, necesariamente

$$y\lambda_2\mu_1 z \notin P,$$

lo que implica que $yRz \nsubseteq P$ y P es primo. Como $I \subseteq P$, P es primo y $x \notin P$ tenemos que $x \notin \mathrm{rad}(I)$. □

Para ver más propiedades puede verse [33, Chapter 2]. Hay situaciones sin embargo en la que ambos conjuntos coinciden:

[4.34]. Lema. *Supongamos que todo ideal primo de R es completamente primo. Entonces $N(I) = \mathrm{rad}(I)$.*

Demostración. Sólo hay que ver la inclusión $N(I) \subseteq \text{rad}(I)$. Sea $x \in N(I)$. Entonces existe $n \in \mathbb{N}$ tal que $x^n \in I$. Si P es un ideal (completamente) primo que contiene a I entonces $x^n \in P$ y $x \in P$, luego $x \in P$ y $x \in \text{rad}(I)$. □

Una consecuencia inmediata es

[4.35]. Lema. *Sea $I \leq R[x;\sigma,\delta]$ un ideal de una extensión de Ore de R y supongamos que tanto en R como en $R[x;\sigma,\delta]$ todo ideal primo es completamente primo. Entonces* $\text{rad}(I) \cap R = \text{rad}(I \cap R)$.

Vamos a comenzar el cálculo de los primos minimales comenzando por $K[x;\sigma,\delta]$ donde K es un anillo de división. Para ello vamos a hacer algunas definiciones en un ámbito más general.

[4.36]. Sea A un anillo. Un elemento $p \in A$ se dice *normalmente irreducible* si $p = ab$ con a y b normalizantes implica que $a \in U(A)$ o $b \in U(A)$, donde $U(A)$ denota las unidades de A.

Si A es un dominio en el que todos los ideales a izquierda y derecho son principales, entonces todo ideal bilátero está generado por un elemento normalizante.

[4.37]. Lema. *Sea A un dominio en el que todos sus ideales a izquierda o derecha son principales. Sea $p \in A$ un elemento normalmente irreducible. Entonces Ap es un ideal maximal.*

Demostración. Supongamos que $Ap \subseteq Aa \subseteq A$ con a normalizante. Entonces $p = ba$ y al ser tanto p como a normalizantes, b es normalizante. Como p es normalmente irreducible $a \in U(A)$ o $b \in U(A)$, es decir, $Aa = A$ o $Aa = Ap$. □

[4.38]. Lema. *Sea A un anillo como en [4.37]. Si $p \in A$ es normalmente irreducible y $p \mid ab$ con a y b normalizantes, entonces $p \mid a$ o $p \mid b$.*

Demostración. Supongamos que $p \nmid a$. Entonces $A = Aa + Ap$ por [4.37], con lo que $1 = rp + sa$ para ciertos $r, s \in A$, así $b = rpb + sab = rb'p + sab$ (p es normalizante). Dado que $p \mid ab$ tenemos que $ab = cp$ para un cierto $c \in Q$, con lo que $b = rb'p + scp = tp$, es decir, $p \mid b$. □

Diremos que dos elementos normalizantes a, b en un anillo A son *asociados* si existe una unidad $u \in U(A)$ tal que $a = ub$. Necesariamente u es normalizante. Esta situación se denota $a \sim b$.

[4.39]. Lema. *Sea A un dominio como en [4.37] y sean $p, q \in A$ normalmente irreducibles. Entonces $pq \sim qp$.*

Demostración. El resultado es inmediato si $p \sim q$, ya que en ese caso $q = up$ y

$$pq = pup = u'pp = u''upp = u''qp.$$

Supongamos pues que $p \not\sim q$. Dado que p es normalizante $pq = q'p$ con q' también normalizante. Como $q \mid pq = q'p$ tenemos que $q \mid p$ o $q \mid q'$ por [4.38]. Si $q \mid p$ entonces $p = aq$, lo que fuerza que $p \sim q$ ya que p es normalmente irreducible. Por tanto $q \mid q'$, de donde $q \sim q'$ y $q' = uq$. Entonces

$$pq = q'p = uqp$$

y $pq \sim qp$. □

[4.40]. Teorema. *Sea $Q = K[x; \sigma, \delta]$. Entonces todo elemento normalizante se escribe como producto de elementos normalmente irreducibles. Esta descomposición es única salvo asociados.*

Demostración. Observemos que por [4.14] Q está en las condiciones de [4.37]. La demostración es completamente análoga al caso conmutativo, utilizando los resultados [4.39] y [4.38]. Para la existencia, si $a \in Q$ es normalizante y no es normalmente irreducible entonces $a = a_1 a_2$ con a_1, a_2 normalizantes. Repetimos el proceso con a_1 y a_2. Este procedimiento debe terminar argumentando con el grado. Para la unicidad, si $a = p_1 \cdots p_n = q_1 \cdots q_m$ con p_i, q_j normalmente ireducibles, entonces $p_n \mid q_1 \cdots q_m$ y existe q_i tal que $p_n \sim q_i$. Por [4.39] $p_1 \cdots p_n = uq_1 \cdots q_{i-1} q_{i+1} \cdots q_m q_i$, de donde $p_1 \cdots p_{n-1} = q_1' \cdots q_{i-1} q_{i+1} \cdots q_m$. Reiterando el proceso llegamos a que $n = m$ y a que cada p_i está asociado a un q_j y viceversa. □

[4.41]. Corolario. *Sipodemos dar en Q la descomposición de un elemento normalizante como producto de elementos normalmente irreducibles entonces podemos calcular los primos minimales sobre un ideal dado.*

Demostración. Todo ideal se escribe como Qa con a irreducible. Si $a = up_1^{n_1} \cdots p_m^{n_m}$ con p_i no asociado a p_j cuando $i \neq j$ y u unidad, entonces los primos minimales sobre Qa son $Qp_1, \ldots, Qp_m$. □

[4.42]. Observación. El algoritmo de descomposición primaria se basa precisamente en reducirnos a descomponer en anillos de la forma $Q = K[x; \sigma, \delta]$ con K un anillo de división. De hecho, tendremos en todos los casos que σ es la identidad. Asumiremos en cada casoque dichas descomposiciones pueden hacerse.

[4.43]. Proposición. *Sea S un anillo semiprimo noetheriano y llamemos $P_1, \ldots, P_n$ a sus primos minimales. Supongamos que para todo $i = 1, \ldots, n$ existe $P_i' \supseteq P_i$ tal que $0 = P_1' \cap \cdots \cap P_n'$. Si cada P_i es completamente primo entonces $P_i' = P_i$ para todo i.*

Demostración. Sea $Q = Q_{cl}(S)$. Ya que $P_1, \ldots, P_n$ son los primos minimales de S, los ideales $M_i = QP_i$ constituyen el conjunto de ideales maximales de Q ([35, (2.1.15) Proposition] y [58, 2.1.16]), que es un anillo semisimple [35, (2.3.7) Goldies's Theorem]. Como $P_i' \supseteq P_i$ tenemos que $QP_i' = Q$ o $QP_i' = M_i$ para cada i. Supongamos que $QP_{i_0}' = Q$ para un cierto i_0. Como la localización clásica es un funtor exacto, el monomorfismo canónico

$$R \longrightarrow \frac{R}{P_1'} \oplus \cdots \oplus \frac{R}{P_n'}$$

proporciona el siguiente monomorfismo

$$Q \longrightarrow \frac{Q}{QP_1'} \oplus \cdots \oplus \frac{Q}{QP_n'}.$$

Por otra parte, el monomorfismo esencial [33, Proposition 6.6]

$$R \longrightarrow \frac{R}{P_1} \oplus \cdots \oplus \frac{R}{P_n}$$

proporciona un isomorfismo

$$Q \cong \frac{Q}{M_1} \oplus \cdots \oplus \frac{Q}{M_n}$$

de donde $\operatorname{rank}(Q) = k_1 + \cdots + k_n$, $k_i = \operatorname{rank}\left(\frac{Q}{M_i}\right)$. Pero como $QP_{i_0}' = Q$,

$$\operatorname{rank}(Q) \leq k_1 + \ldots k_n - k_{i_0} < k_1 + \ldots k_n = \operatorname{rank}(Q),$$

lo que es imposible. Por tanto $QP_i' = M_i$ para todo i. Consideremos la siguiente sucesión exacta:

$$0 \longrightarrow P_i \longrightarrow P_i' \longrightarrow \frac{P_i'}{P_i} \longrightarrow 0.$$

Como $Q_{cl}(P_i'/P_i) = 0$, tenemos que para todo $q \in P_i' \setminus P_i$, existe un elemento regular en S tal que $rq \in P_i$. Por ser P_i completamente primo tenemos que $r \in P_i$, luego hay un elemento regular en un primo minimal, lo que contradice [33, Proposition 6.3]. Por tanto $P_i' = P_i$. □

El cálculo de los primos minimales se basa en dos pasos previos.

[4.44]. Lema. *Sea R un álgebra de tipo PBW en la que todo ideal primo es comletamente primo, δ una derivación sobre R y supongamos que en $R[x;\delta]$ todo ideal primo es completamente primo. Sea $I \leq R[x;\delta]$ un ideal bilátero tal que $I \cap R = P$ es un ideal primo. Entonces podemos calcular los primos minimales sobre I. Además, si P' es un primo minimal sobre I entonces $P' \cap R = P$.*

Demostración. Como P es un δ–ideal, podemos construir el morfismo canónico

$$\begin{aligned} \pi : R[x;\delta] &\longrightarrow \tfrac{R}{P}[x;\delta] \\ rx^n &\longmapsto \overline{r}x^n \qquad \text{donde } \overline{r} = r + P \end{aligned}$$

ver [4.4]. Si $\pi(I) = 0$, como $\frac{R}{P}[x;\delta] \cong \frac{R[x;\delta]}{P[x;\delta]}$ tenemos que $I = P[x;\delta]$ que es primo, luego el teorema se satisface para $P_1 = I$.

Supongamos pues que $\pi(I) = J \neq 0$. Llamemos $S = \frac{R}{P}$. S es un dominio y $J \leq S[x;\delta]$ bilátero. Además, por [4.9], $J \cap S = 0$. Sea $K = Q_{cl}(S)$ y $Q = K[x;\delta]$. Existe una biyección entre los ideales primos de Q y los ideales primos de $T = S[x;\delta]$ que no cortan a $S \setminus \{0\}$. Sea $QJ \leq Q$ (recordemos que QJ es bilátero [58, 2.1.16]). Si P_1 es un primo minimal sobre J entonces QP_1 es un primo minimal sobre QJ. Recíprocamente, si Q_1 es un primo minimal sobre QJ entonces $Q_1 \cap T$ es un primo sobre $QJ \cap T \supseteq J$, y si $Q_1 \cap T \supsetneq P' \subseteq J$, entonces $Q_1 = Q(Q_1 \cap T) \supsetneq QP' \supseteq QJ$, lo que contradice la minimalidad de Q_1. Hemos demostrado que si $\{Q_1, \ldots, Q_n\}$ son los primos minimales de QJ y para cada $i = 1, \ldots, n$ $P_i = Q_i \cap T$ entonces $\{P_1, \ldots, P_n\}$ son los primos minimales sobre J. Debemos observar que [4.24] junto con [4.42] nos permiten calcular efectivamente $\{Q_1, \ldots, Q_n\}$. Observemos además que $Q_i \cap T$ es calculable en vista de [4.20] y [4.21]. Como $\frac{R}{P}[x;\delta] \cong \frac{R[x;\delta]}{P[x;\delta]}$, hay un isomorfismo de retículos entre los ideales de $\frac{R}{P}[x;\delta]$ y los ideales de $R[x;\delta]$ que contienen a $P[x;\delta]$ dado por π y π^{-1}. Por tanto el conjunto $\{\pi^{-1}(P_1), \ldots, \pi^{-1}(P_n)\}$ son los primos minimales de I. Además, como $P_i \cap S = \{0\}$ tenemos que $\pi^{-1}(P_i) \cap R = P$. □

[4.45]. Lema. *Sea $R[x;\delta]$ un álgebra en las condiciones de [4.44] y sean $I, I_1, \ldots, I_m \leq R[x;\delta]$ ideales tales que*

(a) $I \subseteq \bigcap_{i=1}^{m} I_i \subseteq \mathrm{rad}(I)$.

(b) Si $P_i = I_i \cap R$ para cada i, entonces $\{P_1, \ldots, P_m\}$ son los primos minimales de $I \cap R$.

Entoces podemos construir los primos minimales de I.

Demostración. Mediante [4.44] calculo para cada $i = 1, \ldots, m$ los primos minimales de I_i, llamémoslos P_{ij} con $j = 1, \ldots, n_i$. En vista de [4.44] $P_{ij} \cap R = I_i \cap R = P_i$ para cada i. Sea P un primo minimal sobre I. Entonces $P \supseteq \text{rad}(I) \supseteq \bigcap_{i=1}^{m}$, por lo que existe un índice i_0 tal que $P \supseteq I_{i_0}$ al ser P primo. Necesariamente existe un $j_0 \in \{1, \ldots, n_{i_0}\}$ tal que $P \supseteq P_{i_0 j_0}$. Por la minimalidad de P y dado que $P_{i_0 j_0} \supseteq I$ tenemnos que $P = P_{i_0 j_0}$. Hemos visto que los primos minimales sobre I se encuentran en el conjunto $\{P_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n_i\}$. Queda ver que no hay inclusiones entre ellos. Supongamos pues que $P_{ij} \supseteq P_{kl}$. Si $i = k$ entonces $j = l$ por la minimalidad de los P_{ij} sobre I_i. Si $i \neq k$ entonces $P_i = P_{ij} \cap R \supseteq P_{kl} \cap R = P_k$, lo que es imposible por la minimalidad de los ideales $P_1, \ldots, P_m$ sobre $I \cap R$. Así, el conjunto $\{P_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n_i\}$ es el conjunto de los primos minimales sobre I. □

[4.46]. Teorema. *Sea R un álgebra de tipo PBW en la que todo ideal primo es completamente primo, así como en todas las iteraciones de la extensión $R[x_1; \delta_1] \cdots [x_p; \delta_p]$. Sean $I, I_1, \ldots, I_m \leq R[x_1; \delta_1] \cdots [x_p; \delta_p]$ tales que*

(a) $I \subseteq \bigcap_{i=1}^{m} I_i \subseteq \text{rad}(I)$.

(b) Si llamamos $P_i = I_i \cap R$ para cada i entonces $\{P_1, \ldots, P_m\}$ son los primos minimales sobre $I \cap R$.

Entonces podemos construir ideales $J_1, \ldots, J_n$ tales que

(a') $I \subseteq \bigcap_{i=1}^{n} J_i \subseteq \text{rad}(I)$.

(b') Si llamamos $P'_i = J_i \cap R[x_1; \delta_1]$ para cada i entonces $\{P'_1, \ldots, P'_n\}$ son los primos minimales sobre $I \cap R[x_1; \delta_1]$.

Demostración. Llamemos $I^c = I \cap R[x_1; \delta_1]$ y $I_i^c = I_i \cap R[x_1; \delta_1]$. Es inmediato que $I^c \subseteq \bigcap_{i=1}^{m} I_i^c$. Además, por [4.35], $\text{rad}(I^c) = \text{rad}(I) \cap R[x_1; \delta_1]$, de donde $\bigcap_{i=1}^{m} I_i^c \subseteq \text{rad}(I^c)$. Por [4.45] podemos calcular los primos minimales $\{P_1, \ldots, P_n\}$ sobre I^c. Definamos para cada $i = 1, \ldots, n$ $J_i = I + \langle\langle P_i \rangle\rangle$, donde $\langle\langle P_i \rangle\rangle$ es el ideal bilátero generado por P_i. Es claro que $I \subseteq \bigcap_{i=1}^{n} J_i$. Por otra parte, si P es un primo sobre I entonces $P^c = P \cap R[x_1; \delta_1]$ es un primo sobre I^c, así pues existe un índice i tal que $P^c \supseteq P_i$, luego $P \supseteq J_i$. Hemos demostrado (a'). Dado que $J_i \cap R[x_1; \delta_1] \supseteq P_i$, el apartado (b') es consecuencia inmediata de aplicar la proposición [4.43] al anillo $S = \frac{R[x_1; \delta_1]}{\text{rad}(I^c)}$. □

[4.47]. Corolario. *Dado un ideal $I \leq \Bbbk[x_1][x_2; \delta_2] \cdots [x_p; \delta_p]$, es posible calcular el conjunto de los primos minimales sobre I.*

Finalicemos con algunos ejemplos.

[4.48]. Ejemplo. Sea R el álgebra envolvente del álgebra de Lie compleja de dimensión tres con base $\{x, y, z\}$ y corchete definido por

$$[x, y] = 0, \quad [x, z] = -x - y, \quad [y, z] = -y$$

es decir, R está generada por los elementos x, y, z y tiene las relaciones

$$yx = xy, \quad zx = xz + x + y, \quad zy = yz + y.$$

Este álgebra se puede escribir como extensión iterada de Ore,

$$R = \mathbb{C}[x][y][z; \delta],$$

donde $\delta(x) = x + y$ y $\delta(y) = y$. Vamos a calcular los primos minimales de varios ideales en este anillo. Vamos a llamar $R_1 = \mathbb{C}[x]$, y $R_2 = \mathbb{C}[x][y]$.

Sea I el ideal bilátero $I = R(x^2 - yz)R$. Calculamos una base de Gröbner para I, y obtenemos $G = \{x^2, xy, y^2, yz\}$. Así, $I \cap R_1 = R_1 x^2$, cuyo primo minimal es $P_1 = R_1 x$. Llamemos $I_1 = I + \langle\langle P_1 \rangle\rangle = \langle\langle x^2 - yz, x \rangle\rangle$. Entonces una base de Gröbner para I_1 es $G_1 = \{x, y\}$. En este punto podemos observar que I_1 es primo, por lo que $P = I_1$ es el único primo minimal sobre I.

Consideremos ahora un nuevo ideal $J = \langle\langle z^2 - z + x^2 y \rangle\rangle$. Una base de Gröbner para J es $\{x^2, y, xz, z^2 - z\}$. $J \cap R_1 = R_1 x^2$, y el primo minimal sobre $R_1 x^2$ en R_1 es $R_1 x$, por lo que debemos pasar al ideal $J' = J + \langle\langle x \rangle\rangle$. Una base de Gröbner de J' es $\{z^2 - z, y, x\}$. Observemos que $J' \cap R_2$ es ya primo, por lo que podemos aplicar el lema [4.44] a $R_2[z; \delta]$. Tenemos que $J' \cap R_2 = P = R_2 x + R_2 y$, por lo que $\frac{R_2}{P} \cong \mathbb{C}$ y la derivación inducida en $\frac{R_2}{P}$ es nula. Debemos descomponer entonces en $S[z]$ el ideal generado por $z^2 - z$, pero sus primos minimales son los ideales generados por $z - 1$ y z. Así, tenemos que los primos minimales sobre J' son $P_1 = J' + \langle\langle z - 1 \rangle\rangle$ y $P_2 = J' + \langle\langle z \rangle\rangle$, es decir, $P_1 = \langle\langle x, y, z - 1 \rangle\rangle$ y $P_2 = \langle\langle x, y, z \rangle\rangle$.

4.6 Ideales 0–dimensionales.

Sea R una $\Bbbk$–álgebra. Un ideal $I \leq R$ se dice 0–dimensional si R/I es un $\Bbbk$–espacio vectorial de dimensión finita.

[4.49]. Lema. *Sea R una PBW lgebra e $I \leq R$ un ideal. El conjunto*

$$\mathcal{B}' = \{X^\alpha + I \mid \alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(I)\}$$

es una $\Bbbk$–base de R/I.

Demostración. Sea $f + I \in R/I$. Entonces $f + I = r + I$ con $\mathcal{N}(r) \cap \text{Exp}(I) = \varnothing$. Esto demuestra que $\mathcal{B}'$ es un sistema de generadores. Para ver la independencia lineal supongamos que

$$\sum_{\alpha \notin \text{Exp}(I)} c_\alpha (X^\alpha + I) = 0$$

Entonces $r = \sum_{\alpha \notin \text{Exp}(I)} c_\alpha X^\alpha \in I$ donde $\mathcal{N}(r) \cap \text{Exp}(I) = \varnothing$. Sea G una base de Gröbner de I. Utilizando el algoritmo de la división $\text{lres}(r, G) = r$ y $\text{lres}(r, G) = 0$, por lo que $r = 0$ y $c_\alpha = 0$ para cualquier α. □

[4.50]. Proposición. *Sea R una PBW–lgebra respecto a un orden graduado. Sea $I \leq R$. I es 0–dimensional si y sólo si la dimensión de Gelfand–Kirillov de R/I es cero.*

Demostración. [⇒] Por el lema previo $\mathbb{N}^p \setminus \text{Exp}(I)$ es un conjunto finito, luego el polinomio de Hilbert–Samuel de $\text{Exp}(I)$ es constante y la dimensión de Gelfand–Kirillov de R/I es cero.

[⇐] Recíprocamente, si dicha dimensión es cero tenemos que el polinomio anterior es constante, por lo que $\dim_{\Bbbk}(F_s(R/I)) < \infty$ y constante a partir de un cierto s. Por tanto $\dim_{\Bbbk}(R/I) = \dim_{\Bbbk}(F_s(R/I))$ es finita. □

[4.51]. Proposición. *Sea R una $\Bbbk$–álgebra de tipo PBW. Sea $I \leq R$ y G una base de Gröbner de I. I es cero dimensional si y sólo si para todo $i \in \{1, \ldots, p\}$ existe $g_i \in G$ tal que $\exp(g_i) = n\varepsilon_i$.*

Demostración. [⇒] Supongamos que existe $i_0 \in \{1, \ldots, p\}$ tal que para todo natural n y todo $g \in G$ $\exp(g) \neq n\varepsilon_{i_0}$; entonces $n\varepsilon_{i_0} \notin \text{Exp}(I)$ para todo $n \in \mathbb{N}$ y por tanto $\mathbb{N}^p \setminus \text{Exp}(I)$ no es finito.

[⇐] Si $\exp(g_i) = n_i\varepsilon_i$ y si $\alpha \notin \text{Exp}(I)$ entonces $\alpha_i < n_i$, ya que si $\alpha_i \geq n_i$ entonces $\alpha = \alpha' + n_i\varepsilon_i$, luego $\mathbb{N}^p \setminus \text{Exp}(I)$ es finito. □

4.7 El radical de un ideal 0–dimensional.

En esta sección proporcionamos un método alternativo para calcular el radical de un ideal reduciendo el problema a una cuestión de álgebra lineal. Consiste en una adaptación al caso no conmutativo del método empleado por Vasconcelos en [80].

Si I es un ideal 0–dimensional y primo entonces R/I es un anillo artiniano primo y por tanto R/I es artiniano simple [43, 11.7] y I es maximal. También es sabido que si I es un ideal 0–dimensional entonces el número de ideales primos (maximales) que lo contienen es finito. Para un ideal I, si notamos

$\{P_1, \ldots, P_m\}$ a los ideales primos por encima de I tenemos que $\mathrm{rad}(I) = P_1 \cap \cdots \cap P_m$ siendo esta intersección irredundante.

El radical de Jacobson de un anillo A se define como la intersección de los ideales maximales a izquierda (o derecha) de A y se nota por $J(A)$.

[4.52]. Proposición. *Sea A una $\Bbbk$–álgebra finito dimensional con $\Bbbk$–base $B = \{u_1, \ldots, u_n\}$. Para un elemento $a \in A$, son equivalentes:*

[a] $a \in J(A)$.

[b] *Para cualquier n–upla $(u_{i_1}, \ldots, u_{i_n}) \in B^n$, $u_{i_1} a u_{i_2} a \ldots u_{i_n} a = 0$.*

Demostración. [$\Rightarrow$] Como A es artiniano, J es un ideal nipotente, con lo que $J^k = 0$ para algún k. Por otra parte A es un subanillo de $M_n(A)$, con lo que $J^n = 0$. Esta implicación es ahora clara.

[$\Leftarrow$] Sea $r \in A$. $r = r_1 u_1 + \cdots + r_n u_n$, con lo que $ra = \sum_{i=1}^n r_i u_i a$. Entonces

$$(ra)^n = \sum_{i_1, \ldots, i_n = 1}^{n} r_{i_1} \ldots r_{i_n} u_{i_1} a \ldots u_{i_n} a = 0.$$

Por tanto

$$\left(1 + ra + (ra)^2 + \cdots + (ra)^{n-1}\right)(1 - ra) = 1 - (ra)^n = 1,$$

i.e., $(1 - ra)$ es invertible a izquierda y por [43, (4.1) Lemma] $a \in J(A)$. □

Estamos interesados entonces en aquellos ideales en los que $\mathrm{rad}(I) = N(I)$. El lema [4.34] proporciona un ejemplo de estos anillos y el siguiente lema nos da más ejemplos.

[4.53]. Lema. *Sea A una $\Bbbk$–álgebra finito dimensional tal que $A/J(A)$ es conmutativo. Entonces*

$$J(A) = \{a \in A \mid \exists n \in \mathbb{N}, a^n = 0\}$$

Demostración. Como A es artiniano, $J(A)$ es nilpotente y

$$J(A) \subseteq \{a \in A \mid \exists n \in \mathbb{N}, a^n = 0\} = N.$$

En vista de [43, (4.11) Lemma] es suficiente con demostar que N es un ideal. Sean $a, b \in N$. Existe $n \in \mathbb{N}$ tal que $a^n = b^n = 0$. La conmutatividad de $A/J(A)$ nos pemite ver que

$$(a+b)^{2n} - \sum_{i=1}^{2n} \binom{n}{i} a^i b^{2n-i} \in J(A)$$

y como la segunda parte vale cero, tenemos que $(a+b)^{2n} \in J(A) \subseteq N$, de donde $(a+b) \in N$.

Análogamente se demuestra que $ra, ar \in N$ para cualesquiera $a \in J$, $r \in A$. □

Estamos ya en condiciones de calcular el radical de un ideal 0–dimensional cuando este coincida con el conjunto de los elementos nilpotentes.

[4.54]. Lema. *Sea $x \in M_n(\Bbbk)$. x es nilpotente si y slo si $\mathrm{tr}(x^i) = 0$ para todo $1 \leq i \leq n$.*

Demostración. Es sabido que $x = sys^{-1}$ con y una matriz triangular. Además $x^i = sy^is^{-1}$ y $\mathrm{tr}(x^i) = \mathrm{tr}(y^i)$, con lo que podemos suponer que x es triangular:

$$x = \begin{pmatrix} x_1 & & * \\ & \ddots & \\ & & x_n \end{pmatrix}.$$

Como

$$x^i = \begin{pmatrix} x_1^i & & * \\ & \ddots & \\ & & x_n^i \end{pmatrix},$$

x es nilpotente si y sólo si $x_1 = \cdots = x_n = 0$, luego ser nilpotente implica $\mathrm{tr}(x^i) = x_1^i + \cdots + x_n^i = 0$ con $1 \leq i \leq n$. Por otra parte, si $\mathrm{tr}(x^i) = 0$ para $1 \leq i \leq n$, entonces

$$\begin{aligned} x_1 + \cdots + x_n &= 0 \\ x_1^2 + \cdots + x_n^2 &= 0 \\ &\vdots \\ x_1^n + \cdots + x_n^n &= 0, \end{aligned}$$

de donde $x_1 = \cdots = x_n = 0$. □

Sea A una $\Bbbk$–álgebra finito dimensional y sea $x \in A$. Podemos dar una aplicación lineal

$$\begin{aligned} \lambda(x) : A &\longrightarrow A \\ a &\longmapsto xa \end{aligned}$$

Llamamos $\mathrm{tr}(x) = \mathrm{tr}(\lambda(x))$.

[4.55]. Lema. *Sea* $A = \Bbbk e_1 \oplus \cdots \oplus \Bbbk e_n$. *Supongamos que* $e_i e_j = \sum_{l=1}^n c_{ijl} e_l$. *Entonces*

$$\operatorname{tr}(xe_k) = \sum_{i=1}^n \left(\sum_{p,l=1}^n c_{ikl} c_{lpp} \right) x_i$$

donde $x = x_1 e_1 + \cdots + x_n e_n$.

Demostración. $xe_k = \sum_{i=1}^n x_i e_i e_k = \sum_{i=1} \sum_{l=1}^n x_i c_{ikl} e_l$. Hagamos actuar xe_k sobre e_p:

$$xe_k e_p = \sum_{i=1}^n \sum_{l=1}^n x_i c_{ikl} e_l e_p = \sum_{i=1}^n \sum_{l=1}^n \sum_{j=1}^n x_i c_{ikl} c_{lpj} e_j,$$

luego

$$\operatorname{tr}(xe_k) = \sum_{p=1}^n \sum_{i=1}^n \sum_{l=1}^n x_i c_{ikl} c_{lpp} = \sum_{i=1}^n \left(\sum_{p,l=1}^n c_{ikl} c_{lpp} \right) x_i$$

□

[4.56]. Proposición. *Sea* A *una* $\Bbbk$*–lgebra finito dimensional cuya* $\Bbbk$*–base es* $\{e_1, \ldots, e_n\}$ *y* $e_i e_j = \sum_{l=1}^n c_{ijl} e_l$. *Supongamos que el conjunto* N *de los elementos nilpotentes de* A *es un ideal. Entonces* $x = x_1 e_1 + \cdots + x_n e_n \in N$ *si y sólo si*

$$\sum_{i=1}^n \left(\sum_{p,l=1}^n c_{ikl} c_{lpp} \right) x_i = 0 \qquad 1 \leq k \leq n$$

Observemos que los lemas [4.34] y [4.53] proporcionan ejemplos donde aplicar esta proposición.

Demostración de la Proposición. [⇒] Si $x \in N$ y $1 \leq k \leq n$, entonces $xe_k \in N$, por tanto xe_k es nilpotente, por lo que $\operatorname{tr}(xe_k) = 0$ en vista del lema [4.54].

[⇐] Si $\operatorname{tr}(xe_k) = 0$ cuando $1 \leq k \leq n$, entonces $\operatorname{tr}(xy) = 0$ para cualquier y por la linealidad de la traza. Por tanto $\operatorname{tr}(x^i) = 0$ para cualquier $1 \leq i \leq n$, i.e., x es nilpotente de nuevo por el lema [4.54]. □

Debemos notar que la proposición [4.56] proporciona un conjunto de ecuaciones del subespacio vectorial N de A. Aplicando las técnicas usuales de álgebra lineal podemos encontrar una base de N como $\Bbbk$–espacio vectorial.

Sea R una $\Bbbk$–lgebra e I un ideal 0–dimensional. La siguiente proposición nos permite calcular un conjunto de generadores de $N(I)$ cuando $N(I)$ es un ideal. Si llamamos $A = R/I$, y N al conjunto de los elementos nilpotentes de A, entonces es claro que $N = N(I)/I$. Seguimos con la hipótesis de que N es un ideal.

[4.57]. Proposición. *Sean $g_1, \ldots, g_s \in R$ tales que $\{g_1 + I, \ldots, g_s + I\}$ es una $\Bbbk$–base de N. Si $I = Rf_1 + \cdots + Rf_t$ entonces*

$$N(I) = Rg_1 + \cdots + Rg_s + Rf_1 + \cdots + Rf_t.$$

Demostración. Como $g_i + I \in N$, tenemos que $g_i \in N(I)$, por lo que la inclusión $Rg_1 + \cdots + Rg_s + Rf_1 + \cdots + Rf_t \subseteq N(I)$ es clara. Por otra parte, supongamos que $f \in N(I)$. Entonces $f+I \in N$, luego $f+I = \sum_{i=1}^{s} k_i(g_i+I)$, por tanto $f - \sum_{i=1}^{s} k_i g_i \in I$ y as $f - \sum_{i=1}^{s} k_i g_i = \sum_{j=1}^{t} l_i f_i$, lo que demuestra la otra inclusión. □

5. DIMENSIONES.

El objetivo fundamental de esta última parte es proporcionar un método de cálculo e la dimensión de Gelfand–Kirillov. El origen de esta dimensión se encuentra en una conjetura propuesta por los autores que le dan nombre sobre anillos de fracciones de ciertas álgebras envolventes, en el intento de demostrar la invarianza de ciertos enteros asociados a dichas álgebras. Cabe citar como literatura más relevante sobre el tema [58, 41, 67]. Dado que en el caso conmutativo esta dimensión coincide con la dimensión de Krull (ver al efecto [58, Theorem 8.2.14]), los antecedentes en el cálculo hay que buscarlos en los métodos conmutativos para calcular dicha dimensión, que pueden verse por ejemplo en [4, 19]. Para álgebras casi conmutativas, los autores Bueso, Castro y Jara [9] proponen un método de cálculo que debemos considerar como el antecedente más inmediato de los resultados de esta memoria. También debemos citar [28], que aporta nuevas líneas para el estudio de la dimensión de Gelfand–Kirillov.

5.1 Dimensión de subconjuntos estables.

[5.1]. Vamos a comenzar con elemento $\alpha = (\alpha_1, \ldots, \alpha_p) \in \mathbb{N}^p$. Definimos el *soporte* de α como el conjunto

$$\operatorname{supp}(\alpha) = \{i \in \{1, \ldots, p\} \mid \alpha_i \neq 0\}.$$

Es evidente que $\operatorname{supp}(\alpha) = \varnothing$ si y sólo si $\alpha = \mathbf{0}$. Dado un subconjunto $X \subseteq \mathbb{N}^p$, definimos:

$$T(X) = \{\sigma \subseteq \{1, \ldots, p\} \mid \sigma \cap \operatorname{supp}(\alpha) \neq \varnothing \quad \forall \alpha \in X\}.$$

[5.2]. Lema.

[5.2.1]. *$T(X) = \varnothing$ si y sólo si $\mathbf{0} \in X$.*

[5.2.2]. *Si $\sigma_1 \in T(X)$ y $\sigma_1 \subseteq \sigma_2$ entonces $\sigma_2 \in T(X)$.*

[5.2.3]. *Si $\sigma \in T(X_1)$ y $X_2 \subseteq X_1$ entonces $\sigma \in T(X_2)$.*

Demostración. La primera propiedad es consecuencia de que si $\mathbf{0} \notin X$ entonces $\{1,\dots,p\} \in T(X)$. Las demás son inmediatas. □

Si X es un monoideal, podemos decir más.

[5.3]. Proposición. *Sea $E \subseteq \mathbb{N}^p$ un monoideal y sea $\{\alpha^1,\dots,\alpha^s\}$ un conjunto de generadores de E. Entonces*

$$T(E) = T(\alpha^1,\dots,\alpha^s).$$

Demostración. Dado que $\{\alpha^1,\dots,\alpha^s\} \subseteq E$, por [5.2] $T(E) \subseteq T(\alpha^1,\dots,\alpha^s)$. Sea por tanto $\sigma \in T(\alpha^1,\dots,\alpha^s)$ y supongamos que $\alpha \in T(E)$. existen $i \in \{1,\dots,s\}$ y $\beta \in \mathbb{N}^p$ tales que $\alpha = \alpha^i + \beta$. Es claro que $\operatorname{supp}(\alpha^i) \subseteq \operatorname{supp}(\alpha)$ y como $\sigma \cap \operatorname{supp}(\alpha^i) \neq \varnothing$ tenemos que $\sigma \cap \operatorname{supp}(\alpha) \neq \varnothing$. Como α es un elemento cualquiera tenemos que $\sigma \in T(E)$. □

La proposición [5.3] nos permite redefinir $T(E)$ cuando E es un monoideal:

$$T(E) = \{\sigma \subseteq \{1,\dots,p\} \mid \sigma \cap \operatorname{supp}(\alpha^i) \neq \varnothing \quad \forall i \in \{1,\dots,s\}\},$$

donde $\{\alpha^1,\dots,\alpha^s\}$ es un conjunto de generadores de E. Además, es independiente del conjunto de generadores elegido.

[5.4]. Sea E un monoideal. Definimos la *dimensión* de E como

$$\dim(E) = \begin{cases} p & \text{si } E = \varnothing, \\ 0 & \text{si } E = \mathbb{N}^p, \\ p - \min\{\operatorname{card}(\sigma) \mid \sigma \in T(E)\} & \text{en otro caso.} \end{cases}$$

Como todos los conjuntos que están envueltos en el cálculo de $\dim(E)$ son finitos (gracias a [5.3]), el número $\dim(E)$ puede ser sencillamente calculado por rastreo.

[5.5]. Sea ahora $E \subseteq \mathbb{N}^{p,n}$ un subconjunto estable. Recordemos que $E = \bigcup_{i=1}^{n} (E_i + (\mathbf{0}, i))$, donde $E_i = \{\alpha \in \mathbb{N}^p \mid (\alpha, i) \in E\}$. Además, cada E_i es un monoideal (ver [1.12]). Definimos la *dimensión* de E como

$$\dim(E) = \sup\{\dim(E_i) \mid 1 \leq i \leq n\}.$$

Las mismas observaciones sobre el cálculo de la dimensión de un monoideal son aplicables aquí.

5.2 Función de Hilbert.

[5.6]. Recordemos (ver [1.4] y [1.16]) que dado $\alpha = (\alpha_1, \ldots, \alpha_p) \in \mathbb{N}^p$, definimos el *grado* de α como

$$|\alpha| = \alpha_1 + \cdots + \alpha_p.$$

Dado un elemento $(\alpha, i) \in \mathbb{N}^{p,n}$, el grado de (α, i) es el número

$$|(\alpha, i)| = |\alpha|.$$

Un orden admisible $\prec$ sobre $\mathbb{N}^{p,n}$ se dice graduado si $|\mathfrak{a}| < |\mathfrak{b}|$ implica $\mathfrak{a} \prec \mathfrak{b}$.

[5.7]. Dado un subconjunto estable $E \subseteq \mathbb{N}^{p,n}$, se define la *función de Hilbert* de E como la aplicación

$$\begin{aligned} HF_E : \mathbb{N} &\longrightarrow \mathbb{N} \\ s &\longmapsto \operatorname{card}\{\mathfrak{a} \in \mathbb{N}^{p,n} \setminus E \mid |\mathfrak{a}| \leq s\}. \end{aligned}$$

El caso $n = 1$ nos da la función de Hilbert de un monoideal.

[5.8]. Proposición. *Dado un subconjunto estable $E \subseteq \mathbb{N}^{p,n}$,*

$$HF_E(s) = HF_{E_1}(s) + \cdots + HF_{E_n}(s),$$

donde $E_1, \ldots, E_n \subseteq \mathbb{N}^p$ son monoideales tales que $E = \bigcup_{i=1}^n (E_i + (\mathbf{0}, i))$.

Demostración. Dado que $(\alpha, i) \notin E$ y $|(\alpha, i)| \leq s$ si y sólo si $\alpha \notin E_i$ y $|\alpha| \leq s$, el resultado en claro. □

Vamos a conectar función de Hilbert con dimensión de un subconjunto estable. Para ello vamos a empezar con la conexión en el caso de monoideales.

[5.9]. Sea $m \in \mathbb{N}$ y $\alpha \in \mathbb{N}^p$. Seguimos [11] y definimos

$$\operatorname{top}_m(\alpha) = \{i \in \{1, \ldots, p\} \mid \alpha_i \geq m\}$$

es decir, los índices donde α supera a m. Definimos también la aplicación

$$\begin{aligned} \operatorname{sh}_m : \mathbb{N}^p &\longrightarrow \mathbb{N}^p \\ \alpha &\longmapsto \beta \text{ con } \begin{cases} \beta_i = m & i \in \operatorname{top}_m(\alpha), \\ \beta_i = \alpha_i & i \notin \operatorname{top}_m(\alpha). \end{cases} \end{aligned}$$

La aplicación anterior representa un "afeitado" de α al nivel m. Es claro que $\operatorname{sh}_m(\operatorname{sh}_m(\alpha)) = \operatorname{sh}_m(\alpha)$ y que $\operatorname{top}_m(\operatorname{sh}_m(\alpha)) = \operatorname{top}_m(\alpha)$. Definimos la siguiente relación de equivalencia sobre $\mathbb{N}^p$:

$$\alpha \sim_m \beta \iff \operatorname{sh}_m(\alpha) = \operatorname{sh}_m(\beta).$$

[5.10]. Lema. *Sean $m \in \mathbb{N}$ y $F \subseteq \mathbb{N}^p$ tales que para todo $\alpha \in F$, $\mathrm{sh}_m(\alpha) \in F$. Sea además*

$$R_m = \{\beta \in F \mid \mathrm{sh}_m(\beta) = \beta\} = \{\beta \in F \mid \beta_i \leq m, 1 \leq i \leq p\}.$$

Entonces,

(1) $F = \biguplus_{\alpha \in R_m} ([\alpha]_m \cap F)$, *donde* $\uplus$ *denota la unión disjunta y* $[\alpha]_m$ *es la clase de equivalencia de* α *respecto a* $\sim_m$.

(2) Si $\alpha \in R_m$ *entonces* $[\alpha]_m \cap F = \{\alpha + \beta \in F \mid \beta_i = 0, \forall i \notin \mathrm{top}_m(\alpha)\}$.

Demostración. La primera parte es consecuencia de que una relación de equivalencia proporciona una partición, y la segunda un sencillo cálculo consecuencia de la definición de sh_m y $\sim_m$. □

[5.11]. Lema. *Sea E el monoideal generado por $\{\alpha^1, \ldots, \alpha^t\}$, llamemos $m = \max\{\alpha_i^j \mid 1 \leq j \leq t, 1 \leq i \leq p\}$ y sea $s \geq pm$. Entonces*

$$\dim(E) = \max\{\mathrm{card}(\mathrm{top}_m(\alpha) \mid \alpha \in \mathbb{N}^p \setminus E, |\alpha| \leq s\}.$$

Demostración. Llamemos $F = \mathbb{N}^p \setminus E$ y $d = \dim(E)$. Supongamos que existe un elemento $\alpha \in F$ tal que $|\alpha| \leq s$ y $\mathrm{card}(\mathrm{top}_m(\alpha)) > d$. Podemos descomponer $\alpha = \beta + \gamma$ donde

$$\beta_i = \begin{cases} \alpha_i & \text{si } i \in \mathrm{top}_m(\alpha) \\ 0 & \text{si } i \notin \mathrm{top}_m(\alpha) \end{cases} \qquad \gamma_i = \begin{cases} 0 & \text{si } i \in \mathrm{top}_m(\alpha) \\ \alpha_i & \text{si } i \notin \mathrm{top}_m(\alpha) \end{cases}$$

Dado que $\alpha \notin E$ tenemos que $\beta, \gamma \notin E$. Además, tal y como se ha construido β tenemos que $\mathrm{supp}(\beta) = \mathrm{top}_m(\alpha)$. Sea $\sigma = \{1, \ldots, p\} \setminus \mathrm{top}_m(\alpha)$. Si $\sigma \in T(E)$ entonces tenemos que $\dim(E) \geq p - \mathrm{card}(\sigma) = \mathrm{card}(\mathrm{top}_m(\alpha)) > \dim(E)$, luego $\sigma \notin T(E)$. Existe un índice k tal que $\sigma \cap \mathrm{supp}(\alpha^k) = \varnothing$, es decir, $\mathrm{supp}(\alpha^k) \subseteq \mathrm{top}_m(\alpha) = \mathrm{supp}(\beta)$. Para todo $i \in \mathrm{supp}(\alpha^k)$, tenemos que $\beta_i \geq m \geq \alpha_i^k$, de donde tenemos que $\beta \in E$, lo que es imposible. Hemos demostrado que

$$\max\{\mathrm{card}(\mathrm{top}_m(\alpha) \mid \alpha \in \mathbb{N}^p \setminus E,\ |\alpha| \leq s\} \leq \dim(E).$$

Veamos la otra desigualdad. Existe un $\sigma \in T(E)$ tal que $\mathrm{card}(\sigma) = p - d$. Consideremos el elemento $\alpha \in \mathbb{N}^p$ definido por

$$\alpha_i = \begin{cases} m & \text{si } i \notin \sigma, \\ 0 & \text{si } i \in \sigma. \end{cases}$$

Es evidente que $|\alpha| \leq s$ y que $\text{supp}(\alpha) = \text{top}_m(\alpha) = \{1, \ldots, p\} \setminus \sigma$. Como $\sigma \in T(E)$, para todo $k \in \{1, \ldots, t\}$, $\sigma \cap \text{supp}(\alpha^k) \neq \varnothing$, es decir, para todo k existe un $i_k \in \text{supp}(\alpha^k)$ tal que $i_k \notin \text{supp}(\alpha)$. Esto implica que $\alpha \notin E$. Como $\text{card}(\text{top}_m(\alpha)) = d$ tenemos que

$$\max\{\text{card}(\text{top}_m(\alpha) \mid \alpha \in \mathbb{N}^p \setminus E,\ |\alpha| \leq s\} \geq \dim(E),$$

lo que termina la demostración. □

[5.12]. Teorema. *Sea E el monoideal que viene generado por $\{\alpha^1, \ldots, \alpha^t\}$, y $m = \max\{\alpha_i^j \mid 1 \leq j \leq t, 1 \leq i \leq p\}$. Entonces existe un único polinomio $h(x) \in \mathbb{Q}[x]$ tal que $HF_E(s) = h(s)$ para todo $s \geq pm$. Además* $\deg(h) = \dim(E)$.

Demostración. El polinomio que deseamos exista debe satisfacer que

$$h(s) = \text{card}\{\alpha \in \mathbb{N}^p \setminus E \mid |\alpha| \leq s\}$$

para todo $s \geq pm$, luego en caso de existir debe ser único. Para demostrar su existencia vamos a contar los elementos de los conjuntos $F_s = \{\alpha \in \mathbb{N}^p \setminus E \mid |\alpha| \leq s\}$. Sea pues $s \geq pm$. El que $\alpha \in F_s$ implica que $\text{sh}_m(\alpha) \in F_s$. Usando [5.10], tenemos que

$$\text{card}(F_s) = \sum_{\alpha \in R_m} \text{card}([\alpha]_m \cap F_s). \tag{5.1}$$

Observemos que para todo $\alpha \in R_m$, $|\alpha| \leq pm < s$. Nuevamente por [5.10] tenemos

$$[\alpha]_m \cap F_s = \{\alpha + \beta \in F_s \mid \beta_i = 0, \forall i \notin \text{top}_m(\alpha)\}$$

si $\alpha \in R_m$. Sea $A = \{\alpha + \beta \mid |\beta| \leq s - |\alpha|;\ \beta_i = 0\, \forall i \notin \text{top}_m(\alpha)$, donde $\alpha \in R_m$. Es sencillo comprobar que $[\alpha]_m \cap F_s \subseteq A$. Por otra parte, si $|\alpha + \beta| \leq s$, $\beta_i = 0$ si $i \notin \text{top}_m(\alpha)$ y $\alpha + \beta \in E$, entonces existe un generador α^k tal que $\alpha_i + \beta_i \geq \alpha_i^k$ para cualquier $i = 1, \ldots, p$. Si $i \notin \text{top}_m(\alpha)$ entonces $\alpha_i = \alpha_i + \beta_i$, luego $\alpha_i \geq \alpha_i^k$; por otra parte, si $i \in \text{top}_m(\alpha)$ entonces $\alpha_i = m \geq \alpha_i^k$, es decir, si $\alpha + \beta \in E$ entonces $\alpha \in E$, lo que es imposible. Con esto se demuestra que $A \cap E = \varnothing$ y $A = [\alpha]_m \cap F_s$. Un sencillo cálculo combinatorio establece que

$$\text{card}(A) = \binom{s - |\alpha| + \text{card}(\text{top}_m(\alpha))}{\text{card}(\text{top}_m(\alpha))},$$

por lo que podemos dar una mejor descripción de (5.1) cuando $s \geq pm$,

$$\operatorname{card}(F_s) = \sum_{\alpha \in R_m} \binom{s - |\alpha| + \operatorname{card}(\operatorname{top}_m(\alpha))}{\operatorname{card}(\operatorname{top}_m(\alpha))}.$$

El polinomio buscado es por tanto

$$h(s) = \sum_{\alpha \in R_m} \binom{s - |\alpha| + \operatorname{card}(\operatorname{top}_m(\alpha))}{\operatorname{card}(\operatorname{top}_m(\alpha))}. \tag{5.2}$$

Si $k \in \mathbb{N}$ entonces $\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$, de donde cada sumando de (5.2) tiene grado $\operatorname{card}(\operatorname{top}_m(\alpha))$ y coeficiente líder positivo. Vemos con esto que

$$\deg(h) = \max\{\operatorname{card}(\operatorname{top}_m(\alpha)) \mid \alpha \in R_m\} = \max\{\operatorname{card}(\operatorname{top}_m(\alpha)) \mid \alpha \in F_s\}.$$

El lema [5.11] garantiza que $\deg(h) = \dim(E)$, lo que termina la demostración del teorema. □

[5.13]. Corolario. *Sean* $\{(\alpha^1, i_1), \ldots, (\alpha^t, i_t)\}$ *generadores del subconjunto estable* $E \subseteq \mathbb{N}^{p,n}$ *y* $m = \max\{\alpha_i^j \mid 1 \leq j \leq t, 1 \leq i \leq p\}$. *Existe un único polinomio* $h(x) \in \mathbb{Q}[x]$ *tal que* $HF_E(s) = h(s)$ *cuando* $s \geq pm$. *Además* $\deg(h) = \dim(E)$.

Demostración. Consecuencia directa de la definición de $\dim(E)$, de [5.8] y de [5.12]. □

5.3 Dimensión de Gelfand–Kirillov.

Las definiciones y primeras propiedades expuestas en esta sección pueden verse con más detalle en [67, Chapter 10] y [58, Chapter 8]. A lo largo del capítulo $\Bbbk$ representa un cuerpo conmutativo.

[5.14]. Sea $F : \mathbb{N} \to \mathbb{R}$ una función creciente y positiva a partir de un cierto natural $n \gg 0$. Decimos que F tiene *crecimiento polinomial* si existe un $d \in \mathbb{R}$ tal que $F(n) \leq n^d$ para todo $n \gg 0$. Si F tiene crecimiento polinomial, definimos

$$\gamma(F) = \inf\{d \in \mathbb{R} \mid F(n) \leq n^d \text{para } n \gg 0\}.$$

En caso de que F no tenga crecimiento polinomial pondremos $\gamma(F) = \infty$.

[5.15]. Lema. *(1)* $\gamma(F) = \limsup \frac{\log(F(n))}{\log(n)}$.

(2) $\gamma(F+G) = \max\{\gamma(f), \gamma(G)\}$.

(3) $\gamma(FG) \leq \gamma(F) + \gamma(G)$.

(4) Si $F(n) = p(n)$ *para* $n \gg 0$ *donde* $p(x) \in \mathbb{R}[x]$ *con coeficiente líder positivo, entonces* $\gamma(F) = \deg(p(x))$.

(5) Si existen $a, b \in \mathbb{N}$ *tales que* $G(n) \leq F(an+b)$ *para todo* $n \in \mathbb{N}$, *entonces* $\gamma(G) \leq \gamma(F)$.

Demostración. Las demostraciónes son sencillas. Pueden verse en [58, 8.1.6 y 8.1.7]. □

[5.16]. Sea R una $\Bbbk$–álgebra finitamente generada. Un *subespacio generador* de R es un $\Bbbk$–subespacio vectorial V finito-dimensional que contiene a 1 y genera a R. Definimos

$$V^0 = \Bbbk, V^1 = V, \ldots, V^n = V \cdot V^{n-1}, \ldots$$

[5.17]. Lema. *1.* $V^n \subseteq V^{n+1}$ *para todo* $n \in \mathbb{N}$.

2. Dado $f \in R$ *existe* $n \in \mathbb{N}$ *tal que* $f \in V^n$.

Demostración. La primera es consecuencia inmediata de que $1 \in V$ y la segunda de que R es finitamente generada. □

El lema [5.17] nos dice que la cadena $\Bbbk \subseteq V \subseteq \cdots \subseteq V^n \subseteq \cdots$ es una filtración exhaustiva (y trivialmente separada) para R. Definiciones y primeras propiedades de álgebras filtradas pueden verse en [66].

[5.18]. Se define la *función de Hilbert* de R asociada a V como la aplicación $HF_V(n) = \dim_{\Bbbk}(V^n)$. La definición depende del subespacio generador. Sin embargo, el crecimiento de la función de Hilbert depende sólo de R:

[5.19]. Proposición. *Sean* V, V' *dos subespacios generadores de* R. *Entonces* $\gamma(HF_V) = \gamma(HF_{V'})$.

Demostración. Dado que V' es finito dimensional y que $V' \subseteq R$ tenemos que existe un $a \in \mathbb{N}$ tal que $V' \subseteq V^a$. En consecuencia, para todo $n \in \mathbb{N}$ tenemos que $(V')^n \subseteq V^{an}$, y es inmediato que $\dim_{\Bbbk}((V')^n) \leq \dim_{\Bbbk}(V^{an})$. En vista de que $HF_{V'}(n) \leq HF_V(an)$ el lema [5.15] nos dice que $\gamma(HF_{V'}) \leq \gamma(HF_V)$. La otra desigualdad se obtiene por simetría. □

[5.20]. Se define la *dimensión de Gelfand–Kirillov* de R como $\mathrm{GKdim}(R) = \gamma(HF_V)$ para cualquier subespacio generador V. La definición es correcta porque toda $\Bbbk$–álgebra R finitamente generada tiene un subespacio generador, y [5.19] asegura que los crecimientos son iguales.

Vamos a rehacer las definiciones anteriores para un R–módulo finitamente generado. Sea M un R–módulo a izquierda finitamente generado por el $\Bbbk$–subespacio vectorial U, que llamaremos también *subespacio generador.* Supondremos que V es un subespacio generador de R.

[5.21]. Lema. *Dado $u \in M$ existe $n \in \mathbb{N}$ tal que $u \in V^n U$.*

Demostración. Consecuencia de que M está finitamente generado por U y [5.17]. □

[5.22]. Definimos la *función de Hilbert* de M respecto de V y U como

$$HF_{V,U}(n) = \dim_{\Bbbk}(V^n U).$$

[5.23]. Proposición. *Si V, V' son subespacios generadores de R y U, U' dos subespacios generadores de M, entonces $\gamma(HF_{V,U}) = \gamma(HF_{V',U'})$.*

Demostración. Análogamente a [5.19], existen $a, b \in \mathbb{N}$ tales que $V' \subseteq V^a$ y $U' \subseteq V^b U$. Por tanto $(V')^n U' \subseteq V^{an+b} U$. El resto se razona igual que [5.19]. □

[5.24]. En vista de [5.23] podemos definir $\mathrm{GKdim}(M) = \gamma(HF_{V,U})$, donde V y U son subespacios generadores de R y M respectivamente.

El resto de la sección lo dedicaremos a relacionar la dimensión de Gelfand–Kirillov de un R–módulo finitamente generado con la dimensión de subconjuntos estables cuando R es un álgebra de tipo PBW. Esto nos dará un método de cálculo de la dimensión de Gelfand–Kirillov. En lo que sigue, R va a ser un álgebra de tipo PBW con $\Bbbk$–base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$ con respecto a un orden graduado ' $\leq'$. Además, ' $\preceq'$ denotará al orden TOP sobre $\mathbb{N}^{p,n}$.

[5.25]. Lema. *Sea $V = \Bbbk 1 + \Bbbk u_{\epsilon_1} + \cdots + \Bbbk u_{\epsilon_p}$. Entonces V es un subespacio generador de R.*

Demostración. Consecuencia de [2.6]. □

A partir de ahora V es el subespacio generador dado en [5.25].

[5.26]. Lema. *Si $f \in R$ entonces $f \in V^k$ si y sólo si $|\exp(f)| \leq k$.*

Demostración. Por inducción sobre k. Si $k = 1$ el resultado es inmediato. Sea $k > 1$ y supongamos que $f \in V^k$. Entonces $f = \sum_{i=1}^{p} u_{\epsilon_i} g_i$ con $g_i \in V^{k-1}$. Por hipótesis de inducción $|\exp(g_i)| \leq k-1$, además $\exp(f) \leq \max\{\epsilon_i + \exp(g_i) \mid 1 \leq i \leq p\}$. Existe un índice i_0 tal que $\exp(f) \leq \epsilon_{i_0} + \exp(g_{i_0})$ y por ser el orden graduado $|\exp(f)| \leq |\epsilon_{i_0} + \exp(g_{i_0})| \leq k - 1 + 1 = k$.

Recíprocamente supongamos que $|\exp(f)| \leq k$. Claramente podemos suponer que $f = u_\alpha$ con $|\alpha| \leq k$. Hacemos inducción sobre α. Si $\alpha = \mathbf{0}$ es claro que $u_\alpha \in V^k$. Si $\alpha \neq \mathbf{0}$ entonces $\alpha = \alpha' + \epsilon_i$ para un cierto i, con $|\alpha'| \leq k-1$. Dado que

$$u_\alpha = q^{-1}_{\epsilon_i,\alpha'} u_{\epsilon_i} u_{\alpha'} + g \text{ con } \exp(g) < \alpha.$$

Por las hipótesis de inducción tenemos que $g \in V^k$ y $u_{\alpha'} \in V^{k-1}$, luego $u_\alpha \in V^k$. □

[5.27]. Proposición. *Sea $L \leq R^n$ un R–submódulo a izquierda y supongamos que $\mathbb{N}^{p,n}$ tiene el orden TOP. Llamemos además $U = \Bbbk(\mathbf{e}_1 + L) + \cdots + \Bbbk(\mathbf{e}_n + L)$. Entonces*

$$V^k U = \{\mathbf{f} + L \mid |\exp(\mathbf{f})| \leq k\}.$$

Demostración. Supongamos que $|\exp(\mathbf{f})| \leq k$. Pongamos $\mathbf{f} = f_1\mathbf{e}_1 + \cdots + f_n\mathbf{e}_n$. Supongamos que existe un i_0 tal que $|\exp(f_{i_0})| > k$. Entonces $|\exp(f_{i_0}\mathbf{e}_{i_0})| = |\exp(f_{i_0})| > k \geq |\exp(\mathbf{f})|$, y siendo el orden graduado,

$$\exp(f_{i_0}\mathbf{e}_{i_0}) \succ \exp(\mathbf{f}) = \max\{\exp(f_i\mathbf{e}_i) \mid 1 \leq i \leq n\},$$

lo que es imposible. Necesariamente $|\exp(f_i)| \leq k$ y por el lemma [5.26] $f_i \in V^k$, lo que implica la inclusión

$$V^k U \supseteq \{\mathbf{f} + L \mid |\exp(\mathbf{f})| \leq k\}.$$

Recíprocamente, si $\mathbf{f}+L \in V^k U$, entonces $\mathbf{f}+L = \sum_{i=1}^n f_i(\mathbf{e}_i+L)$ con $f_i \in V^k$. En este caso $\mathbf{f} + L = \left(\sum_{i=1}^n f_i\mathbf{e}_i\right) + L$. Por otra parte, $|\exp(\sum_{i=1}^n f_i\mathbf{e}_i)| = |\max\{\exp(f_i\mathbf{e}_i) \mid 1 \leq i \leq n\}| \leq k$, lo que demuestra la otra inclusión. □

[5.28]. Teorema. *Sea $M = R^n/L$, V el subespacio geberador usual sobre R y U el subespacio generador descrito en [5.27]. Entonces*

$$\dim_{\Bbbk}(V^k U) = \operatorname{card}\left\{\mathfrak{a} \in \mathbb{N}^{p,n} \setminus \operatorname{Exp}(L) \mid |\mathfrak{a}| \leq k\right\}.$$

Demostración. Sea $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ una base de Gröbner para L. Sea $\mathbf{f}+I \in V^k U$. Por [5.27] podemos suponer que $|\exp(\mathbf{f})| \leq k$. Por el teorema [3.9] $\mathbf{f} = q_1\mathbf{g}_1 + \cdots + q_t\mathbf{g}_t + \mathbf{r}$ donde $\exp(\mathbf{r}) \preceq \exp(\mathbf{f})$ y $\mathcal{N}(\mathbf{r}) \cap \operatorname{Exp}(L) = \varnothing$, es decir,

$$\mathbf{r} = \sum_{\mathfrak{a} \notin \operatorname{Exp}(L)} c_{\mathfrak{a}} \mathbf{u}_{\mathfrak{a}}.$$

Dado que $\mathfrak{a} \preceq \exp(\mathbf{r})$ para todo $\mathfrak{a} \in \mathcal{N}(\mathbf{r})$ y que el orden es graduado podemos comprobar que $|\mathfrak{a}| \leq k$, luego

$$\mathbf{r} = \sum_{\substack{\mathfrak{a} \notin \mathrm{Exp}(L) \\ |\mathfrak{a}| \leq k}} c_{\mathfrak{a}} \mathbf{u}_{\mathfrak{a}}.$$

Por otra parte, si $\mathfrak{a} \notin \mathrm{Exp}(L)$ entonces $\mathbf{u}_{\mathfrak{a}} \notin L$. Hemos demostrado que $\{\mathbf{u}_{\mathfrak{a}} + L \mid |\mathfrak{a}| \leq k, \mathfrak{a} \notin \mathrm{Exp}(L)\}$ es un sistema de generadores de $V^k U$. Para ver la independencia lineal supongamos que

$$0 = \sum_{\substack{\mathfrak{a} \notin \mathrm{Exp}(L) \\ |\mathfrak{a}| \leq k}} c_{\mathfrak{a}} (\mathbf{u}_{\mathfrak{a}} + L).$$

Entonces $\mathbf{r} = \sum_{\mathfrak{a} \notin \mathrm{Exp}(L)} c_{\mathfrak{a}} \mathbf{u}_{\mathfrak{a}} \in L$, donde además $\mathcal{N}(\mathbf{r}) \cap \mathrm{Exp}(L) = \varnothing$. Por [3.9] y [3.11.2]. tenemos que $\mathbf{r} = \mathrm{lres}(\mathbf{r}, G) = 0$, por lo que $c_{\mathfrak{a}} = 0$. La independencia lineal queda así demostrada. □

[5.29]. Corolario. *Sea $M \cong R^n/L$. Entonces*

$$\mathrm{GKdim}(M) = \dim(\mathrm{Exp}(L))$$

Demostración. El teorema [5.28] nos dice que $HF_{V,U}(k) = HF_{\mathrm{Exp}(L)}(k)$, y por lo tanto $\gamma(HF_{V,U}) = \gamma(HF_{\mathrm{Exp}(L)})$. □

[5.30]. Corolario. *Todo R–módulo finitamente generado sobre una $\Bbbk$–álgebra de tipo PBW sobre un orden graduado tiene dimensión de Gelfand–Kirillov entera.*

Finalicemos la sección con algunos ejemplos.

[5.31]. Ejemplo. Seguimos con el ejemplo [2.61], en el que $U = U(\mathfrak{sl}(2))$ e $I = Ux^2 + Uy^2 + Uh^2$. Una base de Gröbner para I es $G = \{x^2, y^2, h^2, 2xyh - h, xh, yh, h\}$. Por tanto $\mathrm{Exp}(I)$ está generado por los elementos

$$\{(2,0,0), (0,2,0), (0,0,2), (1,1,1), (1,0,1), (0,1,1), (0,0,1)\}.$$

Dado que $\mathrm{supp}((2,0,0)) = \{1\}$, $\mathrm{supp}((0,2,0)) = \{2\}$ y $\mathrm{supp}((0,0,1)) = \{3\}$, necesariamente $T(\mathrm{Exp}(I)) = \{\{1,2,3\}\}$ y por consiguiente

$$\mathrm{GKdim}(U/I) = \dim(\mathrm{Exp}(I)) = 3 - 3 = 0.$$

como U–módulo a izquierda.

[5.32]. Ejemplo. El anterior es un caso particular de uno de los ejemplos clásicos, las álgebras envolventes universales de álgebras de Lie $U(\mathfrak{g})$. Éstas, junto con las álgebras de Weyl $\mathbb{A}_n(\Bbbk)$, aparecen tratadas en [9]. Todas ellas son álgebras de tipo PBW con respecto a un orden graduado, por lo que podemos aplicarles este método.

[5.33]. Ejemplo. Vamos a calcular la dimensión de Gelfand–Kirillov en un caso no clásico. Sea R la $\Bbbk$–álgebra generada por e, f, k, l con relaciones

$$\begin{aligned} ek &= q^{-2}ke & el &= q^2le \\ kf &= q^{-2}fk & lf &= q^2fl \\ kl &= lk & ef &= fe + \frac{k^2 - l^2}{q^2 - q^{-2}} \end{aligned}$$

donde $q \in \Bbbk^\times$ no es una raíz cuarta de 1. Podemos ver R como una extensión iterada de Ore, $\Bbbk[f][k; \sigma_k, \delta_k][l; \sigma_l, \delta_l][e, \sigma_e, \delta_e]$, donde

$$\begin{gathered} \sigma_k(f) = q^{-2}f, \\ \delta_k(f) = 0 \\ \sigma_l(k) = k, \quad \sigma_l(f) = q^2f, \\ \delta_l(k) = 0, \quad , \delta_l(f) = 0 \\ \sigma_e(l) = q^2l, \quad , \sigma_e(k) = q^{-2}k, \quad , \sigma_e(f) = f, \\ \delta_e(l) = 0, \quad \delta_e(k) = 0, \quad , \delta_e(f) = \frac{k^2 - l^2}{q^2 - q^{-2}}. \end{gathered}$$

Es fácil comprobar que R es un álgebra de tipo PBW con base los monomios $f^a k^b l^c e^d$ $(a, b, c, d) \in \mathbb{N}^4$ y orden lexicográfico graduado con $\epsilon_1 < \epsilon_2 < \epsilon_3 < \epsilon_4$. El elemento kl es central, es decir, $rkl = klr$ para cualquier $r \in R$, por tanto el ideal $I = R(kl - 1)$ es bilátero. Es conocido que $R/I \cong U_q(\mathfrak{sl}(2))$, por lo que podemos calcular de manera sencilla la dimensión de Gelfand–Kirillov de $U_q(\mathfrak{sl}(2))$. Como I es principal, $G = \{kl - 1\}$ es una base de Gröbner para I, y en consecuencia $\mathrm{Exp}(I) = \exp(kl - 1) + \mathbb{N}^4 = (0, 1, 1, 0) + \mathbb{N}^4$. Entonces $\mathrm{supp}((0, 1, 1, 0)) = \{2, 3\}$ y $\{2\} \in T(\mathrm{Exp}(I))$, por lo que $\dim(\mathrm{Exp}(I)) = 4 - 1 = 3$. Necesariamente, $\mathrm{GKdim}(U_q(\mathfrak{sl}(2))) = 3$.

De manera análoga al ejemplo anterior podemos demostrar el siguiente resultado,

[5.34]. Corolario. *Sea R una PBW álgebra con respecto a un orden graduado sobre $\mathbb{N}^p$. Si $I = Rf \neq R$ entonces* $\mathrm{GKdim}(R/I) = p - 1$.

[5.35]. Ejemplo. El álgebra cuántica $\mathcal{O}_q(SL(n))$ se define como el cociente de $\mathcal{O}_q(M_n(\mathbb{C}))$ sobre el ideal generado por el elemento central

$$\det_q(X) = \sum_{\sigma \in S_n} (-q^{-2})^{\ell(\sigma)} u_{1,\sigma 1} \dots u_{n,\sigma n}$$

(donde $\ell(\sigma)$ es el mínimo número de trasposiciones requerido para expresar σ como producto de trasposiciones simples $(i, i+1)$). Es por tanto claro que la dimensión de Gelfand–Kirillov de $\mathcal{O}_q(SL(n))$ es $n^2 - 1$ (véase [78]).

[5.36]. Ejemplo. El anillo de coordenadas cuántico $\mathcal{O}_q(GL(n))$. Este álgebra se define como la localización de $\mathcal{O}_q(M_n(\Bbbk))$ con respecto al elemento central $\det_q(X)$, es decir,

$$\mathcal{O}_q(GL(n)) = \mathcal{O}_q(M_n(\Bbbk))[\det_q(X)^{-1}].$$

Como $\det_q(X)$ es central, podemos dar una descrpción alternativa,

$$\mathcal{O}_q(GL(n)) = \frac{\mathcal{O}_q(M_n(\Bbbk))[Y]}{(Y \det_q(X) - 1)},$$

donde Y es una nueva variable. Por consiguiente, la dimensión de Gelfand–Kirillov es

$$\mathrm{GKdim}(\mathcal{O}_q(GL(n))) = (n^2 + 1) - 1 = n^2.$$

(véase [78]).

5.4 Ordenes casi–graduados.

En esta sección vamos a ampliar la clase de PBW álgebras a las que podemos calcular la dimensión de Gelfand–Kirillov. Dado que la definición que hicimos anteriormente de la función de Hilbert implica el uso del grado, podemos reformularla utilizando ahora la aplicación $\langle \mathfrak{a}, \omega \rangle$. Sin embargo, aunque la función de Hilbert cambie, el crecimiento sigue siendo el mismo:

[5.37]. Proposición. *Sea $E \subseteq \mathbb{N}^{p,n}$ un subconjunto estable. Sea la función*

$$HF_E^{\omega}(n) = \mathrm{card}\{\mathfrak{a} \in \mathbb{N}^{p,n} \setminus E \mid \langle \mathfrak{a}, \omega \rangle \leq n\}$$

Entonces $\gamma(HF_E^{\omega}) = \gamma(HF_E^{\omega'})$ para cualesquiera $\omega, \omega' \in (\mathbb{R}^+)^p$.

Demostración. Sea $h \in \mathbb{N}$ tal que $h\omega_i \geq 1$ para todo $i = 1, \ldots, p$. Si $\langle \mathfrak{a}, \omega \rangle \leq n$ entonces $\langle \mathfrak{a}, h\omega \rangle \leq hn$. Además, $|\mathfrak{a}| \leq \langle \mathfrak{a}, h\omega \rangle$. Por otra parte sea $k = \max\{\omega'_1, \ldots, \omega'_p\}$. Entonces $\langle \mathfrak{a}, \omega' \rangle \leq k|\mathfrak{a}| \leq khn$. Hemos demostrado que si $\langle \mathfrak{a}, \omega \rangle \leq n$ entonces $\langle \mathfrak{a}, \omega' \rangle \leq khn$, de donde $F_E^{\omega}(n) \leq F_E^{\omega'}(khn)$. El resultado es pues consecuencia de [5.15]. □

[5.38]. Corolario. *Si $E \subseteq \mathbb{N}^{p,n}$, $\omega \in (\mathbb{R}^+)^p$ y HF_E^{ω} es la función definida en [5.37] entonces $\gamma(HF_E^{\omega}) = \dim(E)$.*

Demostración. Tomando $\omega' = (1, \ldots, 1)$, el resultado es consecuencia inmediata de [5.37] y [5.12]. □

En lo que sigue, R es una $\mathbb{k}$–álgebra de tipo PBW con respecto a un orden $\leq$ casi graduado con pesos ω. El orden TOP se representa por $\preceq$ y $L \subseteq R^n$ es un R–submódulo a izquierda. El objetivo es conectar la dimensión $\mathrm{GKdim}(R^n/L)$ con $\dim(\mathrm{Exp}(L))$. V y U son los espacios generadores usuales.

[5.39]. Lema. *En las condiciones anteriores*

$$\mathrm{card}\{\mathfrak{a} \in \mathbb{N}^{p,n} \setminus \mathrm{Exp}(L) \mid \langle \mathfrak{a}, \omega \rangle \leq k\} = \dim_{\mathbb{k}}\{\mathbf{f} + L \mid \langle \exp(\mathbf{f}), \omega \rangle \leq k\}$$

Demostración. La demostración es esencialmente idéntica a [5.28]. Sea $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ una base de Gröbner para L. Sea $\mathbf{f} + L$ tal que $\langle \exp(\mathbf{f}), \omega \rangle \leq k$. Por el teorema [3.9] $\mathbf{f} = q_1\mathbf{g}_1 + \cdots + q_t\mathbf{g}_t + \mathbf{r}$ donde $\exp(\mathbf{r}) \preceq \exp(\mathbf{f})$ y $\mathcal{N}(\mathbf{r}) \cap \mathrm{Exp}(L) = \varnothing$, es decir,

$$\mathbf{r} = \sum_{\mathfrak{a} \notin \mathrm{Exp}(L)} c_{\mathfrak{a}}\mathbf{u}_{\mathfrak{a}}.$$

Dado que $\mathfrak{a} \preceq \exp(\mathbf{r})$ para todo $\mathfrak{a} \in \mathcal{N}(\mathbf{r})$ y que el orden es casi graduado podemos comprobar que $\langle \mathfrak{a}, \omega \rangle \leq k$, luego

$$\mathbf{r} = \sum_{\substack{\mathfrak{a} \notin \mathrm{Exp}(L) \\ \langle \mathfrak{a}, \omega \rangle \leq k}} c_{\mathfrak{a}}\mathbf{u}_{\mathfrak{a}}.$$

Por otra parte, si $\mathfrak{a} \notin \mathrm{Exp}(L)$ entonces $\mathbf{u}_{\mathfrak{a}} \notin L$. Hemos demostrado que $\{\mathbf{u}_{\mathfrak{a}} + L \mid \langle \mathfrak{a}, \omega \rangle \leq k, \mathfrak{a} \notin \mathrm{Exp}(L)\}$ es un sistema de generadores de $\{\mathbf{f} + L \mid \langle \exp(\mathbf{f}), \omega \rangle \leq k\}$. Para ver la independencia lineal supongamos que

$$0 = \sum_{\substack{\mathfrak{a} \notin \mathrm{Exp}(L) \\ \langle \mathfrak{a}, \omega \rangle \leq k}} c_{\mathfrak{a}}(\mathbf{u}_{\mathfrak{a}} + L).$$

Entonces $\mathbf{r} = \sum_{\mathfrak{a} \notin \mathrm{Exp}(L)} c_{\mathfrak{a}}\mathbf{u}_{\mathfrak{a}} \in L$, donde además $\mathcal{N}(\mathbf{r}) \cap \mathrm{Exp}(L) = \varnothing$. Por [3.9] y [3.11.2]. tenemos que $\mathbf{r} = \mathrm{lres}(\mathbf{r}, G) = 0$, por lo que $c_{\mathfrak{a}} = 0$. La independencia lineal queda así demostrada. □

Nos queda por último comparar los $\Bbbk$–espacios vectoriales V^kU y $\{\mathbf{f}+L \mid \langle \exp(\mathbf{f}), \omega\rangle \leq k\}$ para calcular la dimensión de Gelfand–Kirillov de R^n/L a través de la dimensión de $\mathrm{Exp}(L)$.

[5.40]. Lema. *Sea* $w = \max\{\omega_1, \ldots, \omega_p\}$. *Entonces*

$$V^kU \subseteq \{\mathbf{f}+L \mid \langle \exp(\mathbf{f}), \omega\rangle \leq wk\}$$

Demostración. Sea $\mathbf{f}+L \in V^kU$. Entonces $\mathbf{f} = \sum_{i=1}^n f_i\mathbf{e}_i + L$ con $f_i \in V^k$. Razonamos por inducción sobre k. Si $k=1$ entonces para cada i, $f_i = c_0 + c_1u_{\epsilon_1} + \cdots + c_pu_{\epsilon_p}$, de donde $\exp(\mathbf{f}) = (\epsilon_j, i)$ para ciertos $i \in \{1,\ldots,n\}$ y $j \in \{1,\ldots,p\}$. Pero $\langle(\epsilon_j,i),\omega\rangle = \omega_j \leq w$, de donde se obtiene el caso $k=1$. Supongamos el resultado cierto para naturales menores que k. Existe $j_0 \in \{1,\ldots,n\}$ tal que $\exp(\mathbf{f}) = \exp(f_{j_0}\mathbf{e}_{j_0}+L) = (\exp(f_{j_0}), j_0)$. Dado que $f_{j_0} \in V^k$, tenemos que $f_{j_0} = g_0 + \sum_{i=1}^p u_{\epsilon_i}g_i$, con $g_i \in V^{k-1}$. Existe un índice $i_0 \in \{1,\ldots,p\}$ tal que $\exp(f_{j_0}) \leq \epsilon_{i_0} + \exp(g_{i_0})$, o $\exp(f_{j_0}) \leq \exp(g_0)$. En el segundo caso, por ser el orden casi graduado $\langle\exp(\mathbf{f}),\omega\rangle = \langle\exp(f_{j_0}),\omega\rangle \leq \langle\exp(g_0),\omega\rangle$, y en el primer caso $\langle\exp(\mathbf{f}),\omega\rangle = \langle\exp(f_{j_0}),\omega\rangle \leq \langle\epsilon_{i_0}+\exp(g_{i_0}),\omega\rangle = \langle\epsilon_{i_0},\omega\rangle + \langle\exp(g_{i_0}),\omega\rangle$. Por hipótesis de inducción, $\langle\epsilon_i,\omega\rangle \leq w$ y $\langle\exp(g),\omega\rangle \leq w(k-1)$ para todo $g \in V^{k-1}$, de donde se concluye que $\langle\exp(f_{j_0}),\omega\rangle \leq w(k-1) < wk$ o $\langle\exp(f_{j_0}),\omega\rangle \leq w + w(k-1) = wk$, como queríamos. □

[5.41]. Lema. *Existe* $a \in \mathbb{N}$ *tal que*

$$\{\mathbf{f}+L \mid \langle\exp(\mathbf{f}),\omega\rangle \leq k\} \subseteq V^{ak}U$$

Demostración. Sea $h \in \mathbb{N}$ tal que $h\omega_i \geq 1$ para todo i. Entonces la igualdad

$$\{\mathbf{f}+L \mid \langle\exp(\mathbf{f}),\omega\rangle \leq k\} = \{\mathbf{f}+L \mid \langle\exp(\mathbf{f}),h\omega\rangle \leq hk\}$$

nos permite limitarnos a comprobar que

$$\{\mathbf{f}+L \mid \langle\exp(\mathbf{f}),h\omega\rangle \leq k\} \subseteq V^{bk}U \tag{5.3}$$

para un cierto $b \in \mathbb{N}$. Dado que el conjnto de los $\alpha \in \mathbb{N}^p$ tales que $\langle\alpha,h\omega\rangle \leq 1$ es finito, veamos que $b \in \mathbb{N}$ es cualquier natural que satisfaga $\langle\alpha,h\omega\rangle \leq 1$ implica $u_\alpha \in V^b$. Demostramos 5.3 por inducción sobre k. Si $k=1$ y $\langle\exp(\mathbf{f}),h\omega\rangle \leq 1$, dado que el orden es casi graduado tenemos que $\mathbf{f} = \sum c_{\alpha,j}u_\alpha\mathbf{e}_j$ con $\langle\alpha,h\omega\rangle \leq 1$. Por la elección de b obtenemos que $\mathbf{f}+L \in V^{bk}U$.

Supongamos el resultado cierto para naturales menores que k y supongamos que $\langle\mathbf{f},h\omega\rangle \leq k$. Pongamos $\exp(\mathbf{f}) = (\alpha,i)$. Demostramos que $\mathbf{f}+L \in V^{bk}U$ por inducción sobre $\exp(\mathbf{f})$. Si $\exp(\mathbf{f}) = (\mathbf{0},i)$ entonces

$\mathbf{f} + L = \sum_{j=1}^{i} c_j \mathbf{e}_j + L \in U \subseteq V^m U$ para todo $m \in \mathbb{N}$. Pongamos $\alpha > \mathbf{0}$, con lo que $\alpha = \alpha' + \epsilon_j$ para un cierto j. Como $\langle \alpha, h\omega \rangle = \langle \alpha', h\omega \rangle + \langle \epsilon_j, h\omega \rangle$ y dado que $h\omega_j \geq 1$ tenemos que $\langle \alpha', h\omega \rangle \leq k - 1$. La inducción sobre k demuestra que $u_{\alpha'} \mathbf{e}_i + L \in V^{b(k-1)} U$.

Por otra parte $\mathbf{f} = c u_\alpha \mathbf{e}_j + \mathbf{f}'$, con $\exp(\mathbf{f}') \prec \exp(\mathbf{f})$. Además $u_\alpha = u_{\epsilon_j + \alpha'} = q u_{\epsilon_j} u_{\alpha'} + g$ con $\exp(g) < \alpha$, por lo que $\exp(g\mathbf{e}_i) \prec \exp(\mathbf{f})$. Resumiendo $\mathbf{f} = c u_{\epsilon_j} u_{\alpha'} \mathbf{e}_i + \mathbf{g}'$ con $\exp(\mathbf{g}') \prec \exp(\mathbf{f})$. Por ser el orden casi graduado tenemos que $\langle \exp(\mathbf{g}'), \omega \rangle \leq \langle \exp(\mathbf{f}), \omega \rangle$ y multiplicando por h tenemos que $\langle \exp(\mathbf{g}'), h\omega \rangle \leq \langle \exp(\mathbf{f}), h\omega \rangle$. La inducción sobre $\exp(\mathbf{f})$ implica que $\mathbf{g}' + L \in V^{bk} U$. Esta última pertenencia, junto con el hecho de que $u_{\alpha'} \mathbf{e}_i + L \in V^{b(k-1)} U$ y que $u_{\epsilon_i} \in V \subseteq V^b$, nos demuestra que $\mathbf{f} + L \in V^{bk} U$. □

[5.42]. Teorema. *Si R es un álgebra de tipo PBW con respecto a un orden casi graduado sobre $\mathbb{N}^p$ y $L \subseteq R^n$ es un R–submódulo a izquierda, entonces* $\mathrm{GKdim}(R^n/L) = \dim(\mathrm{Exp}(L))$.

Demostración. Por definición, $\mathrm{GKdim}(R^n/L) = \gamma(\dim_{\Bbbk}(V^k U))$, y por los lemas [5.40], [5.41] y [5.15] tenemos que

$$\gamma(\dim_{\Bbbk}(V^k U)) = \gamma(\dim_{\Bbbk}(\{\mathbf{f} + L \mid \langle \exp(\mathbf{f}), \omega \rangle \leq k\})).$$

El resultado es consecuencia de [5.38] y [5.39]. □

[5.43]. El corolario [5.29] y el teorema [5.42] nos permiten dar un álgoritmo para calcular la dimensión de Gelfand–Kirillov de R^n/L cuando R es un álgebra de tipo PBW con respecto a un orden casi graduado. Suponiendo que tenemos un álgebra de tipo PBW R en dichas condiciones con base $\mathcal{B} = \{u_\alpha \mid \alpha \in \mathbb{N}^p\}$, damos una descripción del algoritmo:

Entrada: Un conjunto de generadores de $L \subseteq R^n$.

Salida: Dimensión de Gelfand–Kirillov de R^n/L.

Paso 1. Calculamos una base de Gröbner para L mediante [3.15]. La llamamos $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$.

Paso 2. Ponemos $i = 1$.

Paso 3. Llamamos $E_i = \{\alpha \in \mathbb{N}^p \mid (\alpha, i) = \exp(\mathbf{g}_j) \text{ para algún } j = 1, \ldots, t\}$.

Paso 4. Si $E_i = \varnothing$ entonces $d_i = p$. Si $\mathbf{0} \in E_i$ entonces $d_i = 0$. Ir al paso 7. Si no, $j = 1$

Paso 5. Si existe $\sigma \subseteq \{1, \ldots, p\}$ con $\mathrm{card}(\sigma) = j$ tal que $\sigma \cap \mathrm{supp}(\alpha) \neq \varnothing$ para todo $\alpha \in E_i$, entonces $d_i = p - j$ y vamos al paso 7.

Paso 6. Ponemos $j = j + 1$ y vamos a 5.

Paso 7. Si $i = n$ vamos al paso 8. Si no, $i = i + 1$ y vamos al paso 3.

Paso 8. Ponemos $d = \max\{d_1, \ldots, d_n\}$, y d es la dimensión de Gelfand–Kirillov de R^n/L.

[5.44]. Ejemplo. Sea $R = \Bbbk[x_1][x_2; \sigma_2, \delta_2] \ldots [x_p; \sigma_p, \delta_p]$ una extensión iterada de Ore $\Bbbk$ y supongamos que $\sigma_j(x_i) = q_{ij}x_i$, para cualesquiera $0 \leq i < j \leq p$, donde $q_{ij} \in \Bbbk^\times$. Como observamos en [2.11] $\mathcal{B} = \{x_1^{\alpha_1} \cdots x_p^{\alpha_p} \mid \alpha \in \mathbb{N}^p\}$ es una $\Bbbk$–base de R. Vamos a construir un elemento $\omega = (\omega_1, \ldots, \omega_p)$ que nos proporcione un orden casi graduado sobre $\mathbb{N}^p$ que dote a R de estructura de PBW álgebra. Pongamos $\omega_1 = 1$ y sea w_{12} el grado en x_1 del polinomio $\delta_2(x_1)$. Pongamos $\omega_2 = \max\{1, \omega_{12}\}$. Una vez definidos $\omega_1, \ldots, \omega_{j-1}$ para $j \geq 2$, para cada $k = 1, \ldots, j-1$, ponemos $\omega_{kj} = \max\{\alpha_1\omega_1 + \cdots + \alpha_{j-1}\omega_{j-1} \mid \alpha \in \mathcal{N}(\delta_j(x_k))\}$ y llamamos $\omega_j = \max\{1, \omega_{kj} - \omega_i \mid 1 \leq i, k \leq j-1\}$. Llamando $\omega = (\omega_1, \ldots, \omega_p)$, consideramos en $\mathbb{N}^p$ el orden admisible definido en [1.19] a partir de el orden lexicográfico con $\epsilon_1 < \cdots < \epsilon_p$ mediante ω, y lo notamos $\leq_\omega$. Para ver R es una PBW álgebra respecto de $\leq_\omega$ vamos a aplicar [2.7]. Si $0 \leq i < j \leq p$, $\langle \epsilon_i + \epsilon_j, \omega \rangle = \omega_i + \omega_j \geq \omega_{ij} \geq \langle \alpha, \omega \rangle$ para todo $\alpha \in \mathcal{N}(\delta_j(x_i))$. Además, para todo $\alpha \in \mathcal{N}(\delta_j(x_i))$ con $i < j$, $\alpha_j = \alpha_{j+1} = \alpha_p = 0$, por lo que $\alpha <_\omega \epsilon_i + \epsilon_j$, es decir,

$$x_j x_i = q_{ij} x_i x_j + \sum_{\alpha <_\omega \epsilon_i + \epsilon_j} d_\alpha X^\alpha.$$

Entre los ejemplos que podemos cubrir on las extensiones iteradas de Ore tenemos $H(p, \lambda)$ definida en [3], la cual incluye el álgebra de coordenadas cuánticas de las matrices $M_n(\Bbbk)$, También el álgebra de Weyl cuántica multiparamétrica $R = A_n^{Q,\Gamma}(\Bbbk)$ introducida en [56] (véase también [30]). También se cubren las álgebras de operadores diferenciales de [75].

Referencias

[1] W. W. Adams and Ph. Loustaunau. *An introduction to Gröbner Bases.* Number 3 in Graduate Studies in Mathematics. American Mathematical Society, 1994.

[2] J. Apel and W. Lassner. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *J. Symb. Comput.*, 6:361–360, 1988.

[3] M. Artin, W. Schelter, and J. Tate. Quantum deformations of GL_n. *Commun. Pur. Appl. Math.*, 44:879–895, 1991.

[4] Thomas Becker and Volker Weispfenning. *Gröbner bases. A computational approach to commutative algebra.* Springer–Verlag, 1993.

[5] Roland Berger. The quantum Poincaré–Birkhoff–Witt theorem. *Commun. Math. Phys.*, 143:215–234, 1992.

[6] J.E. Bjork. Filtered noetherian rings, noetherian rings and their applications. *Math. Surveys and monographs*, pages 59–97, 1987. Amer. Math. Soc.

[7] W. Borho, P. Gabriel, and R. Rentschler. *Primideale in Einhüllenden auflösbarer Lie–Algebren.* Lecture Notes in Mathematics, 357. Springer–Verlag, 1973.

[8] B. Buchberger. Ein algorithmisches Kriterium fur die lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Mathematicae*, 4:374–383, 1970.

[9] J. L. Bueso, F. J. Castro, and P. Jara. The effective computation of the Gelfand-Kirillov dimension. *P. Edinburgh Math. Soc.*, pages 111–117, 1997.

[10] José L. Bueso, F. J. Castro, J. Gómez Torrecillas, and F. J. Lobillo. Primality test in iterated ore extensions. submitted to JSC, 1997.

[11] José. L. Bueso, F. J. Castro, J. Gómez Torrecillas, and F. J. Lobillo. An introduction to effective calculus in quantum groups. In S. Caenepeel and A. Verschoren, editors, *Algebraic and Geometric Methods in Ring Theory.*, pages 55–83. Marcel Dekker, 1998.

[12] José L. Bueso, Francisco Castro, José Gómez Torrecillas, and Francisco J. Lobillo. Computing the Gelfand–Kirillov dimension. *SAC Newsletter*, 1:39–52, December 1996.

[13] José Luis Bueso, Pascual Jara, and Alain Verschoren. *Compatibility, stability and sheaves.* Marcel Dekker, 1995.

[14] F. J. Castro. *Théorème de division pour les opérateurs différentiels et calcul des multiplicités.* PhD thesis, Univ. Paris VII, Oct-1984.

[15] Francisco Castro Jiménez. Calculs effectifs pour les idéaux d'opérateurs différentiels. In *Travaux en Cours. Géométrie Algébrique et Applications, Tome III*, pages 1–19. Hermann (Paris), 1987.

[16] W. Chin and I. M. Musson. Multiparameter quantum enveloping algebras. *J. Pure Appl. Algebra.*, 107:171–191, 1996.

[17] P. M. Cohn. *Algebra*, volume 2. John Wiley and Sons., 1977.

[18] A. Connes. *Geometrie non commutative.* InterEditions, 1990.

[19] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Springer–Verlag, 1992.

[20] C. De Concini and C. Procesi. *Quantum Groups.* Number 1565 in Lecture Notes in Math. Springer, 1993.

[21] Jacques Dixmier. *Enveloping Algebras.* Number 11 in Graduate Studies in Mathematics. American Mathematical Society, 1996. The 1996 Printing of the 1977 English Translation.

[22] V. G. Drinfeld. Quantum groups. In *Proc. Int. Cong. Math., Berkeley/Calif.*, volume 1, pages 798–820., 1986.

[23] L. Feddeev, N. Reshetikhin, and Takhtajan. Quantization of Lie groups and Lie algebras. 1989.

[24] André Galligo. Algorithmes de calcul de base standards. Preprint., 1983.

[25] André Galligo. Some algorithmicquestions on ideals of differential operators. In *EUROCAL'85, vol. 2, Linz*, number 204 in Lecture Notes in Comput. Sci., pages 413–421, 1985.

[26] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, 6(2–3):149–167, 1988.

[27] J. Gómez Torrecilas, P. Jara, and L. Merino. Locally finite representations of algebras. *Commun. Algebra*, to appear.

[28] José Gómez Torrecillas. Gelfand–Kirillov dimension of multi-filtered algebras. *P. Edinburgh Math. Soc*, to appear.

[29] K. R. Goodearl. Prime ideals in skew polynomial rings and quantized Weyl algebras. *J. Algebra*, 150:324–377, 1992.

[30] K. R. Goodearl and T. H. Lenagan. Catenarity in quantum algebras. *J. Pure Appl. Algebra*, 111:123–142, 1996.

[31] K. R. Goodearl and E. S. Letzter. Prime factor algebras of the coordinate ring of quantum matrices. *Proc. Amer. Math. Soc.*, 121:1017–1025, 1994.

[32] K. R. Goodearl and E. S. Letzter. Prime ideals in skew and q–skew polynomial rings. *Mem. Am. Math. Soc.*, 109, May 1994.

[33] K. R. Goodearl and R. B. Warfield Jr. *An Introduction to Noncommutative Noetherian Rings.* London Mathematical Society Student Texts, 16. Cambridge University Press, 1989.

[34] T. Hayashi. Q–analogues of Clifford and Weyl algebras. spinor and oscillator representations of quantum enveloping algebras. *Comm. Math. Phys.*, 127:129–144, 1990.

[35] A. V. Jategaonkar. *Localization in Noetherian Rings.* London Mathematical Society Lecture Note Series, 98. Cambridge University Press, 1986.

[36] M. Jimbo. A q–difference analog of $u(g)$ and the Yang-Baxter equation. *Lett. Math. Phys.*, 10:63–69, 1985.

[37] M. Jimbo. A q–analogue of $U(\mathfrak{gl}(N+1))$, Hecke algebra, and the Yang–Baxter equation. *Lett. Math. Phys.*, 11:247–252, 1986.

[38] A. Joseph. *Quantum Groups and their primitive ideals.* Springer, 1995.

[39] A. Kandri-Rody and V. Weispfenning. Non–commutative Gröbner bases in algebras of solvable type. *J. Symb. Comput.*, 9/1:1–26, 1990.

[40] C. Kassel. *Quantum Groups.* Springer, 1995.

[41] G.R. Krause and T.H. Lenagan. *Growth of algebras and Gelfand–Kirillov dimension*, volume 116 of *Research Notes in Mathematics.* Pitman Pub. Inc., London, 1985.

[42] Heinz Kredel. *Solvable Polynomial Rings.* PhD thesis, Universität Passau, 1992.

[43] T. Y. Lam. *A first Course in Noncommutative Rings.* Graduate Texts in Mathematics, 131. Springer–Verlag, 1991.

[44] M. Lejeune-Jalabert. Effectivité des calculs polynomiaux, 1984–85. Cours de D.E.A., Univ. Grenoble.

[45] A. Leroy and J. Matczuk. Prime ideals in Ore extensions. *Comm. Algebra*, 19(7):1893–1907, 1991.

[46] A. Leroy and J. Matczuk. The extended centroid and X–inner automorphisms of Ore extensions. *J. Algebra*, 145:143–177, 1992.

[47] T. Levasseur. Some properties of noncommutative regular graded rings. *Glasgow Math. J.*, 1992.

[48] T. Levasseur. Complexe bidualisant en algebre non commutative. In *Seminaire Dubreil-Malliavin 1983-84*, number 1146 in Lect. Notes in Math., pages 270–287. Springer, 1995.

[49] M. Lorentz. Gelfand–Kirillov dimension and Poincaré series. In *Cuadernos de Algebra*, volume 7. Universidad de Granada, 1988.

[50] G. Lusztig. Canonical bases arising from quantized enveloping algebras. *J. Amer. Math. Soc.*, 3:447–498, 1990.

[51] G. Lusztig. Finite dimensional Hopf algebras arising from quantized enveloping algebras. *J. Am. Math. Soc.*, 3:447–498, 1990.

[52] G. Lusztig. Quantum groups at roots of 1. *Geometriae Dedicata*, 35:89–114, 1990.

[53] G. Lusztig. *Introduction to Quantum groups*, volume 110 of *Progr. Math.* Birkhauser, 1993.

[54] S. Majid. Physics for algebraists: non-commutative and non-cocommutative Hopf algebras by a bicrossproduct construction. *J. Algebra*, 130:17–64, 1990.

[55] S. Majid. Quasi-triangular Hopf algebras and Yang-Baxter equations. *Intern. J. Modern Phys. A*, 5, 1990.

[56] G. Maltsiniotis. Calcul différentiel quantique. 1992.

[57] Y. I. Manin. Quantum gropus and non–commutative geometry. Technical report, Pub. Centre Rech. Math., Univ. Montréal., 1988.

[58] J. McConnell and J. C. Robson. *Noncommutative noetherian rings.* Wiley Interscience, New York, 1987.

[59] J. C. McConnell. Quantum groups, filtered rings and Gelfand–Kirillov dimension. *Lecture Notes in Mathematics*, 1448:139–147, 1991.

[60] J.C. McConnell and J.T. Stafford. Gelfand-Kirillov dimension and associated graded modules. *J. Algebra*, 125:197–214, 1989.

[61] F. Mora. Gröbner bases for non–commutative polynomials rings. *AAECC-3. Lecture Notes in Computer Science*, 229:353–362, 1985.

[62] T. Mora. Seven variations on standard bases. Preprint, 1988.

[63] T. Mora. Gröbner bases in non–commutative algebras. *ISSAC'88. Lecture Notes in Computer Science*, 358:150–161, 1989.

[64] Teo Mora. Standard bases and non-noetherianity: non-commutative polynomial rings. In *Proc. AAECC4*, volume 307 of *Lecture Notes in Comput. Sci.*, pages 98–109, 1988.

[65] Teo Mora. An introduction to commutative and non–commutative Gröbner bases. *Theoretical Computer Science*, 134:131–173, 1994.

[66] Constantin Nastasescu and Fred Van Oystaeyen. *Graded Ring Theory.* North-Holland Mathematical Library, 1982.

[67] Constantin Năstăsescu and Fred van Oystaeyen. *Dimensions of Ring Theory.* D. Reidel Publishing Company, 1987.

[68] O. Ore. Theory of non–commutative polynomials. *Annals of Mathematics*, 34:480–508, 1933.

[69] P. Podles. Quantum spheres. *Lett. Math. Phys.*, 14:193–202, 1987.

[70] C. M. Ringel. PBW–bases of quantum groups. *J. reine angew. Math.*, 470:51–88, 1996.

[71] A. L. Rosenberg. *Noncommutative Algebraic Geometry and Representations of Quantized Algebras.* Number 330 in Mathematics and Its Applications. Kluver Academic Publishers, 1995.

[72] Joseph J. Rotman. *An introduction to homological algebra.* Academic Press, Inc., 1979.

[73] J. Shapiro. Critical series over stable noetherian rings with applications to prime principal right ideal rings. *Commun. Algebra*, 13:543–565, 1985.

[74] G. Sigurdsson. Differential operator rings whose prime factor have bounded Goldie dimension. *Arch. Math. (Basel)*, 42:348–353, 1984.

[75] G. Sigurdsson. Ideals in universal enveloping algebras of solvable Lie algebras. *Comm. Algebra*, 15:813–826, 1987.

[76] S. P. Smith. Quantum groups: An introduction and survey for ring theorists. In S. Montgomery and L. Small, editors, *Noncommutative Rings*, pages 131–178. MSRI Publ. 24, 1992.

[77] Bo Stenström. *Rings of Quotients.* Springer Verlag, 1975.

[78] Levasseur T. and J. T. Stafford. The quantum coordinate ring of special linear group. *J. Pure Appl. Algebra*, 86:181–186, 1993.

[79] P. Tauvel. Sur la dimension de Gelfand-Kirillov. *Comm. Algebra*, 10:939–963, 1982.

[80] Wolmer V. Vasconcelos. Computational methods in commutative algebra and algebraic geometry. Technical report, Department of Mathematics, Rutgers University, 1996.

[81] S. L. Woronowicz. Twisted $SU(2)$ group. an example of a noncommutative diferential calculus. *Publ. RIMS*, 23:117–191, 1987.

[82] H. Yamane. A Poincaré–Birkoff–Witt theorem for quantized universal enveloping algebras of type A_N. *Publ. RIMS Kyoto Univ.*, 25:503–520, 1989.

[83] O. Zariski and P. Samuel. *Conmutative Algebra, Volume I*, volume 28 of *Graduate Text in Mathematics.* Springer–Verlag, 1975.