NOTAS DE TRABAJO

13. ÁLGEBRAS CUADRÁTICAS

Pascual Jara Martínez

Departamento de Álgebra
Universidad de Granada

Granada, 1996/98

Primera redacción: Febrero 1996
Segunda redacción: Diciembre 1998 .

Pascual Jara
Departamento de Álgebra
Facultad de Ciencias
Universidad de Granada
18071–Granada. ESPAÑA

Partially supported by DGICYT(PB94–0791), (PB97–0837)

La matemática nació del juego, y el juego es la vida del niño. El niño nace matemático y suele dejar de serlo en cuanto se hace hombre. Y si no deja de serlo es que sigue siendo niño.
M. de Unamuno

Introducción.

El uso de bases estándar ó bases de Groebner en anillos conmutativos ha sido muy fructífero en los últimos años en Álgebra Conmutativa y por consiguiente en Geometría Algebraica y Teoría de Números. En esta monografía vamos a desarrollar una teoría no conmutativa de bases de Groebner con aplicaciones al estudio de la estructura de álgebras no necesariamente conmutativas.

Esta teoría puede ser desarrollada en un contexto no conmutativo general. Sin embargo, de cara a aplicaciones concretas, que estamos desarrollando simultáneamente, es necesario un estudio en detalle de las bases de Groebner: su definición y propiedades, en los que vamos a llamar *álgebras cuadráticas*, esto es, álgebras finitamente presentadas con un sistema de generadores $\{x_i\colon\ i = 1, \ldots, n\}$, verificando relaciones de conmutación del siguiente tipo:

$$x_j x_i = q_{i,j} x_i x_j + r_{i,j}(x),$$

siendo $q_{i,j} \in K^*$, $r_{i,j}(x) \in K[x_1, \ldots, x_n]$ un polinomio de grado menor o igual que 2. En el desarrollo que vamos a realizar necesitaremos imponer ciertas condiciones a los polinomios $r_{i,j}(x)$ de cara a obtener propiedades de interés.

Las álgebras cuadráticas recogen una gran cantidad de ejemplos recientemente estudiados; citaremos algunas referencias a las mismas: [3], [5] [8] [9] [10] [11] [14] [16] [18] [20]

Estos ejemplos son estudiados de forma unificada por la teoría introducida en esta monografía. Esta teoría además presenta una forma nueva de atacar los problemas en los ejemplos mencionados; en contraposición con las técnicas empleadas hasta el presente (fundamentalmente técnicas combinatorias, que dependen estrechamente de cada uno de los ejemplos que se está estudiando). Las técnicas introducidas en esta

monografía ofrecen además una sistematización que simplifica enormemente el estudio de los problemas abordados.

Es necesario destacar que aunque la presente memoria presenta una exposición en álgebra no conmutativa de resultados y técnicas conmutativas y que por lo tanto podría ser considerada como un ejercicio estilístico; resulta que estas técnicas han permitido, en el caso no conmutativo, obtener nuevos resultados (incluso resultados teóricos) cuya demostración, por otros métodos no ha sido posible hasta el momento. Esto pone de manifiesto que la teoría de bases de Groebner en un contexto no conmutativo puede suponer un nuevo impulso al estudio de álgebras no necesariamente conmutativas.

Terminamos señalando que el objetivo fundamental de esta monografía es el de hacer una exposición de la teoría de bases de Groebner en un contexto no conmutativo, que, al fijar la notación, sirva de referencia para posteriores trabajos sobre este tema.

Este trabajo está dividido en cinco capítulos. En los dos primeros se estudian las relaciones de orden y se muestra la forma de construir relaciones de orden compatibles con estructuras algebraicas; se enuncian y prueban los resultados fundamentales que serán de aplicación en el resto de la teoría.

El capítulo tres se dedica a estudiar bajo qué condiciones las álgebras base de nuestro estudio tienen una base, como espacio vectorial, formada por términos en un cierto orden; esta condición permite la extensión de la construcción que en álgebras envolventes de álgebras de Lie prueba el teorema de Poincaré–Birkhoff–Witt. Para probarla hemos tenidos que introducir un nuevo índice que mida el desorden de un término.

Los dos últimos capítulos se dedican a la aplicación de métodos elementales/computacionales a estas álgebras; fundamentalmente introducimos las bases de Groebner; damos criterios para su existencia y mostramos algunas de las aplicaciones de la existencia de bases de Groebner, fundamentalmente en la aritmética de ideales y en el estudio de la dimensión.

Índice General

P. Jara

Capítulo 1

Relaciones de orden.

1. Relaciones en un conjunto.

Sea X un conjunto no vacío. Una *relación* en X es un subconjunto $\mathcal{R} \subseteq X \times X$. Para indicar que el par (a, b) pertenece a $\mathcal{R}$, escribimos $a\,\mathcal{R}\,b$.

Propiedades que puede verificar una relación.

Propiedad reflexiva. Para cada $a \in X$ se tiene $a\,\mathcal{R}\,a$.

Llamamos $\Delta(X) = \{(a, a) \in X \times X\colon\ a \in X\}$. Es claro que $\mathcal{R}$ verifica la propiedad reflexiva si y sólo si $\Delta(X) \subseteq \mathcal{R}$.

Propiedad simétrica. Para cada cualesquiera elementos $a,\ b \in X$, si $a\,\mathcal{R}\,b$, entonces $b\,\mathcal{R}\,a$.

Propiedad antisimétrica. Para cada cualesquiera elementos $a,\ b \in X$, si $a\,\mathcal{R}\,b$ y $b\,\mathcal{R}\,a$, entonces $a = b$.

Si llamamos $\mathcal{R}^{op} = \{(a, b) \in X \times X\colon\ (b, a) \in \mathcal{R}\}$, entonces $\mathcal{R}$ verifica la propiedad simétrica si y sólo si $\mathcal{R} = \mathcal{R}^{op}$ y la propiedad antisimétrica si y sólo si $\mathcal{R} \cap \mathcal{R}^{op} \subseteq \Delta(X)$.

Propiedad transitiva. Para cada cualesquiera elementos $a,\ b,\ c \in X$, si $a\,\mathcal{R}\,b$ y $b\,\mathcal{R}\,c$, entonces $a\,\mathcal{R}\,c$.

Dadas dos relaciones $\mathcal{R}$ y $\mathcal{S}$ en un conjunto X, definimos una nueva relación $\mathcal{R} \circ \mathcal{S}$ mediante:

$$\mathcal{R} \circ \mathcal{S} = \{(a, b) \in X \times X\colon\ \exists x \in X,\ (a, x) \in \mathcal{R},\ (x, b) \in \mathcal{S}\}.$$

Es claro que una relación $\mathcal{R}$ verifica la propiedad transitiva si y sólo si

$\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.

Propiedad total o conexa. Para cualesquiera elementos $a, b \in X$ se verifica: $a \mathcal{R} b$ ó $b \mathcal{R} a$.

Es claro que una relación es total si y sólo si $\mathcal{R} \cup \mathcal{R}^{op} = X \times X$.

Dadas dos relaciones $\mathcal{R}$ y $\mathcal{S}$, decimos que $\mathcal{S}$ *extiende* a $\mathcal{R}$ si $\mathcal{R} \subseteq \mathcal{S}$.

Una relación $\mathcal{R}$ se llama *relación de equivalencia* si verifica la propiedades reflexiva, simétrica y transitiva; es un *preorden* si verifica las propiedades reflexiva y transitiva; es un *orden parcial* si verifica las propiedades reflexiva, antisimétrica y transitiva, y es un *orden total* si es un orden parcial que es total ó conexo.

Si $\preceq$ es un preorden en un conjunto X, definimos una nueva relación, a la que vamos a representar por $\prec$, mediante:

$$a \prec b \text{ si } a \preceq b \text{ y } b \not\preceq a.$$

Es claro que $\prec$ verifica la propiedad transitiva y para cada $a \in X$ se tiene $a \not\prec a$.

Si $\preceq_1$ y $\preceq_2$ son preórdenes en X_1 y X_2 respectivamente, definimos un preorden $\preceq$ en el producto cartesiano $X_1 \times X_2$ mediante:

$$(a_1, a_2) \preceq (b_1, b_2) \text{ si } \begin{cases} a_1 \preceq_1 b_1 \text{ y} \\ a_2 \preceq_2 b_2 \end{cases}$$

Llamamos a $\preceq$ el *preorden producto* de $\preceq_1$ y $\preceq_2$. Esta construcción se puede hacer en el caso en que $\preceq_i$ sean órdenes parciales u órdenes totales, obteniendo en ambos casos que $\preceq$ es un orden parcial en $X_1 \times X_2$

Si $\preceq_1$ y $\preceq_2$ son preórdenes en un conjunto X definimos una nueva relación $\preceq$ en X, mediante

$$a \preceq b \text{ si } \begin{cases} a \preceq_1 b \text{ y} \\ a \preceq_2 b \end{cases}$$

Llamamos a $\preceq$ la *intersección* o *composición* de $\preceq_1$ y $\preceq_2$, ya que considerados con subconjuntos de $X \times X$ se verifica $\preceq = \preceq_1 \cap \preceq_2$. Es claro que $\preceq$ es un preorden, y si $\preceq_1$ y $\preceq_2$ son órdenes parciales, entonces $\preceq$ es un orden parcial.

En cambio, si $\preceq_1$ y $\preceq_2$ son órdenes totales, no necesariamente $\preceq$ es un orden total. Para corregir este problema vamos a hacer la siguiente definición.

Sean $\preceq_1$ y $\preceq_2$ preórdenes en un conjunto X, definimos una nueva relación $\preceq_{1,2}$ en X, mediante:

$$a \preceq_{1,2} b \text{ si } \begin{cases} a \prec_1 b \text{ ó} \\ a \preceq_1 b,\ b \preceq_1 a \text{ y } a \preceq_2 b \end{cases}$$

Llamamos a $\preceq_{1,2}$ la *composición lexicográfica* de $\preceq_1$ y $\preceq_2$. Es claro que $\preceq_{1,2}$ es un preorden, y si $\preceq_1$, $\preceq_2$ son órdenes parciales, respectivamente totales, entonces $\preceq_{1,2}$ es un orden parcial, respectivamente total.

2. Elementos asociados a una relación de orden.

Consideramos en un conjunto no vacío X un preorden $\preceq$. Si $\varnothing \neq Y \subseteq X$ es un subconjunto, un elemento $y_0 \in Y$ se llama *minimal* en Y si no existe un elemento $y \in Y$ tal que $y \prec y_0$, y se llama *maximal* en Y si no existe $y \in Y$ tal que $y_0 \prec y$.

Un preorden $\preceq$ se llama *artiniano* si cada subconjunto $\varnothing \neq Y \subseteq X$ tiene un elemento minimal, y se llama *noetheriano* si cada subconjunto $\varnothing \neq Y \subseteq X$ tiene un elemento maximal.

Sea $\preceq$ un orden parcial en X. Si $\varnothing \neq Y \subseteq X$, un elemento $y_0 \in Y$ se llama el *mínimo* de Y si para cada $y \in Y$ se verifica $y_0 \preceq y$, y se llama un *máximo* si para cada $y \in Y$ se verifica $y \preceq y_0$.

A un orden total artiniano $\preceq$ lo llamamos un *buen orden*. En este caso cada $\varnothing \neq Y \subseteq X$ tiene un único elemento minimal que resulta ser un mínimo.

3. Propiedad de Dickson.

Sea $\preceq$ un preorden. Para un subconjunto $\varnothing \neq Y \subseteq X$ una *base de Dickson* es un subconjunto finito $F \subseteq Y$ verificando que para cada $y \in Y$ existe $f \in F$ tal que $f \preceq y$.

Un preorden $\preceq$ verifica la *propiedad de Dickson*, o es un *preorden de Dickson*, si cada subconjunto $\varnothing \neq Y \subseteq X$ tiene una base de Dickson.

(3.1) Lema.
Cada preorden total artiniano es un preorden de Dickson.

DEMOSTRACIÓN. Sea $\varnothing \neq Y \subseteq X$, entonces Y tiene un elemento minimal, llamémoslo y_0. Vamos a ver que $\{y_0\}$ es una base de Dickson de Y. Sea $y_0 \neq y \in Y$, entonces $y \preceq y_0$ (y por ser y_0 minimal resulta $y_0 = y$), lo que es una contradicción, ó $y_0 \preceq y$. □

(3.2) Proposición.
Todo preorden de Dickson es artiniano.

DEMOSTRACIÓN. Dado $\varnothing \neq Y \subseteq X$, tomamos una base de Dickson $F \subseteq Y$ de Y. Si $f_1 \preceq f_2, f_1, f_2 \in F$, entonces $F \setminus \{f_2\}$ es también una base de Dickson de Y. Como F es un conjunto finito, podemos tomar una base de Dickson que sea minimal entre las bases de Dickson de Y. Llamémosla también F. Si $f \in F$ es un elemento minimal en F, (existe por ser F finito) entonces f es un elemento minimal en Y, y en consecuencia Y tiene elementos minimales. □

(3.3) Teorema.
Sea $\preceq$ un preorden en un conjunto no vacío X. Los siguientes enunciados son equivalentes:

(a) $\preceq$ es un preorden de Dickson;

(b) Para cualquier sucesión $\{a_n\}_n$ de elementos de X existen índices $i < j$ tales que $a_i \preceq a_j$.

DEMOSTRACIÓN. a $\Rightarrow$ b. Dada una sucesión $\{a_n\}_n$, llamamos $Y = \{a_n\colon\ n \in \mathbb{N}\}$. Existe F una base de Dickson de Y. Tomamos un índice j verificando que $j > h$ para cada índice h tal que $a_h \in F$. Entonces se verifica que existe un elemento $a_i \in F$, y por lo tanto un índice i, tal que $i < j$ y $a_i \preceq a_j$.
b $\Rightarrow$ a. Consideramos un subconjunto $\varnothing \neq Y \subseteq X$. En el conjunto de los elementos minimales de Y consideramos las clases de equivalencia definida por el preorden. Si el número de clases es finito, tomando un representante de cada clase tenemos una bases de Dickson de Y. Si el número de clases es infinito, entonces construimos una sucesión $\{a_n\}_n$ formada por representantes de las clases. Por la hipótesis existen índices $i < j$ con $a_i \leq a_j$, lo que es una contradicción. □

(3.4) Proposición.
Sea $\preceq$ un preorden de Dickson en un conjunto no vacío X, y sea $\{a_n\}_n$ una sucesión de elementos de X. Entonces existe una subsucesión estrictamente ascendente de números naturales $\{n_i\}_i$ tal que $a_{n_i} \preceq a_{n_j}$ para todo par de índices $i < j$.

DEMOSTRACIÓN. Construimos la sucesión $\{n_i\}_i$ de la siguiente forma. Tomamos $i = 0$; sea $\{b_1, \dots, b_k\}$ una base de Dickson de $\{a_n\colon\ n \in \mathbb{N}\}$. Para cada $1 \leq j \leq k$ definimos

$$B_j = \{n \in \mathbb{N}\colon\ b_j \preceq a_n\}$$

Es claro que $\mathbb{N} = B_1 \cup \cdots \cup B_k$. Entonces uno de los B_j es infinito; supongamos que sea B_j; definimos $n_0 = m$, siendo m un índice verificando $b_j = a_m$.

Si ahora $i > 0$, definimos

$$U_{i-1} = \{a_n\colon\ a_{n_{i-1}} \preceq a_n,\ n_{i-1} < n\}$$

Por la construcción, el conjunto $\{n \in \mathbb{N}\colon\ a_n \in U_{i-1}\}$ es infinito. Tomamos una base de Dickson para U_{i-1}. Podemos encontrar un elemento a_m en esta base tal que $a_m \preceq a_n$ para un número infinito de índices n. Tomamos entonces $n_i = m$.

De esta forma construimos una sucesión $\{n_i\}_i$ verificando las condiciones del enunciado. □

El comportamiento de los preórdenes de Dickson es de interés; veamos a continuación que el producto de preórdenes de Dickson es un preorden de Dickson.

(3.5) Lema.
Sean $\preceq_1$ y $\preceq_2$ preórdenes de Dickson en conjuntos X_1 y X_2 respectivamente, entonces su producto es un preorden de Dickson.

DEMOSTRACIÓN. Sea $\{(a_n, b_n)\}_n$ una sucesión en $X_1 \times X_2$. Existe una sucesión estrictamente ascendente $\{n_i\}_i$ tal que $a_{n_i} \preceq_1 a_{n_j}$ si $i < j$. Se considera ahora la sucesión $\{b_{n_i}\}_i$; existen índices $n_i < n_j$ con $b_{n_i} \preceq_2 b_{n_j}$, y es claro que $(a_{n_i}, b_{n_i}) \preceq (a_{n_j}, b_{n_j})$. Por tanto $\preceq$ es un preorden de Dickson. □

(3.6) Lema.
Sean $\preceq_1$ y $\preceq_2$ preórdenes de Dickson en un conjunto X, entonces su composición y composición lexicográfica son preórdenes de Dickson.

DEMOSTRACIÓN. Hacemos al demostración para la composición lexicográfica, el otro caso es similar. Sea $\{a_n\}_n$ una sucesión en X; existe una sucesión estrictamente ascendente $\{n_i\}_i$ tal que si $i < j$, entonces $a_{n_i} \preceq_1 a_{n_j}$. Si para algún índice i se verifica $a_{n_i} \prec_1 a_{n_{i+1}}$, tenemos el

resultado. En caso contrario $a_{n_j} \preceq_1 a_{n_i}$ si $i < j$. Existe entonces una subsucesión $\{a_{n_h}\}_{n_h}$ tal que $a_{n_k} \preceq_2 a_{n_h}$ si $k < h$, y por tanto $\preceq_{1,2}$ es un preorden de Dickson. □

El siguiente resultado nos proporciona una caracterización de preórdenes de Dickson en términos de preórdenes artinianos.

(3.7) Teorema.
Sea $\preceq$ un preorden de Dickson en un conjunto X y sea $\preceq'$ un preorden extensión de $\preceq$. Entonces $\preceq'$ es un preorden de artiniano. Se tiene además que un preorden $\preceq$ es de Dickson si y sólo si cada preorden extensión de $\preceq$ es artiniano.

DEMOSTRACIÓN. La primera parte es consecuencia de que cada preorden de Dickson es artiniano y cada extensión de un preorden de Dickson es de Dickson.
Para la segunda parte, supongamos que existe una sucesión $\{a_n\}_n$ tal que $a_i \not\preceq a_j$ si $i < j$. Vamos a deducir que existe un preorden $\preceq'$ que extiende a $\preceq$ y que no es artiniano. Definimos $\preceq'$ mediante:

$$a \preceq' b \text{ si } \begin{cases} a \preceq b \text{ ó} \\ \exists i < j \text{ tal que } a \preceq a_j \text{ y } a_i \preceq b \end{cases}$$

Por la hipótesis $\{a_n\}_n$ es una cadena estrictamente $\preceq'$–descendente. Por la definición de $\preceq'$ es claro que $a_j \preceq' a_i$ si $i < j$. Vamos a ver que no se verifica $a_i \preceq' a_j$. Si suponemos que $a_i \preceq' a_j$, entonces existen k, $l \in \mathbb{N}$ tales que $k < l$, $a_i \preceq a_l$ y $a_k \preceq a_j$. Se tiene entonces $l \leq i$ y $j \leq k$, luego $l < k$, lo que es una contradicción. □

Capítulo 2

Órdenes en monoides.

1. Monoides ordenados.

Sea M un monoide, al que vamos a suponer con notación aditiva, y $\preceq$ un orden parcial en M. Decimos que $\preceq$ es un *orden parcial lineal* si para cualesquiera $a, b, c \in M$, tales que $a \preceq b$, se tiene que $a + c \preceq b + c$.

Un par $(M, \preceq)$ formado por un monoide M y un orden parcial lineal $\preceq$ en M se llama un *monoide ordenado*. Si G es un grupo podemos hacer las mismas definiciones y obtenemos el concepto de *grupo ordenado*. Si la relación de orden $\preceq$ es total entonces tenemos los monoides y los grupos *totalmente ordenados*.

(1.1) Ejercicio.
Si $(G, \preceq)$ es un grupo ordenado, para cada par de elementos $a, b \in G$ son equivalentes los siguientes enunciados:
(a) $a \preceq b$;
(b) $0 \preceq b - a$;
(c) $a - b \preceq 0$;
(d) $-b \preceq -a$.

2. Monoides preordenados.

Sea M un monoide y $\preceq$ un *preorden* en M, esto es, una relación en M que verifica las propiedades reflexiva y transitiva.

(2.1) Lema.
Si $\preceq$ es un preorden en M, entonces

$$a \equiv b \text{ si } a \preceq b \text{ y } b \preceq a$$

es una relación de equivalencia en M. En $M/\equiv$ se tiene una relación de orden si definimos

$$[a] \preceq [b] \text{ si } a \preceq b,$$

siendo $[a]$ la clase de equivalencia de a.

Si M es un monoide, decimos que un preorden $\preceq$ en M es *lineal* si para cualesquiera $a, b, c \in M$ tales que $a \preceq b$ se tiene que $a + c \preceq b + c$.

Un par $(M, \preceq)$ formado por un monoide M y un preorden lineal $\preceq$ en M se llama un *monoide preordenado*. Si G es un grupo podemos hacer las mismas definiciones y obtenemos el concepto de *grupo preordenado*.

(2.2) Lema.
Si $(M, \preceq)$ es un monoide preordenado, entonces $(M/\equiv, \prec)$ es un monoide ordenado. En particular si $(G, \preceq)$ es un grupo preordenado, entonces se verifica que $(G/\equiv, \preceq)$ es un grupo ordenado.

Si $(G, \preceq)$ es un grupo preordenado, entonces el conjunto

$$G_+ = \{g \in G\colon\ 0 \preceq g\}$$

es cerrado para la suma y verifica $a \preceq b$ si y sólo si $b - a \in G_+$, para cualesquiera elementos $a, b \in G$. Los elementos de G_+ se llaman *elementos positivos* de G.

Vamos a tratar de detallar las propiedades que verifican los elementos positivos y comprobar que son suficientes para definir un orden parcial lineal en un grupo G.

(2.3) Proposición.
Si $P \subseteq G$ es un subconjunto verificando:

(i) $0 \in P$;

(ii) $P + P \subseteq P$;

(iii) *la relación definida por $b - a \in P$ es compatible con la estructura de grupo (es lineal).*

Entonces tenemos una estructura de grupo ordenado si y sólo si $P \cap (-P) = \{0\}$. *Tenemos una estructura de grupo totalmente ordenado si y sólo si se verifica además* $P \cup (-P) = G$.

3. Inducción de órdenes.

(3.1) Observación.
Si $H \subseteq G$ es un submonoide de un monoide ordenado, entonces la estructura de monoide ordenado de G induce en H una estructura de grupo ordenado. En particular si G es un grupo ordenado y H un subgrupo, los elementos positivos de H son los elementos del conjunto $H \cap G_+$.

(3.2) Observación.
Si $\{G_\lambda\colon\ \lambda \in \Lambda\}$ es una familia de monoides ordenados, es posible definir un orden parcial en $\prod G_\lambda$ mediante

$$(a_\lambda)_\lambda \preceq (b_\lambda)_\lambda \text{ si } a_\lambda \preceq b_\lambda \text{ para cada índice } \lambda \in \Lambda.$$

Se obtiene así el *producto* de monoides ordenados. Es claro además que si los G_λ son grupos ordenados el conjunto de los elementos positivos es exactamente $\prod (G_\lambda)_+$.

Esta definición es útil, y la usaremos en un futuro, pero tiene el inconveniente que si los monoides G_λ son totalmente ordenados, no es cierto en general que $\prod_\lambda G_\lambda$ sea totalmente ordenado. Este problema se arregla con la siguiente definición.

(3.3) Observación.
Si $\{G_\lambda\colon\ \lambda \in \Lambda\}$ es una familia de monoides ordenados con Λ un conjunto de índices bien ordenado, entonces en $\prod G_\lambda$ definimos una relación de orden mediante:

$$\begin{array}{l}(a_\lambda)_\lambda \preceq (b_\lambda)_\lambda \text{ si para el menor índice } \lambda \text{ para el que } a_\lambda \neq b_\lambda \\ \text{se tiene } a_\lambda \prec b_\lambda.\end{array}$$

Si cada monoide G_λ es totalmente ordenado, entonces $\prod G_\lambda$ es totalmente ordenado con esta relación de orden. Se obtiene así el *producto lexicográfico* de monoides ordenados.

En el caso en que $\Lambda = \{1, \ldots, n\}$ sea finito consideramos el orden $1 \leq 2 \leq \cdots \leq n$; el orden en el producto lexicográfico $G_1 \times \cdots \times G_n$ se representa por $\preceq_{lex}$ y lo llamamos el *orden lexicográfico*.

Dados dos preórdenes en un conjunto, definimos un nuevo preorden al que vamos a llamar su *composición lexicográfica*.

4. Órdenes en $\mathbb{N}^n$.

Consideramos un monoide M y un orden total $\preceq$ en M. Decimos que $\preceq$ es *monótono* si 0 es un mínimo de M; esto es, para cada $x \in M$ se verifica $0 \preceq x$.

Sea M un monoide y $\preceq$ un orden total en M. Se dice que $\preceq$ es un *orden (total) admisible* si verifica:

(1) Es monótono;

(2) Para cada $a, b, c \in M$ si $a \prec b$, entonces $a + c \prec b + c$.

(4.1) Lema.
Si M es un monoide y $\preceq$ es un orden total admisible en M, entonces M es un monoide cancelativo.

Como consecuencia, si M es un monoide cancelativo y $\preceq$ es un order total en M, entonces $\preceq$ es un orden total admisible si y sólo si es lineal y monótono.

(4.2) Observación.
La composición lexicográfica de órdenes totales admisibles es admisible.

Vamos a considerar el caso particular del monoide $\mathbb{N}^n$.

Sea $\preceq$ un preorden total en $\mathbb{N}^n$. Decimos que $\preceq$ es *fuertemente monótono* si $\alpha_i \leq \beta_i$ para cada índice i, entonces $(\alpha_1, \ldots, \alpha_n) \preceq (\beta_1, \ldots, \beta_n)$, esto es, es una extensión del orden producto en $\mathbb{N}^n$, ver (3.2).

Es claro que cada orden fuertemente monótono es monótono, sin embargo el recíproco no es siempre cierto. Para órdenes lineales sobre $\mathbb{N}^n$ tenemos:

(4.3) Lema.
Todo orden total lineal y monótono en $\mathbb{N}^n$ es fuertemente monótono.

DEMOSTRACIÓN. Supongamos que $\alpha_i \leq \beta_i$ para cada índice i, entonces existe $\gamma \in \mathbb{N}^n$ tal que $\alpha + \gamma = \beta$, como se verifica $0 \preceq \gamma$, se obtiene $\alpha \preceq \alpha + \gamma = \beta$. □

(Para un preorden en $\mathbb{N}^n$ se puede hacer también las definiciones de monótono, fuertemente monótono, preorden admisible, etc.)

Vamos a relacionar cualquier orden admisible con el orden producto en $\mathbb{N}^n$.

(4.4) Teorema.
Sea $\preceq$ un orden total admisible en $\mathbb{N}^n$ y sea $\preceq^p$ el orden producto en $\mathbb{N}^n$. Entonces $\preceq$ es un buen orden que extiende a $\preceq^p$.

DEMOSTRACIÓN. Dados $\alpha, \beta \in \mathbb{N}^n$, con $\alpha \preceq^p \beta$, existe $\gamma \in \mathbb{N}^n$ tal que $\beta = \alpha + \gamma$. Es claro que $0 \preceq \gamma$, luego se verifica:

$$\alpha = \alpha + 0 \preceq \alpha + \gamma = \beta.$$

Tenemos por tanto que $\preceq$ extiende a $\preceq^p$. Como $\preceq^p$ es un orden de Dickson, entonces $\preceq$ es un orden de Dickson y en consecuencia es un buen orden □

Los siguientes son ejemplos de órdenes admisibles en $\mathbb{N}$. Más adelante veremos que ambos son ejemplos de órdenes inducidos en el producto.

(4.5) Ejemplo.
El *orden lexicográfico* en $\mathbb{N}^n$ se define

$$(a_1, \dots, a_n) \preceq_{lex} (b_1, \dots, b_n) \text{ si } \begin{cases} \text{son iguales ó} \\ \text{existe } 1 \leq i \leq n \text{ tal que } \begin{cases} a_j = b_j, \forall j < i \\ a_i \prec b_i \end{cases} \end{cases}$$

(4.6) Ejemplo.
El *orden lexicográfico inverso* en $\mathbb{N}^n$ se define

$$(a_1, \dots, a_n) \preceq_{invlex} (b_1, \dots, b_n) \text{ si } \begin{cases} \text{son iguales ó} \\ \text{existe } 1 \leq i \leq n \text{ tal que } \begin{cases} a_j = b_j, \forall j > i \\ a_i \prec b_i \end{cases} \end{cases}$$

(4.7) Observación.
En realidad el orden lexicográfico es el producto lexicográfico de los órdenes usuales en $\mathbb{N}$ considerando en $\{1, \dots, n\}$ el orden usual, y el orden lexicográfico inverso es el producto lexicográfico de los órdenes usuales en $\mathbb{N}$, considerando en $\{1, \dots, n\}$ el orden $n < n-1 < \cdots < 2 < 1$.

5. Órdenes vectoriales.

Vamos a introducir en esta sección una forma general de definir órdenes y preórdenes en el monoide $\mathbb{Q}^n$ y por restricción en el monoide $\mathbb{N}^n$.

Dado $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{Q}^n$ definimos un preorden $\preceq_\omega$ en $\mathbb{N}^n$ mediante:

$$\alpha \preceq_\omega \beta \text{ si } \sum_{i=1}^{n} \alpha_i \omega_i \leq \sum_{i=1}^{n} \beta_i \omega_i.$$

Las siguientes propiedades son inmediatas:

1. Es claro que $\preceq_\omega$ es un preorden (verifica las propiedades reflexiva y transitiva);
2. También es lineal (si $\alpha \preceq_\omega \beta$ y $\gamma \in \mathbb{N}^n$, entonces $\sum_i \alpha_i \omega_i \leq \sum_i \beta_i \omega_i$ y $\sum_i (\alpha_i + \gamma_i)\omega_i \leq \sum_i (\beta_i + \gamma_i)\omega_i$);
3. Para que sea monótono es preciso que todo elemento ω_i sea no negativo.

(5.1) Lema.
Para cada $\omega \in \mathbb{Q}^n$ tenemos que son equivalentes:

(a) $\preceq_\omega$ es un preorden, lineal y monótono;

(b) $\omega_i \in \mathbb{Q}^+ \cup \{0\}$ para cada índice $i = 1, \ldots, n$.

Dados $\omega^1, \omega^2 \in \mathbb{Q}^n$ definimos el producto lexicográfico de $\preceq_{\omega^1}$ y $\preceq_{\omega^2}$ y obtenemos un preorden $\preceq_{1,2}$ dado por:

$$\alpha \preceq_{1,2} \beta \text{ si } (\alpha \cdot \omega^1, \alpha \cdot \omega^2) \leq_{lex} (\beta \cdot \omega^1, \beta \cdot \omega^2)$$

Esta construcción se puede generalizar a un número finito de elementos $\omega^1, \ldots, \omega^m \in \mathbb{Q}^n$.

(5.2) Lema.
Si $\omega^1, \ldots, \omega^m \in \mathbb{Q}^n$ es un sistema de generadores de $\mathbb{Q}^n$, entonces $\preceq_{1,\ldots,m}$ es un orden total, y si los ω_i^j son no negativos, entonces $\preceq_{1,\ldots,m}$ es un orden admisible.

DEMOSTRACIÓN. Sean $\alpha, \beta \in \mathbb{N}^n$, si $\alpha \not\preceq_{1,\dots,m} \beta$ entonces $(\alpha \cdot \omega^1, \dots, \alpha \cdot \omega^m) \not\leq (\beta \cdot \omega^1, \dots, \beta \cdot \omega^m)$. Entonces existe un índice *i* tal que $\alpha \cdot \omega^i > \beta \cdot \omega^i$ y $\alpha \cdot \omega^j = \beta \cdot \omega^j$, si $j = 1, \dots, i-1$, pero entonces $(\beta \cdot \omega^1, \dots, \beta \cdot \omega^m) < (\alpha \cdot \omega^1, \dots, \alpha \cdot \omega^m)$.

Para ver que es un orden total es suficiente ver que verifica la propiedad antisimétrica. Si $\alpha \cdot \omega^i = \beta \cdot \omega^i$ para cada índice *i*, como los $\{\omega^i\}_i$ son un sistema de generadores, entonces para cada índice *j* se verifica: $e_j = \sum_i q_{ji} \omega^i$ y por tanto $\alpha_j = \alpha \cdot e_j = \beta \cdot e_j = \beta_j$. □

Los órdenes vectoriales son de interés debido el siguiente resultado:

(5.3) Proposición.
Para cada orden $\preceq$ en $\mathbb{Q}^n$ existen m n–uplas $\omega_1, \dots, \omega_m$, $m \leq n$, tales que $\preceq$ es igual a $\preceq_{1,\dots,m}$

DEMOSTRACIÓN. Ver la demostración en los siguientes trabajos: Robbiano–1986 [23], Robbiano–1985 [22] y Mora–Robbiano–1989 [19]. □

Capítulo 3

Teorema de Poincaré–Birkhoff–Witt.

Vamos a considerar un cuerpo K, usualmente será $\mathbb{C}$, y una K–álgebra R finitamente presentada, esto es, R está generada por elementos $x_1, \ldots, x_n$ verificando las siguientes relaciones:

$$x_j x_i = q_{i,j} x_i x_j + r_{i,j}(x), \quad i < j, \tag{3.1}$$

siendo $0 \neq q_{i,j} \in K$ y $r_{i,j}(x) \in K + KV + KV_{j-1}^2$. Donde $V = \{x_1, \ldots, x_n\}$ y $V_{j-1}^2 = \{x_h x_k \colon\ 1 \leq h \leq k < j\}$.

Es inmediato observar que R es un cociente de $K\langle X_1, \ldots, X_n\rangle$, la K–álgebra libre sobre indeterminadas $X_1, \ldots, X_n$, por el ideal bilátero H generado por los elementos $X_j X_i - q_{i,j} X_i X_j - r_{i,j}(X)$, $i < j$.

Otra consecuencia de la presentación de R es que cada elemento de R se puede escribir en la siguiente forma:

$$\sum_{\alpha} a_\alpha x^\alpha,$$

siendo $a_\alpha \in K$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ y $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Es claro que cuando la expresión anterior es única, la teoría es más sencilla. Para probar que este puede ser el caso en bastantes ejemplos vamos a estudiar un resultado análogo al teorema de Poincaré–Birkhoff–Witt en este tipo de álgebras.

Obtendremos también que el álgebra graduada $\mathrm{gr}(R)$, asociada a la filtración estándar de $\{x_1, \ldots, x_n\}$, de una K–álgebra R verificando las condiciones en (3.1), se puede describir en términos de una extensión de Ore

iterada

$$K[X_1;\sigma_1,\delta_1]\cdots[X_n;\sigma_n,\delta_n],$$

1. Álgebra libres.

Sea $\{X_1,\ldots,X_n\}$ una familia finita de indeterminadas. La *K–álgebra libre* sobre $\{X_1,\ldots,X_n\}$ es el conjunto de polinomios formales

$$\sum_{\alpha} a_\alpha X_{i_1}\cdots X_{i_m},$$

siendo $\alpha=(i_1,\ldots,i_m)$, $i_j\in\{1,\ldots,n\}$, $m\in\mathbb{N}$ y $a_\alpha\in K$.

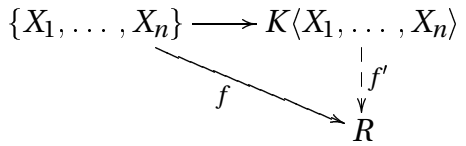
Representamos por $K\langle X_1,\ldots,X_n\rangle$ este conjunto de polinomios y definimos en él, en la forma obvia, dos operaciones internas: la suma y el producto (el producto de los X_i se realiza por yuxtaposición). Obtenemos que con estas operaciones $K\langle X_1,\ldots,X_n\rangle$ es una K–álgebra cuyo elemento uno es 1.

Es sencillo de probar que $K\langle X_1,\ldots,X_n\rangle$ verifica la siguiente propiedad universal:

(1.1) Lema.
Para cada K–álgebra R y cada aplicación $f\colon\{X_1,\ldots,X_n\}\to R$ existe un único homomorfismo de K–álgebras

$$f'\colon K\langle X_1,\ldots,X_n\rangle\to R$$

verificando $f'(X_i)=f(X_i)$, $1\le i\le n$.



La definición de f' para que se tenga la conmutatividad del diagrama es:

$$f'(\sum_{\alpha} a_\alpha X_{i_1}\cdots X_{i_m})=\sum_{\alpha} a_\alpha f(X_{i_1})\cdots f(X_{i_m}).$$

2. Pares índices.

Sea R una K–álgebra finitamente generada y $\{x_1, \ldots, x_n\}$ un sistema de generadores de R. Existe un único homomorfismo de K–álgebras sobreyectivo

$$f' \colon K\langle X_1, \ldots, X_n\rangle \to R$$

verificando $f'(X_i) = x_i$, $1 \leq i \leq n$.

El núcleo de f' es el conjunto de las relaciones que verifican los generadores $\{x_1, \ldots, x_n\}$.

La K–álgebra R se llama *finitamente presentada* si el ideal $H = \mathrm{Ker}(f')$ es un ideal bilátero finitamente generado de $K\langle X_1, \ldots, X_n\rangle$.

Como hemos mencionado anteriormente, en este estudio vamos a considerar únicamente K–álgebras finitamente presentadas. En especial vamos a estudiar la clase especial de K–álgebras finitamente presentadas con sistema de generadores $\{x_1, \ldots, x_n\}$ que verifica las relaciones:

$$x_j x_i = q_{i,j} x_i x_j + r_{i,j}(x), \quad i < j,$$

siendo $0 \neq q_{i,j} \in K$ y $r_{i,j}(x) \in K + KV + KV_{j-1}^2$ (En donde hemos usado las siguientes notaciones: $V = \{x_1, \ldots, x_n\}$ y $V_{j-1}^2 = \{x_h x_k \colon 1 \leq h \leq k < j\}$.) Llamamos a una K–álgebra de este tipo una *K–álgebra cuadrática triangular*, o simplemente una *K–álgebra triangular*.

Sea R una K–álgebra triangular. Un *término* de R es un elemento de la forma:

$$\mathbf{x} = x_{i_1} \cdots x_{i_m}, \quad x_{i_j} \in \{x_1, \ldots, x_n\}.$$

Cuando $m = 0$ tenemos $\mathbf{x} = 1$.

Dado un término $\mathbf{x} = x_{i_1} \cdots x_{i_m}$, vamos a definir dos números asociados a $\mathbf{x}$. El primero es el *peso* de $\mathbf{x}$, y que representamos por $W(\mathbf{x})$. Para definir $W(\mathbf{x})$ primero fijamos una sucesión de números enteros primos positivos $p_1, \ldots, p_n$ que verifique las siguientes condiciones:

$$p_{i-1}^3 < p_i, \quad 2 \leq i \leq n.$$

A continuación definimos

$$W(\mathbf{x}) = (\sum e_i, p_1^{e_1} \cdots p_n^{e_n}),$$

con el orden lexicográfico, siendo e_i el número de copias de x_i en el desarrollo de $\mathbf{x}$. El segundo número que definimos es el *índice* de $\mathbf{x}$, y lo representamos por $I(\mathbf{x})$. Éste es exactamente el índice en el sentido de G. Birkhoff, esto es, primero definimos para cada par $1 \leq j, k \leq m$

$$I_{jk} = \begin{cases} 0 \text{ if } i_j \leq i_k, \\ 1 \text{ if } i_j > i_k \end{cases}$$

y a continuación definimos

$$I(\mathbf{x}) = \sum_{1 \leq j < k \leq m} I_{jk}.$$

El par $(W(\mathbf{x}), I(\mathbf{x}))$ se llama el *par índice* del término $\mathbf{x}$.

En el conjunto $\mathbb{N} \setminus \{0\} \times \mathbb{N}$ definimos un orden total como sigue:

$$(W_1, I_1) \leq (W_2, I_2) \text{ si } \begin{cases} W_1 < W_2 \text{ ó} \\ W_1 = W_2 \text{ y } I_1 \leq I_2 \end{cases}$$

Es el producto lexicográfico de los órdenes usuales en $\mathbb{N} \setminus \{0\}$ y $\mathbb{N}$.

Veamos a continuación una primera aplicación del par índice.

(2.1) Lema.
Para cada término $\mathbf{x} = x_{i_1} \cdots x_{i_m}$ *en* R *existen* $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$, *y* $a_{(\alpha_1, \ldots, \alpha_n)} \in K$ *tales que*

$$\mathbf{x} = \sum a_{(\alpha_1, \ldots, \alpha_n)} x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

DEMOSTRACIÓN. Hacemos la demostración por inducción sobre el par índice de $\mathbf{x}$. El par índice más pequeño de los términos de R es $(1, 0)$; en este caso tenemos que $\mathbf{x} = 1$ y el resultado es cierto. Sea $\mathbf{x}$ un término en R, si $I(\mathbf{x}) = 0$, entonces el resultado es también cierto. Sea $\mathbf{x}$ un término en R tal que $I(\mathbf{x}) > 0$ y supongamos que el resultado es cierto para cada término en R con par índice menor que $(W(\mathbf{x}), I(\mathbf{x}))$. En este caso existe un índice i_j tal que $i_j > i_{j+1}$ y tenemos

$$x_{i_j} x_{i_{j+1}} = q_{i_{j+1}, i_j} x_{i_{j+1}} x_{i_j} + r_{i_{j+1}, i_j}.$$

(Aquí hemos representado $r_{i_{j+1}, i_j}(x)$ sencillamente por r_{i_{j+1}, i_j}; lo seguiremos haciendo así en este capítulo.) Descomponemos $\mathbf{x}$ en dos sumandos

$$\begin{aligned} \mathbf{x} &= x_{i_1} \cdots x_{i_j} x_{i_{j+1}} \cdots x_{i_m} = \\ &= q_{i_{j+1}, i_j} x_{i_1} \cdots x_{i_{j+1}} x_{i_j} \cdots x_{i_m} + x_{i_1} \cdots r_{i_{j+1}, i_j} \cdots x_{i_m}. \end{aligned}$$

Ya que $i_{j+1} < i_j$, tenemos:

$$I(x_{i_1} \cdots x_{i_{j+1}} x_{i_j} \cdots x_{i_m}) < I(\mathbf{x}).$$

Por otro lado tenemos que $r_{i_{j+1},i_j} \in K + KV + KV_{i_j-1}^2$. Podemos descomponer r_{i_{j+1},i_j} en dos partes:

$$r_{i_{j+1},i_j,1} \in K + KV \text{ and } r_{i_{j+1},i_j,2} \in KV_{i_j-1}^2$$

y es claro que el peso de cada término en $x_{i_1} \cdots r_{i_{j+1},i_j,1} \cdots x_{i_m}$ es menor que $W(x)$ y lo mismo ocurre para $x_{i_1} \cdots r_{i_{j+1},i_j,2} \cdots x_{i_m}$. Por lo tanto, por la hipótesis de inducción, tenemos el resultado. □

Como consecuencia inmediata de este Lema tenemos:

(2.2) Corolario.
La familia $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \colon \alpha_1, \ldots, \alpha_n \in \mathbb{N}\}$ *es un sistema de generadores de R como espacio vectorial sobre K.*

Claro que con esto no basta para tener una buena descripción de los elementos de *R*; sería conveniente que además la familia que aparece en el Corolario fuese una base; esto lo conseguimos mediante el teorema de Poincaré–Birkhoff–Witt, pero necesitaremos imponer nuevas propiedades a las álgebras en consideración.

3. Teorema de Poincaré–Birkhoff–Witt.

Estamos ahora interesados en probar un teorema análogo al de Poincaré–Birkhoff–Witt para *K*–álgebras triangulares *R* con respecto a un sistema de generadores $\{x_1, \ldots, x_n\}$.

Como *R* es un cociente de una *K*–álgebra libre sobre $\{X_1, \ldots, X_n\}$, definimos por recurrencia una aplicación *K*–lineal

$$\sigma \colon K\langle X_1, \ldots, X_n\rangle \to K[X_1, \ldots, X_n],$$

siendo $K[X_1, \ldots, X_n]$ el anillo de polinomios en indeterminadas conmutativas. Llamamos $T = K\langle X_1, \ldots, X_n\rangle$. En *T* consideramos la filtración estándar $\{T_m\}_m$ asociada al sistema de generadores $\{X_1, \ldots, X_n\}$ y la graduación $T = \oplus_m T^m$ definida por el grado total. Es claro que $T_m = \oplus_{i \le m} T^i$.

Para definir σ procedemos como sigue.

Definimos $\sigma(1) = 1$, entonces σ está definido sobre $T_0 = T^0$. Supongamos que σ está definido T_{m-1} y que verifica la siguientes relaciones:

(i) $\sigma(X_{i_1} \cdots X_{i_{m-1}}) = X_{i_1} \cdots X_{i_{m-1}}$ si $I(X_{i_1} \cdots X_{i_{m-1}}) = 0$;

(ii) si $i_j > i_{j+1}$, entonces

$$\sigma(X_{i_1} \cdots X_{i_{m-1}}) = q_{i_{j+1},i_j}\sigma(X_{i_1} \cdots X_{i_{j+1}} X_{i_j} \cdots X_{i_{m-1}}) + \sigma(X_{i_1} \cdots r_{i_{j+1},i_j} \cdots X_{i_{m-1}}). \quad (3.2)$$

Por lo tanto, para definir σ en T_m basta con definir σ sobre T^m.

Sea $X_{i_1} \cdots X_{i_m} \in T^m$. Si $I(X_{i_1} \cdots X_{i_m}) = 0$ definimos $\sigma(X_{i_1} \cdots X_{i_m}) = X_{i_1} \cdots X_{i_m}$. El término en T^m con menor par índice es $X_1 \cdots X_1$, el producto de m copias de X_1, y σ se puede definir sobre él; $\sigma(X_1 \cdots X_1) = X_1 \cdots X_1$.

Supongamos que hemos definido σ sobre todos los términos con par índice menor que $X_{i_1} \cdots X_{i_m}$ y que $I(X_{i_1} \cdots X_{i_m}) > 0$. Entonces existe un índice i_a tal que $i_a > i_{a+1}$ y podemos hacer la definición

$$\sigma(X_{i_1} \cdots X_{i_m}) = q_{i_{a+1},i_a}\sigma(X_{i_1} \cdots X_{i_{a+1}} X_{i_a} \cdots X_{i_m}) + \sigma(X_{i_1} \cdots r_{i_{a+1},i_a} \cdots X_{i_m}).$$

Es claro que $X_{i_1} \cdots X_{i_{a+1}} X_{i_a} \cdots X_{i_m}$ y cada término en $X_{i_1} \cdots r_{i_{a+1},i_a} \cdots X_{i_m}$ tiene par índice menor que el par índice de $X_{i_1} \cdots X_{i_m}$.

Para finalizar necesitamos probar que la anterior definición es independiente del índice i_a elegido.

Sea i_b otro índice con $i_b > i_{b+1}$ y $b \geq a$. Si $i_{a+1} < i_b$, entonces no existe contradicción con la definición anterior; en efecto tenemos:

$$\begin{aligned}
&\sigma(\mathrm{X_{i_1}} \cdots \mathrm{X_{i_m}}) = \\
&= q_{i_{a+1},i_a}\sigma(X_{i_1} \cdots X_{i_{a+1}} X_{i_a} \cdots X_{i_m}) + \sigma(X_{i_1} \cdots r_{i_{a+1},i_a} \cdots X_{i_m}) = \\
&= q_{i_{a+1},i_a} q_{i_{b+1},i_b}\sigma(X_{i_1} \cdots X_{i_{a+1}} X_{i_a} \cdots X_{i_{b+1}} X_{i_b} \cdots X_{i_m}) + \\
&+ q_{i_{a+1},i_a}\sigma(X_{i_1} \cdots X_{i_{a+1}} X_{i_a} \cdots r_{i_{b+1},i_b} \cdots X_{i_m}) + \\
&+ q_{i_{b+1},i_b}\sigma(X_{i_1} \cdots r_{i_{a+1},i_a} \cdots X_{i_{b+1}} X_{i_b} \cdots X_{i_m}) + \\
&+ \sigma(X_{i_1} \cdots r_{i_{a+1},i_a} \cdots r_{i_{b+1},i_b} \cdots X_{i_m}),
\end{aligned}$$

por lo tanto en este caso el resultado final es independiente del índice elegido.

Cuando $i_{a+1} = i_b$ la situación es diferente y más complicada. Para simplificar las expresiones vamos a renombrar las indeterminadas que aparecen. Supongamos entonces que se tiene:

$$\begin{aligned} &X_{i_a} = C, \\ &X_{i_{a+1}} = X_{i_b} = B \text{ and} \\ &X_{i_{b+1}} = A; \end{aligned}$$

escribimos también $Q_{AB} = q_{i_{b+1},i_{a+1}}$ etc. para los demás índices. Tenemos por tanto el siguiente desarrollo:

$$\begin{aligned} &\sigma(\mathrm{X_{i_1}} \cdots \mathrm{X_{i_m}}) = \\ &= \sigma(X_{i_1} \cdots CBA \cdots X_{i_n}) = \\ &= q_{BC}\sigma(\cdots BCA \cdots) + \sigma(\cdots r_{BC}A \cdots) = \\ &= q_{BC}q_{AC}\sigma(\cdots BAC \cdots) + q_{BC}\sigma(\cdots Br_{AC} \cdots) + \sigma(\cdots r_{BC}A \cdots) = \\ &= q_{BC}q_{AC}q_{AB}\sigma(\cdots ABC \cdots) + q_{BC}q_{AC}\sigma(\cdots r_{AB}C \cdots) + \\ &+ q_{BC}\sigma(\cdots Br_{AC} \cdots) + \sigma(\cdots r_{BC}A \cdots). \end{aligned}$$

En la misma forma obtenemos:

$$\begin{aligned} &\sigma(\mathrm{X_{i_1}} \cdots \mathrm{X_{i_m}}) = \sigma(X_{i_1} \cdots CBA \cdots X_{i_m}) = \\ &= q_{AB}\sigma(\cdots CAB \cdots) + \sigma(\cdots Cr_{AB} \cdots) = \\ &= q_{AB}q_{AC}\sigma(\cdots ACB \cdots) + q_{AB}\sigma(\cdots r_{AC}B \cdots) + \sigma(\cdots Cr_{AB} \cdots) = \\ &= q_{AB}q_{AC}q_{BC}\sigma(\cdots ABC \cdots) + q_{AB}q_{AC}\sigma(\cdots Ar_{BC} \cdots) + \\ &+ q_{AB}\sigma(\cdots r_{AC}B \cdots) + \sigma(\cdots Cr_{AB} \cdots). \end{aligned}$$

Es necesario probar ahora que estos dos elementos son iguales; esto es equivalente a probar la siguiente igualdad:

$$\begin{aligned} \sigma(q_{BC}q_{AC}(\cdots r_{AB}C \cdots) + q_{BC}(\cdots Br_{AC} \cdots) + (\cdots r_{BC}A \cdots)) = \\ \sigma(q_{AB}q_{AC}(\cdots Ar_{BC} \cdots) + q_{AB}(\cdots r_{AC}B \cdots) + (\cdots Cr_{AB} \cdots)). \end{aligned} \tag{3.3}$$

Veamos en primer lugar que se verifica:

$$q_{BC}q_{AC}r_{AB}C + q_{BC}Br_{AC} + r_{BC}A - q_{AB}q_{AC}Ar_{BC} - q_{AB}r_{AC}B - Cr_{AB} \in H. \tag{3.4}$$

Para probar esto vamos a trabajar módulo el ideal H generado por la relación de R. Tenemos en este caso las congruencias:

$$\begin{aligned} &q_{BC}q_{AC}r_{AB}C + q_{BC}Br_{AC} + r_{BC}A \equiv \\ &\equiv q_{BC}q_{AC}(BA - q_{AB}AB)C + q_{BC}B(CA - q_{AC}AC) + (CB - q_{BC}BC)A \equiv \\ &\equiv q_{BC}q_{AC}BAC - q_{BC}q_{AC}q_{AB}ABC + \\ &+ q_{BC}BCA - q_{BC}Bq_{AC}AC + CBA - q_{BC}BCA \equiv \\ &\equiv -q_{BC}q_{AC}q_{AB}ABC + CBA. \end{aligned}$$

Y de forma análoga tenemos:

$$q_{AB}q_{AC}Ar_{BC} + q_{AB}r_{AC}B + Cr_{AB} \equiv$$
$$\equiv q_{AB}q_{AC}A(CB - q_{BC}BC) + q_{AB}(CA - q_{AC}AC)B + C(BA - q_{AB}AB) \equiv$$
$$\equiv q_{AB}q_{AC}ACB - q_{AB}q_{AC}q_{BC}ABC +$$
$$+q_{AB}CAB - q_{AB}q_{AC}ACB + CBA - q_{AB}CAB \equiv$$
$$\equiv -q_{BC}q_{AC}q_{AB}ABC + CBA.$$

Vamos a llamar, al igual que Berger en ([4]), al elemento en (3.4) la *suma de Jacobi* de R definida por A, B y C, y la vamos a representar por $J(A,B,C)$. Imponemos a R la siguiente condición:

condición PBW. $J(A,B,C)$ es una combinación K–lineal de $R_{X,Y}Z$, $ZR_{X,Y}$ y $R_{X,Y}$ con $X < Y$ y X, Y, $Z < C$ en el orden $X_1 < \cdots < X_n$, siendo $R_{X,Y} = YX - q_{X,Y}XY - r_{X,Y}$.

(Esta es una condición más fuerte que la de $J(A,B,C) \in H$ y la necesitamos para poder hacer inducción sobre el par índice.)

Por lo tanto tenemos una expresión de la forma

$$J(A,B,C) = \sum a_{ZXY}ZR_{X,Y} + \sum a_{XYZ}R_{X,Y}Z + \sum a_{XY}R_{X,Y},$$

en la que cada término de esta suma tiene un par índice menor que el par índice de CBA.

Ahora para aplicar esto a nuestra relación (3.3), procedemos como sigue:

$$\sigma(q_{BC}q_{AC}(\cdots r_{AB}C\cdots) + q_{BC}(\cdots Br_{AC}\cdots) + (\cdots r_{BC}A\cdots)) -$$
$$-\sigma(q_{AB}q_{AC}(\cdots Ar_{BC}\cdots) + q_{AB}(\cdots r_{AC}B\cdots) + (\cdots Cr_{AB}\cdots)) =$$
$$= \sigma(\cdots J(ABC)\cdots) =$$
$$= \sigma(\cdots \sum a_{ZXY}ZR_{X,Y} + \sum a_{XYZ}R_{X,Y}Z + \sum a_{XY}R_{X,Y}\cdots) = 0$$

Obtenemos entonces el siguiente resultado:

(3.1) Teorema.
Sea R una K–álgebra triangular finitamente presentada verificando la condición PBW con respecto a un sistema de generadores $\{x_1,\ldots,x_n\}$. Entonces la familia $\{x_1^{\alpha_1}\cdots x_n^{\alpha_n}\colon\ \alpha_1,\ldots,\alpha_n \in \mathbb{N}\}$ es una base de R como espacio vectorial sobre K.

4. Un poco de aritmética.

Consideramos un anillo de polinomios formales $\mathrm{K}[\mathrm{X}_1,\ldots,\mathrm{X}_\mathrm{n}]$, en indeterminadas no conmutativas, cuyas indeterminadas verifican las relacio-

nes de conmutación siguientes:

$$X_jX_i = q_{i,j}X_iX_j, \text{ if } i < j,$$

siendo $0 \neq q_{i,j} \in K$. Entonces $\mathrm{K[X_1, \ldots, X_n]}$ es una K–álgebra finitamente generada son sistema de generadores formado por: $\{X_1, \ldots, X_n\}$. Evidentemente verifica la condición de PBW.

Vamos a ver algunas relaciones que se verifican en $\mathrm{K[X_1, \ldots, X_n]}$. Por hipótesis tenemos $X_jX_i = q_{i,j}X_iX_j$, si $i < j$. Una regla general de conmutatividad puede construirse de la siguiente forma. Primero, si $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ entonces tenemos:

$$\begin{aligned} X_iX^\alpha &= X_i(X_1^{\alpha_1} \cdots X_n^{\alpha_n}) = \\ &= q_{1,i}X_1X_iX_1^{\alpha_1-1}X_2^{\alpha_2} \cdots X_n^{\alpha_n} \\ &\cdots \\ &= q_{1,i}^{\alpha_1}X_1^{\alpha_1}X_iX_2^{\alpha_2} \cdots X_n^{\alpha_n} \\ &\cdots \\ &= q_{1,i}^{\alpha_1} \cdots q_{i-1,i}^{\alpha_{i-1}}X_1^{\alpha_1} \cdots X_{i-1}^{\alpha_{i-1}}X_i^{1+\alpha_i} \cdots X_n^{\alpha_n}. \end{aligned}$$

Por inducción podemos generalizar esta relación y obtener:

$$X_i^{\beta_i}X^\alpha = q_{1,i}^{\alpha_1\beta_i} \cdots q_{i-1,i}^{\alpha_{i-1}\beta_i}X_1^{\alpha_1} \cdots X_{i-1}^{\alpha_{i-1}}X_i^{\beta_i+\alpha_i} \cdots X_n^{\alpha_n}.$$

Para simplificar esta expresión vamos a introducir la siguiente notación. Definimos una upla $\mathbf{q} = (q_{i,j})_{i,j}$, para $i < j$, y definimos $\mathbf{q}^{(\alpha,\beta)} = \prod_{i<j} q_{i,j}^{\alpha_i\beta_j}$.

Cuando $\beta = (0, \ldots, \beta_i, \ldots, 0)$, se obtiene el resultado anterior. Es fácil ver que se obtiene también la siguiente regla general de conmutatividad:

$$X^\beta X^\alpha = \mathbf{q}^{(\alpha,\beta)}X^{\beta+\alpha}.$$

También se cumplen las siguientes relaciones:

$$\mathbf{q}^{(\alpha+\alpha',\beta+\beta')} = \mathbf{q}^{(\alpha,\beta)}\mathbf{q}^{(\alpha,\beta')}\mathbf{q}^{(\alpha',\beta)}\mathbf{q}^{(\alpha',\beta')}.$$

Ya que los exponentes pueden ser negativos usando $q_{i,j}^{-1}$, tenemos también las relaciones:

$$\mathbf{q}^{-(\alpha,\beta)} = \mathbf{q}^{(-\alpha,\beta)} = \mathbf{q}^{(\alpha,-\beta)}.$$

5. Cocientes de extensiones de Ore.

Sea R una K–álgebra triangular finitamente generada y $\{x_1, \dots, x_n\}$ un sistema de generadores verificando las relaciones:

$$x_j x_i = q_{i,j} x_i x_j + r_{i,j}, \quad i < j \tag{3.1}$$

siendo $0 \neq q_{i,j} \in K$ y $r_{i,j} \in K \oplus KV \oplus KV_{j-1}^2$.

Consideramos en R la filtración estándar $\{R_m\}_m$ asociada a este sistema de generadores y la K–álgebra graduada asociada

$$\mathrm{gr}(R) = \oplus_i R_i/R_{i-1}.$$

Para determinar la estructura de $\mathrm{gr}(R)$ vamos a construir una extensión de Ore y obtendremos $\mathrm{gr}(R)$ como cociente suyo.

Definimos recursivamente automorfismos σ_j y σ_j–derivaciones δ_j, $j = 2, \dots, n$, en

$$S_{j-1} = K[X_1; \sigma_1, \delta_1] \cdots [X_{j-1}; \sigma_{j-1}, \delta_{j-1}],$$

siendo $\sigma_1 = 1$ y $\delta_1 = 0$. La definición de σ_j es fácil; tenemos: $\sigma_j(X_i) = q_{i,j} X_i$ para cada $i < j$. Y se prueban por inducción las siguientes relaciones:

$$\sigma_j(X_1^{\alpha_1} \cdots X_{j-1}^{\alpha_{j-1}}) = \mathbf{q}^{(\alpha, e_j)} X_1^{\alpha_1} \cdots X_{j-1}^{\alpha_{j-1}}, \tag{3.5}$$

usando la notación introducida en la Sección 4.

Para la definición de δ_j hacemos:

$$\begin{array}{l} \delta_j(\sum_\alpha a_\alpha X^\alpha) = \\ = X_j \sum_\alpha a_\alpha X^\alpha - \sigma_j(\sum_\alpha a_\alpha X^\alpha) X_j = \\ = X_j \sum_\alpha a_\alpha X^\alpha - \sum_\alpha a_\alpha \mathbf{q}^{(\alpha, e_j)} X^\alpha X_j \end{array} \tag{3.6}$$

para cada $\sum_\alpha a_\alpha X^\alpha \in S_{j-1}$.

(5.1) Observación.
Podemos probar, también por inducción, que el elemento así definido pertenece a S_{j-1}.

Para probar que δ_j es una σ_j–derivación basta estudiar los siguientes desarrollos:

$$\begin{array}{l} \delta_j(\sum_\alpha a_\alpha X^\alpha \sum_\beta b_\beta X^\beta) = \\ = X_j \sum_\alpha a_\alpha X^\alpha \sum_\beta b_\beta X^\beta - \sigma_j(\sum_\alpha a_\alpha X^\alpha \sum_\beta b_\beta X^\beta) X_j, \end{array}$$

y por otro lado tenemos:

$$\begin{aligned}
&\sigma_j(\textstyle\sum_\alpha a_\alpha X^\alpha)\delta_j(\sum_\beta b_\beta X^\beta) + \delta_j(\sum_\alpha a_\alpha X^\alpha)\sum_\beta b_\beta X^\beta = \\
&= \sigma_j(\textstyle\sum_\alpha a_\alpha X^\alpha)\left(X_j\sum_\beta b_\beta X^\beta - \sigma_j(\sum_\beta b_\beta X^\beta)X_j\right) + \\
&+ \left(X_j\textstyle\sum_\alpha a_\alpha X^\alpha - \sigma_j(\sum_\alpha a_\alpha X^\alpha)X_j\right)\sum_\beta b_\beta X^\beta = \\
&= X_j\textstyle\sum_\alpha a_\alpha X^\alpha\sum_\beta b_\beta X^\beta - \sigma_j(\sum_\alpha a_\alpha X^\alpha\sum_\beta b_\beta X^\beta)X_j.
\end{aligned}$$

(5.2) Observación.
Tenemos pues que $\mathrm{gr}(R)$ es un cociente de una extensión iterada de Ore. Si además verifica la condición de PBW para el sistema de generadores $\{x_1,\dots,x_n\}$ de R, entonces $\mathrm{gr}(R)$ es un cociente impropio y por tanto $\mathrm{gr}(R)$ es una extensión iterada de Ore.

(5.3) Observación.
Es también posible invertir el anterior resultado, esto es, probar que si $\mathrm{gr}(R)$ es una extensión iterada de Ore verificando las condiciones (3.5) y (3.6), entonces R verifica la condición de PBW para un sistema de generadores que verifique la condición (3.1). Este resultado nos proporciona una gran cantidad de ejemplos de álgebras triangulares verificando la condición de PBW.

Capítulo 4

Álgebras triangulares.

Consideramos una K–álgebra R generada por elementos $x_1, \ldots, x_n$ verificando las siguientes relaciones de conmutación:

$$x_j x_i = q_{i,j} x_i x_j + r_{i,j}, \quad i < j, \tag{4.1}$$

siendo $0 \neq q_{i,j} \in K$ y $r_{i,j} \in K + KV + KV_{j-1}^2$. Donde $V = \{x_1, \ldots, x_n\}$ y $V_{j-1}^2 = \{x_h x_k \colon 1 \leq h \leq k < j\}$ y la condición de PBW. Entonces el conjunto $\{\mathbf{x}^\alpha \colon \alpha \in \mathbb{N}^n\}$ es una base de R como espacio vectorial y en consecuencia cada elemento f de R tiene una expresión única en la forma

$$f = \sum_\alpha a_\alpha \mathbf{x}^\alpha,$$

siendo $\alpha \in \mathbb{N}^n$ y $a_\alpha \in K$ casi todos nulos.

Llamamos *término* de R a cada uno de los elementos de la base $\{\mathbf{x}^\alpha \colon \alpha \in \mathbb{N}^n\}$. Es claro que los términos de R están parametrizados por el conjunto $\mathbb{N}^n$. De cara a desarrollar una aritmética en R vamos a considerar un orden admisible en $\mathbb{N}^n$ y en consecuencia un orden total en el conjunto de los términos de R. Cuando R es conmutativo el orden admisible en $\mathbb{N}^n$ implica que el orden total en R es compatible con la multiplicación; sin embargo, cuando R no es conmutativo esto no tiene por que ocurrir.

Veamos como podemos solucionar este problema. Dado un orden admisible $\preceq$ en $\mathbb{N}^n$ podemos escribir cada elemento f de R de forma única como una expresión

$$f = a_{\alpha^1} \mathbf{x}^{\alpha^1} + \cdots + a_{\alpha^r} \mathbf{x}^{\alpha^r},$$

siendo $\alpha^1 > \cdots > \alpha^r$ y $a_{\alpha^i} \neq 0$ para cada $i = 1, \ldots, r$.

Tomemos el caso particular en que $f = x_j$ y consideremos $g = x_i$ con $i < j$. Se verifica:

$$fg = x_j x_i = q_{i,j} x_i x_j + r_{i,j}.$$

Parece natural que $x_i x_j$ sea el mayor término de fg, y que por tanto los términos, que con coeficiente no nulo aparecen en $r_{i,j}$ sean menores. Para conseguir esto necesitamos imponer condiciones al orden admisible en consideración; por ejemplo basta con que $\preceq$ sea la composición lexicográfica del preorden suma y el orden lexicográfico en $\mathbb{N}^n$; llamaremos a este el orden lexicográfico graduado. De esta forma nos aseguramos que para cualquier par de elementos genéricos $f = a_{\alpha^1}\mathbf{x}^{\alpha^1} + \cdots + a_{\alpha^r}\mathbf{x}^{\alpha^r}$ y $g = a_{\beta^1}\mathbf{x}^{\beta^1} + \cdots + a_{\beta^s}\mathbf{x}^{\beta^s}$ de R se tiene que el mayor término de fg es exactamente $\mathbf{x}^{\alpha^1+\beta^1}$.

A partir de aquí podemos desarrollar una aritmética en el anillo R.

1. Expresiones polinómicas.

Consideramos una K–álgebra triangular R verificando la condición de PBW. Comenzamos por fijar el orden lexicográfico en $\mathbb{N}^n$ para la ordenación $e_1 < e_2 < \cdots < e_n$, siendo $e_i = (\delta_{ij})_{j=1}^n$. Supongamos que para $i < j$ se tiene la relación

$$x_j x_i = q_{i,j} x_i x_j + r_{i,j},$$

siendo $r_{i,j} = \sum_{k \leq l < j} a_{i,j}^{k,l} x_k x_l + \sum_{k=1}^n a_{i,j}^k x_k + a_{i,j}$, con $a_{i,j}^{*,*} \in K$. Utilizando el orden anterior y ordenando los monomios respecto a él tenemos la siguiente expresión

$$\begin{aligned} x_j x_i = q_{i,j} x_i x_j + a_{i,j}^{j-1,j-1} x_{j-1}^2 + \cdots + a_{i,j}^{1,2} x_1 x_2 + a_{i,j}^{1,1} x_1^2 + \\ a_{i,j}^n x_n + \cdots + a_{i,j}^1 x_1 + a_{i,j}. \end{aligned}$$

Vamos a utilizar en lo que sigue la siguiente notación:

$$\begin{aligned} r_{i,j,1} &= a_{i,j}^{j-1,j-1} x_{j-1}^2 + \cdots + a_{i,j}^{1,2} x_1 x_2 + a_{i,j}^{1,1} x_1^2 \\ r_{i,j,2} &= a_{i,j}^n x_n + \cdots + a_{i,j}^1 x_1 + a_{i,j} \end{aligned}$$

Dado un elemento $0 \neq f \in R$, podemos escribir f en la forma:

$$f = \sum_{\alpha} a_\alpha x^\alpha,$$

siendo $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ y $a_\alpha \in K$ casi todos nulos.
El *diagrama de Newton* de f es:

$$\mathcal{N}(f) = \{\alpha \in \mathbb{N}^n:\ a_\alpha \neq 0\}$$

El *exponente* de f es:

$$\exp(f) = \max\{\alpha \in \mathbb{N}^n:\ \alpha \in \mathcal{N}(f)\}$$

El *grado* de f es:

$$\operatorname{grad}(f) = \max\{\alpha_1 + \cdots + \alpha_n:\ \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{N}(f)\}$$

El *coeficiente principal* de f es:

$$\operatorname{lc}(f) = a_{\exp(f)}.$$

El *término principal* de f es:

$$\operatorname{lt}(f) = x^{\exp(f)}.$$

El *monomio principal* de f es:

$$\operatorname{lm}(f) = a_{\exp(f)} x^{\exp(f)}.$$

(1.1) Lema.
Dados $0 \neq f, g \in R$ se verifica:

(1) si $f + g \neq 0$, entonces $\exp(f+g) \leq \max\{\exp(f), \exp(g)\}$;

(2) si $\exp(f) < \exp(g)$, entonces $\exp(f+g) = \exp(g)$.

Veamos el comportamiento del exponente ante el producto.

(1.2) Lema.
Para cada $\alpha, \beta \in \mathbb{N}^n$ se verifica:

$$\exp(x^\alpha x^\beta) = \alpha + \beta.$$

DEMOSTRACIÓN. Vamos a hacer la demostración por inducción sobre α y β. Supongamos que $\alpha = e_1$, tenemos

$$x_1 x^\beta = x_1 x_1^{\beta_1} \cdots x_n^{\beta_n},$$

y el resultado es cierto para cada $\beta \in \mathbb{N}^n$. Sea $j > 1$; supongamos que el resultado es cierto para $\alpha = e_1, \ldots, e_{j-1}$ y para cada $\beta \in \mathbb{N}^n$, y que para cada $\gamma < \beta$ se tiene $\exp(x_j x^\gamma) = e_j + \gamma$. Tenemos entonces:

$$\begin{aligned} x_j x^\beta = x_j x_1 x_1^{\beta_1 - 1} \cdots x_n^{\beta_n} = q_{i,j} x_1 x_j x_1^{\beta_1 - 1} \cdots x_n^{\beta_n} + \\ r_{1,j,2} x_1^{\beta_1 - 1} \cdots x_n^{\beta_n} + r_{1,j,1} x_1^{\beta_1 - 1} \cdots x_n^{\beta_n}, \end{aligned}$$

ya que sin pérdida de generalidad podemos suponer que $\beta_1 \neq 0$; al analizar estos sumandos resulta:

(1) el último no cuenta para el exponente, pues su grado es demasiado pequeño;

(2) como $r_{1,j,1} \in KV_{j-1}^2$, el segundo sumando es cero ó su exponente está acotado por $(\beta_1, \ldots, \beta_{j-1} + 2, \beta_j, \ldots, \beta_n)$.;

(3) por la hipótesis de inducción el exponente del primer sumando es:

$$(\beta_1 - 1, \ldots, \beta_j + 1, \ldots, \beta_n) = e_j + \beta.$$

Entonces $\exp(x_j x^\beta) = e_j + \beta$ y por tanto el resultado es cierto para cada índice j y cada $\beta \in \mathbb{N}^n$. Haciendo ahora inducción sobre α se obtiene el resultado. □

Como consecuencia tenemos:

(1.3) Proposición.
Dados $0 \neq f, g \in R$ *se verifica* $fg \neq 0$ *y* $\exp(fg) = \exp(f) + \exp(g)$.

Para desarrollar la aritmética en R necesitamos nuevas definiciones. Si $\alpha^1, \ldots, \alpha^t \in \mathbb{N}^n$ es una lista de elementos de $\mathbb{N}^n$, definimos:

$$\begin{aligned} \Delta^1 &= \alpha^1 + \mathbb{N}^n, \\ \Delta^2 &= (\alpha^2 + \mathbb{N}^n) \setminus \Delta^1, \\ &\vdots \\ \Delta^t &= (\alpha^t + \mathbb{N}^n) \setminus \cup_{i<t} \Delta^i, \\ \overline{\Delta} &= \mathbb{N}^n \setminus \cup_{i \leq t} \Delta^i. \end{aligned}$$

No creemos que la notación α^i para un elemento de $\mathbb{N}^n$ se confunda con la *i*–ésima potencia de α, ya que no vamos a usar potencias de elementos de $\mathbb{N}^n$ a lo largo de este trabajo.

(1.4) Lema.
Para cada lista de elementos de $\mathbb{N}^n$, por ejemplo $\alpha^1, \ldots, \alpha^t$, tenemos que $\{\Delta^1, \Delta^2, \ldots, \Delta^t, \overline{\Delta}\}$ es una partición de $\mathbb{N}^n$.

Como consecuencia tenemos el siguiente algoritmo de la división en *R*.

(1.5) Teorema. (Algoritmo de la división.)
Para cada lista finita de elementos no nulos

$$g_1, \ldots, g_t \in R,$$

consideramos la partición de $\mathbb{N}^n$ determinada por la lista

$$\exp(g_1), \ldots, \exp(g_t).$$

Se verifica entonces que para cada $0 \neq f \in R$ existen elementos $q_1, \ldots, q_t, r \in R$ únicos cumpliendo las propiedades siguientes:

(1) $f = \sum_{i=1}^{t} q_i g_i + r$;

(2) $r = 0$ *ó* $\mathcal{N}(r) \subseteq \overline{\Delta}$;

(3) Para cada índice i se verifica: $\exp(g_i) + \mathcal{N}(q_i) \subseteq \Delta^i$.

Como consecuencia, si $q_i g_i \neq 0$, se tiene $\exp(q_i g_i) \leq \exp(f)$ y si $r \neq 0$, entonces $\exp(r) \leq \exp(f)$.

DEMOSTRACIÓN. Existencia.

Hacemos inducción sobre $\exp(f)$. Si $\exp(f) = 0$, entonces tenemos dos posibilidades:

(i) $\exp(f) = (0, \ldots, 0) \in \Delta^i$, para algún índice *i*;

(ii) $\exp(f) = (0, \ldots, 0) \in \overline{\Delta}$.

(i) Tenemos $\exp(f) = \exp(g_i) + \gamma$, para algún $\gamma \in \mathbb{N}^n$, luego $\exp(g_i) = (0, \ldots, 0)$ y $g_i \in K$. Podemos tomar:

$$\begin{cases} q_j = 0, & \text{si } j \neq i; \\ q_i = f_i / g_i; \\ r = 0 \end{cases}$$

(ii) Tenemos $\exp(f) \in \overline{\Delta}$, entonces podemos tomar:

$$\begin{cases} q_i = 0, & \text{si } i = 1, \dots, t; \\ r = f \end{cases}$$

Supongamos ahora que el resultado es cierto para todos los polinomios g con $\exp(g) < \exp(f)$. Al igual que antes tenemos dos posibilidades:

(i) $\exp(f) \in \Delta^i$, para algún índice i;

(ii) $\exp(f) \in \overline{\Delta}$.

(i) Tenemos $\exp(f) = \exp(g_i) + \gamma$, para algún $\gamma \in \mathbb{N}^n$. Si definimos $h = x^\gamma g_i$ tenemos que $f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(h)} x^\gamma g_i$ es un elemento de R exponente estrictamente menor que f. Aplicando la hipótesis de inducción tenemos:

$$f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(h)} x^\gamma g_i = \sum_i q'_i g_i + r'$$

con los $q'_1, \dots, q'_t, R'$ verificando las condiciones del Teorema. Entonces obtenemos la expresión:

$$f = \sum_i q_i g_i + r,$$

en donde

$$\begin{cases} q_j = q'_j, & \text{si } j \neq i; \\ q_i = q'_i + \frac{\mathrm{lc}(f)}{\mathrm{lc}(h)} x^\gamma; \\ r = r' \end{cases}$$

Para comprobar que se tienen las condiciones del enunciado observemos las siguientes inclusiones:

$$\begin{aligned} \exp(g_i) + \mathcal{N}(q_i) &\subseteq \exp(g_i) + \{\mathcal{N}(q'_i) \cup \{\gamma\}\} = \\ &= (\exp(g_i) + \mathcal{N}(q'_i)) \cup \{\exp(g_i) + \gamma\} \subseteq \\ &\subseteq \Delta^i. \end{aligned}$$

(ii) Si $\exp(f) \in \overline{\Delta}$, entonces $f - \mathrm{lm}(f)$ es un polinomio con exponente estrictamente menor que f, y por tanto, por la hipótesis de inducción, tenemos:

$$f - \mathrm{lm}(f) = \sum_i q'_i g_i + r'$$

con los $q'_1, \ldots, q'_t, r'$ verificando las condiciones del Teorema. Entonces obtenemos la siguiente expresión para f:

$$f = \sum_i q_i g_i + r,$$

en donde

$$\begin{cases} q_i = q'_i, & \text{si } i = 1, \ldots, t; \\ r = r' + \mathrm{lm}(f) \end{cases}$$

Para comprobar que se tienen las condiciones del enunciado tenemos que si $r \neq 0$, entonces, considerando que $\mathcal{N}(0) = \varnothing$, tenemos:

$$\mathcal{N}(r) = \mathcal{N}(r' + \mathrm{lm}(f)) \subseteq \mathcal{N}(r') \cup \{\exp(f)\} \subseteq \overline{\Delta}.$$

Unicidad.

Sean

$$f = \sum_i q_i g_i + r = \sum_i q'_i g_i + r'$$

dos expresiones de f verificando las condiciones. Tenemos entonces:

$$0 = \sum_i (q_i - q'_i) g_i + (r - r').$$

Vamos a analizar los exponentes de los sumandos de esta suma:

$$\exp(r - r') \in \mathcal{N}(r - r') \subseteq \mathcal{N}(r) \cup \mathcal{N}(r') \subseteq \overline{\Delta}.$$

$$\begin{aligned} \exp((q_i - q'_i) g_i) &= \exp(q_i - q'_i) + \exp(g_i) \subseteq \\ &\subseteq \exp(g_i) + (\mathcal{N}(q_i - q'_i)) = \\ &= (\exp(g_i) + \mathcal{N}(q_i)) \cup (\exp(g_i) + \mathcal{N}(q'_i)) \\ &\subseteq \Delta^i. \end{aligned}$$

Ahora como los $\Delta^1, \ldots, \Delta^t, \overline{\Delta}$ forman una partición de $\mathbb{N}^n$, llegamos a que cada uno de los sumandos es cero, y como estamos en un dominio, tenemos $q_i = q'_i$, para cada índice i, y $r = r'$. □

Los elementos $q_1, \ldots, q_t$ se llaman *cocientes a la izquierda* de f y r se llama *resto a la izquierda* de f relativos a $\{g_1, \ldots, g_t\}$. El resto a la izquierda

r se representa también por $r_l(f;\{g_1,\dots,g_t\})$, y si no hay confusión simplemente por $r(f;\{g_1,\dots,g_t\})$.

De forma análoga se definen los cocientes y el resto a la derecha de f relativos a $\{g_1,\dots,g_t\}$.

El orden de los elementos $g_1,\dots,g_t$ es determinante para el cálculo del resto a la izquierda ó a la derecha, esto es, puede ocurrir que:

$$r(f;g_1,\dots,g_i,\dots,g_j,\dots,g_t) \neq r(f;g_1,\dots,g_j,\dots,g_i,\dots,g_t),$$

para $i \neq j$.

2. Bases de Groebner en álgebras triangulares.

Sea R una K–álgebra triangular. Si I es un ideal izquierda de R, definimos

$$\mathrm{Exp}(I) = \{\exp(f)\colon\ f \in I\}.$$

Si $D \subseteq \mathbb{N}^n$, decimos que D es un monoideal de $\mathbb{N}^n$ si para cada $\delta \in D$ y cada $\alpha \in \mathbb{N}^n$ se verifica $\delta + \alpha \in D$.

(2.1) Lema.
$\mathrm{Exp}(I)$ *es un monoideal de* $\mathbb{N}^n$.

(2.2) Proposición.
Cada monoideal D *de* $\mathbb{N}^n$ *tiene un sistema finito de generadores.*

DEMOSTRACIÓN. Tenemos que D es un monoideal de $\mathbb{N}^n$, sea $A \subseteq D$ una base de Dickson de D para el orden usual en $\mathbb{N}^n$, entonces se verifica $D = A + \mathbb{N}^n$, y por tanto A es un sistema de generadores de D. □

(2.3) Lema.
Sea I *un ideal izquierda no nulo de* R *y* A *es un sistema finito de generadores de* $\mathrm{Exp}(I)$*, entonces para cada conjunto de elementos* $\{f_\alpha\colon\ \alpha \in A\} \subseteq I$ *tales que* $\exp(f_\alpha) = \alpha$ *para cada* $\alpha \in A$*, se tiene:* $\{f_\alpha\colon\ \alpha \in A\}$ *es sistema de generadores de* I *como ideal a la izquierda.*

DEMOSTRACIÓN. Como A es finito, supongamos que $\{f_\alpha\colon\ \alpha \in A\} = \{g_1,\dots,g_t\}$. Para cada $0 \neq f \in I$ consideramos el algoritmo de la división para la sucesión $g_1,\dots,g_t$. Obtenemos una expresión $f = \sum_i q_i g_i + r$. Si $r \neq 0$, entonces $\mathcal{N}(r) \subseteq \overline{\Delta}$ y como tenemos $r = f - \sum_i q_i g_i \in I$, se verifica $\exp(r) \in \mathrm{Exp}(I) = A + \mathbb{N}^n = \cup_i \Delta^i$, lo que es una contradicción. □

Si I es un ideal izquierda de R, una *base de Groebner* de I es un conjunto finito de elementos no nulos $\mathbb{G} = \{g_1, \ldots, g_t\} \subseteq I$ verificando que

$$\mathrm{Exp}(I) = \{\exp(g_1), \ldots, \exp(g_t)\} + \mathbb{N}^n.$$

(2.4) Corolario.

(1) Cada ideal izquierda no nulo de R tiene una base de Groebner;

(2) Toda base de Groebner de un ideal izquierda no nulo es un sistema de generadores.

(2.5) Proposición.
Si I es un ideal izquierda no nulo de R, y $\mathbb{G}$, $\mathbb{G}'$ son dos bases de Groebner de I, entonces para cada $0 \neq f \in R$ se verifica $r(f;\mathbb{G}) = r(f;\mathbb{G}')$.

DEMOSTRACIÓN. Supongamos que al aplicar el algoritmo de la división para $\mathbb{G}$ y $\mathbb{G}'$ obtenemos dos expresiones:

$$f = \sum_i q_i g_i + r = \sum_j q'_j g'_j + g',$$

respectivamente. Si $r \neq r'$, como $r - r' \in I$, tenemos

$$\exp(r - r') \in \mathrm{Exp}(I) = \cup_i \Delta^i = \cup_i (\Delta')^i.$$

Pero

$$\exp(r - r') \in \mathcal{N}(r - r') \subseteq \mathcal{N}(r) \cup \mathcal{N}(r') \subseteq \overline{\Delta} = \overline{\Delta'},$$

lo que es una contradicción. □

3. Algoritmo de Buchberger.

Se trata ahora de caracterizar y construir bases de Groebner para ideales a la izquierda de R.

(3.1) Proposición.
Sea I un ideal izquierda no nulo de R y $\mathbb{G}$ una familia finita de elementos de I. Son equivalentes los siguientes enunciados:

(a) $\mathbb{G}$ es una base de Groebner de I;

(b) Para cada $0 \neq f \in I$ se tiene $r(f;\mathbb{G}) = 0$.

DEMOSTRACIÓN. (a)⇒(b). Si $r(f,\mathbb{G}) \neq 0$, entonces $\exp(r(f,\mathbb{G})) \in \mathrm{Exp}(I) \cap \overline{\Delta} = \varnothing$, lo que es una contradicción.

(b)⇒(a). Sea $0 \neq f \in I$, por el algoritmo de la división existen $q_1, \ldots, q_t$, $r \in R$ tales que:

$$\begin{array}{l} f = \sum_i q_i g_i, \text{ y} \\ \exp(g_i) + \mathcal{N}(q_i) \subseteq \Delta^i. \end{array}$$

En consecuencia, $\exp(q_i g_i) \neq \exp(q_j g_j)$ si $i \neq j$, y entonces $\exp(f)$ es el máximo de los exponentes de los sumandos $q_i g_i$, luego existe un índice i tal que

$$\exp(f) = \exp(q_i g_i) \in \Delta^i \subseteq \exp(g_i) + \mathbb{N}^n,$$

y por tanto $\exp(f) \in \{\exp(g_1), \ldots, \exp(g_t)\} + \mathbb{N}^n$. □

Esta caracterización para bases de Groebner no es muy práctica, ya que habría que probar con todos los elementos del ideal a la izquierda I para ver que tenemos una base de Groebner. Se trata entonces de buscar criterios más prácticos para caracterizar bases de Groebner.

Vamos a introducir en este punto la notación necesaria para su desarrollo.

Por hipótesis tenemos que $x_j x_i = q_{i,j} x_i x_j + r_{i,j}$ cuando $i < j$, siendo $0 \neq q_{i,j} \in \mathbb{C}$. Una regla general de conmutatividad en este contexto se puede expresar de la siguiente forma; dados x_i y x^α, se verifican las igualdades siguientes:

$$\begin{aligned} x_i x^\alpha &= x_i(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \\ &= q_{1,i} x_1 x_i x_1^{\alpha_1 - 1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} + \text{monomios con térm. menores} \\ &\cdots \\ &= q_{1,i}^{\alpha_1} x_1^{\alpha_1} x_i x_2^{\alpha_2} \cdots x_n^{\alpha_n} + \text{monomios con térm. menores} \\ &\cdots \\ &= q_{1,i}^{\alpha_1} \cdots q_{i-1,i}^{\alpha_{i-1}} x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} x_i^{1+\alpha_i} \cdots x_n^{\alpha_n} + \text{monomios con térm. menores.} \end{aligned}$$

Que por inducción se puede generalizar fácilmente a:

$$x_i^{\beta_i} x^\alpha = q_{1,i}^{\alpha_1 \beta_i} \cdots q_{i-1,i}^{\alpha_{i-1} \beta_i} x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_i + \beta_i} \cdots x_n^{\alpha_n} + \text{mon. con tér. menores.}$$

Esta expresión final se puede simplificar si consideramos una upla $\mathbf{q} = (q_{i,j})_{i,j}$, con $i < j$, y denotamos $\mathbf{q}^{(\alpha,\beta)} = \prod_{i<j} q_{i,j}^{\alpha_i \beta_j}$.

Es claro que cuando $\beta = (0, \dots, \beta_i, \dots, 0)$, tenemos el resultado anterior y un pequeño ejercicio rutinario prueba que se tiene la ley de conmutación siguiente:

$$\begin{aligned} x^\beta x^\alpha &= \mathbf{q}^{(\alpha,\beta)} x^{\beta+\alpha} + \text{monomios con términos menores} \\ &= \mathbf{q}^{(\alpha,\beta)} x^{\beta+\alpha} + r_{\alpha,\beta}, \end{aligned}$$

en donde, para simplificar notación, hemos representado los monomios con términos menores por $r_{\alpha,\beta}$.

Se verifican las relaciones siguientes:

$$\mathbf{q}^{(\alpha+\alpha',\beta+\beta')} = \mathbf{q}^{(\alpha,\beta)} \mathbf{q}^{(\alpha,\beta')} \mathbf{q}^{(\alpha',\beta)} \mathbf{q}^{(\alpha',\beta')}.$$

Y como los exponentes pueden ser negativos, utilizando $q_{i,j}^{-1}$, tenemos la relación:

$$\mathbf{q}^{-(\alpha,\beta)} = \mathbf{q}^{(-\alpha,\beta)} = \mathbf{q}^{(\alpha,-\beta)}.$$

Desafortunadamente no se verifican relaciones similares para los $r_{\alpha,\beta}$.

Después de establecer estas reglas vamos a definir el *mínimo común múltiplo* de un par de términos. Si x^α y x^β son dos términos definimos

$$\gamma_i = \max\{\alpha_i, \beta_i\}, \qquad 1 \leq i \leq n.$$

Sea $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{N}^n$, entonces llamamos a x^γ el *mínimo común múltiplo* de x^α y x^β. Tenemos que x^γ es realmente un múltiplo cuando la parte $r_{i,j}$ es siempre nula, ya que se verifica:

$$x^\gamma = \mathbf{q}^{-(\alpha,\gamma-\alpha)} x^{\gamma-\alpha} x^\alpha.$$

Y el resultado análogo para x^β:

$$x^\gamma = \mathbf{q}^{-(\beta,\gamma-\beta)} x^{\gamma-\beta} x^\beta.$$

Con este bagaje vamos a definir las *semisicigias* ó *s–polinomios*. Dados f, y $f \in R$, con $\exp(f) = x^\alpha$ y $\exp(g) = x^\beta$, el s–polinomio definido por f y g es:

$$S(f,g) = \frac{\mathbf{q}^{-(\alpha,\gamma-\alpha)}}{\mathrm{lc}(f)} x^{\gamma-\alpha} f - \frac{\mathbf{q}^{-(\beta,\gamma-\beta)}}{\mathrm{lc}(g)} x^{\gamma-\beta} g.$$

(3.2) Lema.
Se considera la expresión $\sum_{i=1}^{t} c_i x^{\alpha^i} f_i$, *en donde: los* f_i *son elementos de* R, $c_i \in K$ *y* $\alpha^i \in \mathbb{N}^n$, *verificando:*

$$\exp(\sum_i c_i x^{\alpha^i} f_i) < \delta = \exp(x^{\alpha^i} f_i), \text{ para cada índice } i.$$

Entonces existen elementos $c_{jk} \in K$ *y* $g_i \in R$ *tales que:*

$$\exp(g_i) < \alpha^i; \sum_i c_i x^{\alpha^i} f_i = \sum_{jk} c_{jk} x^{\delta-\gamma^{jk}} S(f_j, f_k); \exp(x^{\delta-\gamma^{jk}} S(f_j, f_k)) < \delta,$$

en donde $x^{\gamma^{jk}} = \operatorname{mcm}\{x^{\exp(f_j)}, x^{\exp(f_k)}\}$.

DEMOSTRACIÓN. Supongamos que $\exp(f_i) = \beta^i$, entonces $\alpha^i + \beta^i = \delta$. Hacemos el siguiente desarrollo:

$$\sum_i c_i x^{\alpha^i} f_i = \sum_i c_i \operatorname{lc}(f_i) \frac{x^{\alpha^i} f_i}{\operatorname{lc}(f_i)} = \sum_i c_i \operatorname{lc}(f_i) \mathbf{q}^{(\beta^i, \alpha^i)} h_i,$$

donde $\frac{x^{\alpha^i} f_i}{\operatorname{lc}(f_i)} = \mathbf{q}^{(\beta^i, \alpha^i)} h_i$ Podemos completar este desarrollo de la siguiente forma:

$\sum_i c_i x^{\alpha^i} f_i =$
$\sum_i c_i \operatorname{lc}(f_i) \mathbf{q}^{(\beta^i, \alpha^i)} h_i =$
$c_1 \operatorname{lc}(f_1) \mathbf{q}^{(\beta^1, \alpha^1)} (h_1 - h_2) + (c_1 \operatorname{lc}(f_1) \mathbf{q}^{(\beta^1, \alpha^1)} + c_2 \operatorname{lc}(f_2) \mathbf{q}^{(\beta^2, \alpha^2)})(h_2 - h_3) +$
$\cdots + (c_1 \operatorname{lc}(f_1) \mathbf{q}^{(\beta^1, \alpha^1)} + \cdots + c_{t-1} \operatorname{lc}(f_{t-1}) \mathbf{q}^{(\beta^{t-1}, \alpha^{t-1})})(h_{t-1} - h_t) +$
$(c_1 \operatorname{lc}(f_1) \mathbf{q}^{(\beta^1, \alpha^1)} + \cdots + c_t \operatorname{lc}(f_t) \mathbf{q}^{(\beta^t, \alpha^t)}) h_t.$

Consideramos ahora el producto $x^{\delta-\gamma^{jk}}S(f_j,f_k)$. Vamos a desarrollarlo y ver que tiene como sumando un múltiplo escalar de h_j-h_k.

$$
\begin{aligned}
&x^{\delta-\gamma^{jk}}S(f_j,f_k)=\\
&x^{\delta-\gamma^{jk}}\left(\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}x^{\gamma^{jk}-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}x^{\gamma^{jk}-\beta^k}f_k\right)=\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}x^{\delta-\gamma^{jk}}x^{\gamma^{jk}-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}x^{\delta-\gamma^{jk}}x^{\gamma^{jk}-\beta^k}f_k=\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}\mathbf{q}^{(\gamma^{jk}-\beta^j,\delta-\gamma^{jk})}x^{\delta-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}\mathbf{q}^{(\gamma^{jk}-\beta^k,\delta-\gamma^{jk})}x^{\delta-\beta^k}f_k+\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}r_{\gamma^{jk}-\beta^j,\delta-\gamma^{jk}}x^{\delta-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}r_{\gamma^{jk}-\beta^k,\delta-\gamma^{jk}}x^{\delta-\beta^k}f_k=\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)+(\gamma^{jk}-\beta^j,\delta-\gamma^{jk})}}{\mathrm{lc}(f_j)}x^{\delta-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)+(\gamma^{jk}-\beta^k,\delta-\gamma^{jk})}}{\mathrm{lc}(f_k)}x^{\delta-\beta^k}f_k+\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}r_{\gamma^{jk}-\beta^j,\delta-\gamma^{jk}}x^{\delta-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}r_{\gamma^{jk}-\beta^k,\delta-\gamma^{jk}}x^{\delta-\beta^k}f_k=\\
&\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)+(\gamma^{jk}-\beta^j,\delta-\gamma^{jk})}\frac{x^{\alpha^j}f_j}{\mathrm{lc}(f_j)}-\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)+(\gamma^{jk}-\beta^k,\delta-\gamma^{jk})}\frac{x^{\alpha^k}f_k}{\mathrm{lc}(f_k)}+\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}r_{\gamma^{jk}-\beta^j,\delta-\gamma^{jk}}x^{\delta-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}r_{\gamma^{jk}-\beta^k,\delta-\gamma^{jk}}x^{\delta-\beta^k}f_k=\\
&\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)+(\gamma^{jk}-\beta_j,\delta-\gamma^{jk})+(\beta^j,\alpha^j)}h_j-\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)+(\gamma^{jk}-\beta_k,\delta-\gamma^{jk})+(\beta^j,\alpha^j)}h_k+\\
&\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}r_{\gamma^{jk}-\beta^j,\delta-\gamma^{jk}}x^{\delta-\beta^j}f_j-\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}r_{\gamma^{jk}-\beta^k,\delta-\gamma^{jk}}x^{\delta-\beta^k}f_k=\\
&\mathbf{q}^{(\gamma^{jk},\delta-\gamma^{jk})}(h_j-h_k)+\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}r_{\gamma^{jk}-\beta^j,\delta-\gamma^{jk}}x^{\delta-\beta^j}f_j-\\
&\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}r_{\gamma^{jk}-\beta^k,\delta-\gamma^{jk}}x^{\delta-\beta^k}f_k
\end{aligned}
$$

Entonces tenemos

$$
\begin{aligned}
&\mathbf{q}^{-(\gamma^{jk},\delta-\gamma^{jk})}x^{\delta-\gamma^{jk}}S(f_j,f_k)-\\
&\mathbf{q}^{-(\gamma^{jk},\delta-\gamma^{jk})}x^{\delta-\gamma^{jk}}\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(f_j)}r_{\gamma^{jk}-\beta^j,\delta-\gamma^{jk}}x^{\delta-\beta^j}f_j+\\
&\mathbf{q}^{-(\gamma^{jk},\delta-\gamma^{jk})}x^{\delta-\gamma^{jk}}\frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(f_k)}r_{\gamma^{jk}-\beta^k,\delta-\gamma^{jk}}x^{\delta-\beta^k}f_k=h_j-h_k.
\end{aligned}
$$

Ahora como $\sum_i c_i\,\mathrm{lc}(f_i)\mathbf{q}^{(\beta^i,\alpha^i)}=0$, tenemos:

$$
\begin{aligned}
&\textstyle\sum c_i x^{\alpha^i}f_i=\\
&c_1\,\mathrm{lc}(f_1)\mathbf{q}^{(\beta^1,\alpha^1)}\mathbf{q}^{-(\gamma^{12},\delta-\gamma^{12})}x^{\delta-\gamma^{12}}S(f_1,f_2)+\\
&+(c_1\,\mathrm{lc}(f_1)\mathbf{q}^{(\beta^1,\alpha^1)}+c_2\,\mathrm{lc}(f_2)\mathbf{q}^{(\beta^2,\alpha^2)})\mathbf{q}^{-(\gamma^{23},\delta-\gamma^{23})}x^{\delta-\gamma^{23}}S(f_2,f_3)+\cdots\\
&\cdots+(c_1\,\mathrm{lc}(f_1)\mathbf{q}^{(\beta^1,\alpha^1)}+\cdots+c_{t-1}\,\mathrm{lc}(f_{t-1})\mathbf{q}^{(\beta^{t-1},\alpha^{t-1})})\\
&\mathbf{q}^{-(\gamma^{t-1,t},\delta-\gamma^{t-1,t})}x^{\delta-\gamma^{t-1,t}}S(f_{t-1},f_t)+\text{monomios con térm. menores}.
\end{aligned}
$$

Y tenemos la primera parte del enunciado. Para la segunda parte tenemos en cuenta que cada h_i es un polinomio mónico con $\exp(h_i) = \delta$, entonces $\exp(h_i - h_j) < \delta$ y tenemos el resultado. □

(3.3) Teorema. (Buchberger)
Sea I un ideal izquierda no nulo del anillo R y $\mathbb{G}$ un sistema finito de generadores de I. Son equivalentes los siguientes enunciados:

(a) $\mathbb{G}$ es una base de Groebner de I;

(b) Para un orden fijado de $\mathbb{G}$ y para cada $i \neq j$ se tiene $R(S(g_i, g_j); \mathbb{G}) = 0$.

DEMOSTRACIÓN. (a)⇒(b). Es evidente.

(b)⇒(a). Sea $0 \neq f \in I$, entonces $f = \sum q_i g_i$ y tenemos

$$\exp(f) \leq \max\{\exp(q_i g_i):\ i = 1, \ldots, t\}.$$

Vamos a ver que podemos alcanzar la igualdad. Llamamos:

$$\begin{aligned} &\delta = \max\{\exp(q_i g_i):\ i = 1, \ldots, t\}, \\ &\delta^i = \exp(q_i g_i). \end{aligned}$$

Si $\exp(f) < \delta$, descomponemos f en la siguiente forma:

$$\begin{aligned} f &= \textstyle\sum_i q_i g_i = \\ &= \textstyle\sum_{\delta^i = \delta} q_i g_i + \sum_{\delta^i < \delta} q_i g_i = \\ &= \textstyle\sum_{\delta^i = \delta} \operatorname{lm}(q_i) g_i + \sum_{\delta^i = \delta} (q_i - \operatorname{lm}(q_i)) g_i + \sum_{\delta^i < \delta} q_i g_i. \end{aligned}$$

las dos últimas sumas son "despreciables", ya que su exponente es menor que δ. Vamos a cambiar $\sum_{\delta^i = \delta} \operatorname{lm}(q_i) g_i$ mediante otra expresión. Usando el Lema (3.2) tenemos:

$$\sum_{\delta^i = \delta} \operatorname{lm}(q_i) g_i = \sum c_{jk} x^{\delta - \gamma^{jk}} S(g_j, g_k) + \text{monomios con términos menores,}$$

con $\exp(x^{\delta - \gamma^{jk}} S(g_j, g_k)) < \delta$. Los restos de la división de $S(g_j, g_k)$ por g_1, $\ldots$, g_t son cero, entonces resulta:

$$S(g_j, g_k) = \sum q_{jki} g_i, \text{ con } q_{jki} \in R,$$

y por el algoritmo de la división tenemos:

$$\exp(q_{jki} g_i) \leq \exp(S(g_j, g_k)).$$

Encontramos pues una expresión del siguiente tipo:

$$f = \sum_i q_i' g_i, \text{ con } \exp(q_i' g_i) < \delta.$$

Repitiendo el proceso tantas veces como sea necesario, llegamos a una expresión

$$f = \sum_i q_i g_i,$$

en donde $\exp(f) = \max\{\exp(q_i g_i)\colon\ i = 1, \dots, t\}$, y como consecuencia $\exp(f) = \exp(q_i g_i)$ para algún índice i, esto es:

$$\exp(f) = \exp(q_i g_i) = \exp(q_i) + \exp(g_i) \in \{\exp(g_1), \dots, \exp(g_t\} + \mathbb{N}^n$$

y $\mathbb{G}$ es una base de Groebner. □

Vamos ahora a buscar un mecanismo que nos permita construir una base de Groebner de un ideal a la izquierda I.

(3.4) Teorema. (Algoritmo de Buchberger)
Sea I un ideal izquierda no nulo de R con sistema de generadores $\{f_1, \dots, f_t\}$. Es posible construir una base de Groebner de I siguiendo los siguientes pasos:

(1) Se define $\mathbb{G}_0 = \{f_1, \dots, f_t\}$;

(2) Se define $\mathbb{G}_{n+1} = \cup\{r(S(f,g); \mathbb{G}_n) \neq 0\colon\ f, g \in \mathbb{G}_n\}$.

Entonces cuando $\mathbb{G}_i = \mathbb{G}_{i+1}$, tenemos que $\mathbb{G}_i$ es una base de Groebner de I.

DEMOSTRACIÓN. Dado $\mathbb{G}_0 = \{g_1, \dots, g_t\}$, si $r(S(f,g); \mathbb{G}_0) = 0$ para cada par $f, g \in \mathbb{G}_0$, entonces tenemos una base de Groebner. Si no lo es, existen $f, g \in \mathbb{G}_0$ tales que $r(S(f,g); \mathbb{G}_0) \neq 0$. Llamamos $g_{t+1} = r(S(f,g); \mathbb{G})$. Tenemos que $\mathcal{N}(g_{t+1}) \subseteq \overline{\Delta}$. Entonces, si definimos:

$$\mathbb{G}_{(1)} = \{g_1, \dots, g_t, g_{t+1}\},$$

obtenemos una partición

$$\Delta^1, \dots, \Delta^t, \Delta^{t+1}, \overline{\Delta^{(1)}},$$

siendo $\Delta^{t+1} \cup \overline{\Delta^{(1)}} = \overline{\Delta}$. Si $r(f;\mathbb{G}_0) = 0$, para $f \in R$, entonces $r(f;\mathbb{G}_{(1)}) = 0$. Y en el caso en que $r(S(g_i,g_j),\mathbb{G}_0) = 0$, también se tiene $r(S(g_i,g_j),\mathbb{G}_{(1)}) = 0$.

Si para todo f, $g \in \mathbb{G}_{(1)}$ se verifica $r(S(f,g);\mathbb{G}_{(1)}) = 0$, entonces tenemos una base de Groebner. En el caso contrario tenemos un nuevo $g_{t+2} = r(S(f,g);\mathbb{G}_{(1)}) \neq 0$, y definimos $\mathbb{G}_{(2)} = \{g_1,\ldots,g_{t+1},g_{t+2}\}$, teniendo que $\mathcal{N}(g_{t+2}) \subseteq \overline{\Delta^{(1)}}$.

Si en algún momento encontramos una base de Groebner, ya hemos terminado, en caso contrario tendríamos una cadena ascendente de sistemas de generadores:

$$\mathbb{G}_0 \subset \mathbb{G}_{(1)} \subset \cdots$$

Asociada tenemos una cadena ascendente de monoideales:

$$\exp(\mathbb{G}_0) + \mathbb{N}^n \subset \exp(\mathbb{G}_{(1)}) + \mathbb{N}^n \subset \cdots$$

Como consecuencia del Lema de Dickson esta cadena se estabiliza y por tanto existe un índice n tal que

$$\exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \exp(\mathbb{G}_{(n+1)}) + \mathbb{N}^n,$$

tenemos entonces

$$\exp(g_{t+n+1}) \in \exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \mathbb{N}^n \setminus \overline{\Delta^{(n)}},$$

pero $\exp(g_{t+n+1}) \in \overline{\Delta^{(n)}}$, lo que es una contradicción. □

4. Bases de Groebner reducidas.

En el proceso anterior obtenemos un sistema de generadores que es una base de Groebner, y que tiene, posiblemente, demasiados elementos. Vamos a optimizar el proceso de obtención de una base de Groebner.

(4.1) Lema.
Sea I un ideal izquierda no nulo de $\mathbb{C}_q[X_1,\ldots,X_n]$ y $\mathbb{G} = \{g_1,\ldots,g_t\}$ una base de Groebner de I. Sea $f \in \mathbb{G}$ un polinomio que verifica:

$$\exp(f) \in \{\exp(g):\ f \neq g \in \mathbb{G}\} + \mathbb{N}^n,$$

entonces $\mathbb{G} \setminus \{f\}$ es una base de Groebner de I.

Una base de Groebner $\mathbb{G}$ de un ideal izquierda no nulo I de R se llama *minimal* si verifica:

(i) $\mathrm{lc}(f) = 1$ para cada $f \in \mathbb{G}$;

(ii) $\exp(f) \notin \{\exp(g)\colon\ f \neq g \in \mathbb{G}\} + \mathbb{N}^n$ para cada $f \in \mathbb{G}$.

Simplemente eliminando los elementos que sobran tenemos la siguiente Proposición.

(4.2) Proposición.
Todo ideal izquierda no nulo I de R tiene una base de Groebner minimal.

Un ideal puede tener bases de Groebner minimales distintas. Para buscar la unicidad vamos a introducir las bases de Groebner reducidas. Una base de Groebner $\mathbb{G}$ de un ideal izquierda no nulo I se llama *reducida* si verifica:

(i) $\mathrm{lc}(f) = 1$ para cada $f \in \mathbb{G}$;

(ii) $\mathcal{N}(f) \cap (\{\exp(g)\colon\ f \neq g \in \mathbb{G}\} + \mathbb{N}^n) = \varnothing$.

Es claro que toda base de Groebner reducida de un ideal izquierda no nulo I es una base de Groebner minimal.

(4.3) Teorema.
Cada ideal izquierda no nulo tiene una única base de Groebner reducida.

DEMOSTRACIÓN. Si $\mathbb{G}$ es una base de Groebner minimal, un elemento $f \in \mathbb{G}$ se llama *reducido* si

$$\mathcal{N}(f) \cap (\{\exp(g)\colon\ f \neq g \in \mathbb{G}\} + \mathbb{N}^n) = \varnothing.$$

Si $f \in \mathbb{G}$ es reducido, entonces es reducido en cualquier base de Groebner minimal $\mathbb{G}'$ que lo contenga y que verifique:

$$\{\exp(g)\colon\ g \in \mathbb{G}\} = \{\exp(g)\colon\ g \in \mathbb{G}'\}.$$

Definimos para cada $f \in \mathbb{G}$ los siguientes elementos:

$$f' = R(f, \mathbb{G} \setminus \{f\});$$
$$\mathbb{G}' = (\mathbb{G} \setminus \{f\}) \cup \{f'\}.$$

$\mathbb{G}'$ es también una base de Groebner de I. Si $\exp(f) \neq \exp(f')$, entonces de las relaciones:

$$f = \sum q_g g + R(f; \mathbb{G} \setminus \{f\}) = \sum q_g g + f'$$
$$\exp(f) = \max\{\{\exp(q_g g):\ g \in \mathbb{G} \setminus \{f\}\} \cup \{\exp(f')\}\},$$

y por ser todos los exponentes distintos, se tiene que existe $g \in \mathbb{G} \setminus \{f\}$ tal que $\exp(f) = \exp(q_g g)$, lo que es una contradicción con el hecho de ser $\mathbb{G}$ una base de Groebner minimal. Tenemos entonces que $\mathbb{G}'$ es una base de Groebner y que f' es reducido. Aplicando este proceso a cada uno de los elementos obtenemos una base de Groebner reducida.

Para ver la unicidad, si $\mathbb{G}$ y $\mathbb{G}'$ son dos bases de Groebner reducidas, se verifica:

$$\mathrm{Exp}(I) = \exp(\mathbb{G}) + \mathbb{N}^n = \exp(\mathbb{G}') + \mathbb{N}^n.$$

Dado $f \in \mathbb{G}$ tenemos las relaciones siguientes:

$$\exp(f) = \exp(g') + \gamma, \quad g' \in \mathbb{G}',\ \gamma \in \mathbb{N}^n;$$
$$\exp(g') = \exp(g) + \gamma', \quad g \in \mathbb{G},\ \gamma' \in \mathbb{N}^n;$$

de donde se deduce que $\exp(f) = \exp(g) + \gamma + \gamma'$, y por ser $\mathbb{G}$ minimal tenemos $\gamma = 0 = \gamma'$. Entonces $\exp(f) = \exp(g')$ y como consecuencia tenemos la igualdad:

$$\exp(\mathbb{G}) = \exp(\mathbb{G}').$$

Dado ahora $f \in \mathbb{G}$, existe $g' \in \mathbb{G}'$ tal que $\exp(f) = \exp(g')$. Entonces $f - g'$ tiene todos sus términos menores que $\exp(f)$. Como $f - g' \in I$ tenemos $R(f - g'; \mathbb{G}) = 0$. Como $\mathbb{G}$ y $\mathbb{G}'$ son reducidas y $\exp(\mathbb{G}) = \exp(\mathbb{G}')$, tenemos

$$\mathcal{N}(f - g') \subseteq \overline{\Delta} = \mathbb{N}^n \setminus \mathrm{Exp}(I),$$

Para probar esta inclusión consideramos el siguiente desarrollo:

$$\begin{aligned}
&\mathcal{N}(f - g') \cap (\exp(\mathbb{G}) + \mathbb{N}^n) = \\
&\mathcal{N}(f - g') \cap (\cup\{\exp(L) + \mathbb{N}^n:\ L \in \mathbb{G}\}) = \\
&\cup\{\mathcal{N}(f - g') \cap (\exp(L) + \mathbb{N}^n):\ L \in \mathbb{G}\} = \\
&\cup\{\mathcal{N}(f - g') \cap (\exp(L) + \mathbb{N}^n):\ f \neq L \in \mathbb{G}\} = \\
&\mathcal{N}(f - g') \cap (\{\exp(L):\ f \neq L \in \mathbb{G}\} + \mathbb{N}^n) \subseteq \\
&(\mathcal{N}(f) \cap (\{\exp(L):\ f \neq L \in \mathbb{G}\} + \mathbb{N}^n)) \cup \\
&\mathcal{N}(g') \cap (\{\exp(L):\ g' \neq L \in \mathbb{G}'\} + \mathbb{N}^n)) = \varnothing
\end{aligned}$$

Entonces $R(f - g'; \mathbb{G}) = f - g'$, de donde $f = g'$. □

Capítulo 5

Aplicaciones.

Vamos a dedicar este Capítulo a las aplicaciones de la teoría de bases de Groebner hasta ahora desarrollada. En primer lugar estudiamos las aplicaciones clásicas de las bases de Groebner en orden a calcular con elementos en el anillo R.

La última parte del Capítulo la dedicamos al cálculo de la dimensión de Gelfand–Kirillov en algunos ejemplos de anillos noetherianos.

1. Aplicaciones de las bases de Groebner.

Problema de pertenencia.

(1.1) Problema.
Sea I un ideal izquierda de R con un sistema de generadores $\{f_1, \ldots, f_r\}$; dado $f \in R$, nos planteamos el problema de determinar si $f \in I$.

Esto se hace como sigue: se calcula una base de Groebner $\mathbb{G} = \{g_1, \ldots, g_t\}$ de I; entonces tenemos $f \in I$ si, y sólo si, $r(f; \mathbb{G}) = 0$.

Es posible también obtener una expresión de f como combinación lineal de los generadores originales $f_1, \ldots, f_r$. Para ello únicamente hay que tener en cuenta que, por el algoritmo de la división, tenemos una expresión de la forma:

$$f = q_1 g_1 + \cdots + q_t g_t,$$

y como los g_i se obtienen haciendo s–polinomios a partir de los f_j, tenemos que es posible dar la expresión deseada.

Igualdad de ideales.

(1.2) Problema.
Sean I_1 e I_2 ideales izquierda de R con sistemas de generadores $\{f_1^1, \ldots, f_{r_1}^1\}$ y $\{f_1^2, \ldots, f_{r_2}^2\}$, respectivamente. El problema es determinar cuando $I_1 = I_2$. .

Conseguimos bases de Groebner reducidas $\mathbb{G}_1$ y $\mathbb{G}_2$ de I_1 e I_2, respectivamente. Por la unicidad de las bases de Groebner reducidas, tenemos $I_1 = I_2$ si, y sólo si, $\mathbb{G}_1 = \mathbb{G}_2$.

Representantes canónicos.

(1.3) Problema.
Dado un ideal I de R el problema es dar un criterio, y un método, para determinar un representante canónico en cada clase del cociente R/I.

En primer lugar, dado I, construimos una base de Groebner $\mathbb{G}$ de I. Para cada $f \in R$ consideramos el resto $r(f;\mathbb{G})$ y es claro que se verifica:

$$f + I = r(f;\mathbb{G}) + I.$$

Además, $r(f,\mathbb{G})$ es único verificando la igualdad anterior y $\mathcal{N}(r(f;\mathbb{G})) \subseteq \overline{\Delta} = \mathbb{N}^n \setminus \mathrm{Exp}(I)$, ver Proposición (2.5). Este elemento $r(f;\mathbb{G})$ lo llamamos la forma normal de la clase de f con respecto a $\mathbb{G}$.

El comportamiento de la forma normal es bueno respecto a combinaciones K–lineales, ya que si $a_1, a_2 \in K$ y $f_1, f_2 \in K$, entonces se verifica: $r(a_1f_1 + a_2f_2;\mathbb{G}) = a_1r(f_1;\mathbb{G}) + a_2r(f_2;\mathbb{G})$. Es claro que por el algoritmo de la división tenemos:

$$f_i = q_1^i g_1 + \cdots + q_t^i g_t + r(f_i;\mathbb{G}),$$

entonces se verifica:

$$\begin{aligned} &a_1f_1 + a_2f_2 = \\ &a_1q_1^1g_1 + \cdots + a_1q_t^1g_t + a_1r(f_1;\mathbb{G}) + a_2q_1^2g_1 + \cdots + a_2q_t^2g_t + a_2r(f_2;\mathbb{G}) = \\ &(a_1q_1^1 + a_2q_1^2)g_1 + \cdots + (a_1q_t^1 + a_2q_t^2)g_t + a_1r(f_1;\mathbb{G}) + a_2r(r_2;\mathbb{G}), \end{aligned}$$

de donde tenemos el resultado, ya que

$$\mathcal{N}(a_1 r(f_1;\mathbb{G}) + a_2 r(r_2;\mathbb{G})) \subseteq \mathbb{N}^n \setminus \mathrm{Exp}(I),$$

y por tanto $r(a_1 f_1 + a_2 f_2;\mathbb{G}) = a_1 r(f_1;\mathbb{G}) + a_2 r(f_2;\mathbb{G})$. Tenemos entonces, para cualesquiera f_1, $f_2 \in R$, las equivalencias entre los siguientes enunciados:

$$\begin{array}{l} f_1 + I = f_2 + I; \\ f_1 - f_2 \in I; \\ r(f_1 - f_2;\mathbb{G}) = 0; \\ r(f_1;\mathbb{G}) = r(f_2;\mathbb{G}). \end{array}$$

Como consecuencia, cada elemento de R/I está unívocamente determinado, y determina, un elemento r de K con $\mathcal{N}(r) \subseteq \mathbb{N}^n \setminus \mathrm{Exp}(I)$. Para estos elementos las operaciones en R/I están definidas exactamente por estos representantes por la regla:

$$a_1(r_1 + I) + a_2(r_2 + I) = (a_1 r_1 + a_2 r_2) + I.$$

Ideales izquierda cofinitos.

Pasamos ahora a estudiar el caso de ideales cofinitos, esto es, ideales a la izquierda I de R tales que el cociente R/I es de dimensión finita como K–espacio vectorial.

K–base del cociente.

(1.4) Problema.
Se trata de dar un método que permita calcular una base del cociente R/I.

Para cada clase de R/I, considerando una base de Groebner de I, tenemos un representante r de la clase $f + I$ tal que $\mathcal{N}(r) \subseteq \mathbb{N}^n \setminus \mathrm{Exp}(I)$. De aquí resulta que r se puede escribir en la forma

$$r = \sum_{\alpha} c_\alpha x^\alpha,$$

con $\alpha \notin \{\exp(g)\colon\ g \in \mathbb{G}\} + \mathbb{N}^n = \mathrm{Exp}(I)$ y $c_\alpha \in K$. Tenemos entonces que $\{x^\beta\colon\ \beta \in \mathbb{N}^n \setminus \mathrm{Exp}(I)\}$ es un sistema de generadores linealmente independiente de R/I; esto resuelve el problema.

Como subproducto podemos determinar cuándo un ideal a la izquierda es cofinito; lo es si, y sólo si, el cardinal del conjunto $\mathbb{N}^n \setminus \mathrm{Exp}(I)$ es finito. Este resultado lo mejoraremos más adelante al estudiar la dimensión de Gelfand–Kirillov de los cocientes R/I.

Operaciones en el cociente.

(1.5) Problema.
Dar un criterio que permita calcular las operaciones en el cociente R/I cuando I es un ideal bilátero (cofinito) de R.

Supuesto que I es un ideal bilátero cofinito, las clases del cociente $S = R/I$ tienen una K–base finita, y como S es un anillo, tenemos un producto interno en S. Pero S es una K–álgebra finito–dimensional, luego este producto se puede describir completamente en términos de los productos de los elementos de una K–base. El cálculo se realiza considerando una base de Groebner $\mathbb{G}$ y calculando los restos de la división por $\mathbb{G}$.

Caracterización de ideales cofinitos.

Ya conocemos que un ideal a la izquierda I de R es cofinito si, y sólo si, $\mathbb{N}^n \setminus \mathrm{Exp}(I)$ es finito. Vamos a buscar una caracterización más sencilla.

(1.6) Proposición.
Sea I un ideal a la izquierda de R con base de Groebner reducida $\mathbb{G}$. Son equivalentes los siguientes enunciados:

(a) I es cofinito;

(b) Para cada indeterminada x_i existen $g_j \in \mathbb{G}$ y $\nu_i \in \mathbb{N}$ tales que $\mathrm{lm}(g_j) = x_i^{\nu_i}$.

DEMOSTRACIÓN. (a)⇒(b). Como I es cofinito, dado x_i existe $\nu_i \in \mathbb{N}$ tal que $x_i^{\nu_i}$ es el término líder de un polinomio en I, entonces $(0,\ldots,\nu_i,\ldots,0) \in \mathrm{Exp}(I) = \exp(\mathbb{G}) + \mathbb{N}^n$. Llamemos $\alpha^j = \exp(g_j)$ para cada $g_j \in \mathbb{G}$. Existen $j \in \{1,\ldots,t\}$ y $\gamma \in \mathbb{N}^n$ tales que

$$(0,\ldots,\nu_i,\ldots,0) = \alpha^j + \gamma,$$

entonces $\alpha_h^j = 0 = \gamma_h$ si $h \neq i$. Luego $\exp(g_j) = (0\ldots,\mu_i,\ldots,0)$ para algún $\mu_i \in \mathbb{N}$, esto es, $\mathrm{lm}(g_j) = x_i^m$ para algún $m \in \mathbb{N}$.

(b)⇒(a). Consideramos $\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(I)$. Por hipótesis, para cada x_i existe g_j tal que $\mathrm{lt}(g_j) = x_i^{\nu_i}$. Si $\alpha_i \geq \nu_i$, entonces tenemos una expresión del siguiente tipo:

$$\alpha = (0, \ldots, \nu_i, \ldots, 0) + (\alpha_1, \ldots, \alpha_i - \nu_i, \ldots, \alpha_n) \in \exp(g_j) + \mathbb{N}^n \subseteq \mathrm{Exp}(I),$$

lo que es una contradicción, y por tanto necesariamente $\alpha_i < \nu_i$, para cada índice *i*. En consecuencia existe un número finito de elementos $\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(I)$ y por tanto I es cofinito. □

2. Dimensión de Gelfand–Kirillov.

Vamos a aplicar la teoría de bases de Groebner al cálculo de la dimensión de Gelfand–Kirillov de un cociente R/I del anillo R por un ideal a la izquierda I.

Para referencias sobre la dimensión de Gelfand–Kirillov y la función de Hilbert se puede consultar el libro de McConnell y Robson [17].

Ya que I es un ideal a la izquierda de R y R es una K–álgebra triangular verificando la condición de PBW; tenemos, siguiendo la notación de las secciones precedentes, un sistema de generadores de R formado por $x_1, \ldots, x_n$, entonces $x_1 + I, \ldots, x_n + I$ es un sistema de generadores de R/I. Si llamamos W al subespacio de R generado por los $x_1, \ldots, x_n$, y definimos por recurrencia $W^{m+1} = WW^m$, para cada $m \in \mathbb{N}$ y $W^0 = \{1\}$. Podemos definir por recurrencia la *función de Hilbert* H_I de R/I; $H_I(m) = \dim_K(W^m + I/I)$, para cada $m \in \mathbb{N}$. La *dimensión de Gelfand–Kirillov* es la medida del crecimiento de la función de Hilbert, esto es:

$$\mathrm{GKdim}(R/I) = \inf\{r\colon\ H_I(m) \leq m^r, \text{ para } m >> 0\}.$$

si el crecimiento de H_I es polinomial e infinito en caso contrario. La definición de dimensión de Gelfand–Kirillov es independiente del subespacio generador que se considere, no así la definición de la función de Hilbert.

Por ser R una K–álgebra triangular verificando la condición de PBW y por estar considerando en $\mathbb{N}^n$ un orden graduado, el lexicográfico graduado, se obtiene fácilmente la siguiente Proposición.

(2.1) Proposición.
Para cada $f \in R$ son equivalentes los siguientes resultados:

(a) $f \in W^m$;

(b) $\mathrm{gr}(f) \leq m$.

Como una aplicación directa del problema de determinar la dimensión de un cociente para un ideal cofinito obtenemos también de forma inmediata el siguiente resultado:

(2.2) Proposición.
Con las notaciones anteriores se obtiene:

(1) $\dim_K(W^m) = \mathrm{Card}\{\alpha \in \mathbb{N}^n\colon\ \sum_i \alpha_i \leq m\}$;

(2) $\dim_K(W^m) = \mathrm{Card}\{\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(I)\colon\ \sum_i \alpha_i \leq m\}$;

Como consecuencia, para al cálculo de la dimensión de Gelfand–Kirillov de un cociente R/I basta analizar, según la proposición anterior, los cardinales de los subconjuntos de $\mathbb{N}^n$. En este punto conviene destacar que podríamos, sin ninguna restricción abordar el problema del cálculo de la dimensión para un cociente $K[X_1, \ldots, X_n]/J$ del anillo de polinomios en indeterminadas conmutativas. Obtenemos en este caso que la dimensión de Gelfand–Kirillov de $K[X_1, \ldots, X_n]/J$ se calcula considerando el sistema de generadores $X_1, \ldots, X_n$; llamemos W_c al K–subespacio vectorial de $K[X_1, \ldots, X_n]$ generado por $X_1, \ldots, X_n$, entonces se tiene:

$$\dim_K(W_c^m + J/J) = \mathrm{Card}\{\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(J)\colon\ \sum_i \alpha_i \leq m\};$$

de forma que tenemos un nexo de unión entre la dimensión de Gelfand–Kirillov de R/I y la de $K[X_1, \ldots, X_n]/J$ para un J adecuado.

El proceso a seguir es el siguiente: Dado el ideal I de R definimos $\mathrm{Exp}(I) \subseteq \mathbb{N}^n$, el monoideal asociado. A cada monoideal M de $\mathbb{N}^n$ le podemos asociar un ideal J_M de $K[X_1, \ldots, X_n]$ definiendo:

$$J_M = \{X^\alpha\colon\ \alpha \in M\}.$$

Si definimos $J = J_{\mathrm{Exp}(I)}$, tenemos entonces el siguiente resultado:

(2.3) Teorema.
Con la notación anterior se verifica:

$$\mathrm{GKdim}(R/I) = \mathrm{GKdim}(K[X_1, \ldots, X_n]/J)$$

Como consecuencia, el estudio de la dimensión de Gelfand–Kirillov en álgebras triangulares verificando la condición de PBW se reduce completamente al estudio de la dimensión de Gelfand–Kirillov en álgebras afines conmutativas, esto es, al estudio de la dimensión de Krull.

Como consecuencia podemos calcular la dimensión de Gelfand–Kirillov de cualquier R–módulo finitamente generado. Ver [15].

Bibliografía

[1] W. W. Adams y P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, 3, American Mathematical Society, 1994.

[2] T. Becker y V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra*, Graduate texts in Mathematics, 141, Springer–Verlag, 1993.

[3] A. D. Bell, *Notes on localization in noncommutative noetherian rings*, Cuadernos de Álgebra, 9, Universidad de Granada, 1988.

[4] R. Berger, *The quantum Poincaré–Birkhoff–Witt theorem*, Commun. Math. Phys. **143** (1992), 215–234.

[5] K. A. Brown y K. R. Goodearl, *A Hilbert basis theorem for quantum groups*, Glasgow, 1996.

[6] J. L. Bueso, F. Castro, y P. Jara, *Effective computation of the Gelfand–Kirillov dimension*, Proc. Edinburgh Math. Soc. (1997), 8 pp.

[7] D. Cox, J. J. Little, y D. O'Shea, *Ideals, varieties and algorithms*, Undergraduate Texts in Math., Springer–Verlag, 1992.

[8] T. Gateva-Ivanova, *Noetherian properties of skew polynomial rings with binomial relations*, Trans. Amer. Math. Soc. **343** (1994), 203–219.

[9] ———, *Skew polynomial rings with binomial relations*, J. Algebra **185** (1996), 710–753.

[10] K. R. Goodearl, *Prime ideals in skew polynomial rings and quantized Weyl algebras*, J. Algebra **150** (1992), 324–377.

[11] K. R. Goodearl y E. S. Letzter, *Prime factor algebras of the coordinate ring of quantum matrices*, Proc. Amer. Math. Soc. **121** (1994), 1017–1025.

[12] P. Jara y J. Jódar, *An example of bernstein duality*, To appear in Advances in Math. Granada, 1998.

[13] A. Kandri-Rodi y V. Weispfenning, *Non–commutative Gröbner bases in algebras of solvable type*, J. Symb. Comp. **9** (1990), 1–26.

[14] T. Levasseur y J. T. Stafford, *The quantum coordinate rings of the special linear group*, J. Pure Appl. Algebra **86** (1993), 181–186.

[15] M. Lorenz, *Gelfand–Kirillov dimension and Poincaré series*, Cuadernos de Algebra, 7, Univ. Granada, 1988.

[16] J. C. McConnell, *Quantum groups, filtered rings and Gelfand–Kirillov dimension*, Lect. Notes in Math. **1448** (1991), 139–149.

[17] J. C. McConnell y J. C. Robson, *Non commutative noetherian rings*, John Wiley, 1987.

[18] J. C. McConnell y J. T. Stafford, *Gelfand–Kirillov dimension and associated graded modules*, J. Algebra **125** (1989), 197–214.

[19] T Mora y L. Robbiano, *The groebner fan of an ideal*, J. Symb. Comp. **6** (1989), 49–74.

[20] Sei-Qwon Oh, *Finite dimensional simple modules over the coordinate ring of quantum matrices*, Bull. London Math. Soc. **25** (1993), 427–430.

[21] M. Pesch, *Left and right gröbner bases in ore extensions of polynomial rings*, Univ. Passau, 1996.

[22] L. Robbiano, *Term orderings on the polynomial ring*, Lect. Notes in Computer Science **204** (1985), 513–517.

[23] ———, *On the theory of graded structures*, J. Symb. Comp. **2** (1986), 139–170.

Índice de Materias