Sección de Matemáticas
Universidad de La Laguna

Enrique José Padrón Alemán

Semigrupos numéricos e ideales asociados.

Numerical semigroups and associated ideals.

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, junio de 2019

Dirigido por
Ignacio García Marco

Ignacio García Marco
Matemáticas, Estadística e Investigación Operativa
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A Nacho, por su inagotable paciencia y todo el apoyo brindado en el desarrollo de este trabajo.

A mi familia, por brindarme la oportunidad de aventurarme en el mundo de las Matemáticas.

A Cory, mi hermana de otra madre, por creer en mí cuando ni yo mismo creía.

A Fabrizio, por los cafés eternos, las quejas, las risas y las discusiones por culpa de los teoremas.

Y por último, a La Sede y todos los que han pasado por ella: Adrián, Luis, Johanna, Walkiria, Andrea, Cynthia, Sergio...

A todos vosotros, **gracias**.

Enrique José Padrón Alemán
La Laguna, 10 de junio de 2019

Resumen · Abstract

Resumen

El objetivo de esta memoria es introducir al lector a la Teoría de Semigrupos Numéricos y de Bases de Gröbner, mostrando alguna interacción entre ellas. En primer lugar estudiamos la estructura de semigrupo numérico. Demostramos que todo semigrupo numérico está finitamente generado y tiene un único sistema minimal de generadores. También estudiamos diversos conjuntos notables asociados como el conjunto de Apéry y el de huecos. En el segundo capítulo estudiamos la teoría clásica de Bases de Gröbner. Comenzamos introduciendo un orden monomial en el anillo de polinomios sobre un cuerpo, lo que nos permite descubrir un algoritmo de división que generaliza la división euclídea y, haciendo uso del mismo, hallar sistemas generadores de ideales con propiedades deseables. Finalmente, afrontamos dos problemas de la Teoría de Semigrupos: el de pertenencia a un semigrupo y el de obtención del conjunto de Apéry, ambos empleando las herramientas que brindan las bases de Gröbner.

Palabras clave: *Semigrupos numéricos – Conjunto de Apéry – Orden monomial – Algoritmo de división– Base de Gröbner.*

Abstract

This manuscript aims to introduce the reader to both Numerical Semigroups and Gröbner Bases theories, showing some interactions between them. In the first chapter, we study the structure of numerical semigroup. We prove that every numerical semigroup is finitely generated and has a unique minimal set of generators. We also study several relevant sets associated to the semigroup as the Apéry set and the set of gaps. In the second chapter, we study classical Gröbner Bases theory defining a monomial order in the polynomial ring over a field. We describe a division algorithm which allows us to generalise the Euclidean division and we use this tool to find generating systems for ideals with reasonably good properties. Finally, we approach two problems of Numerical Semigroups theory: the semigroup membership problem and the computation of the Apéry set, both of them applying tools given by Gröbner bases.

Keywords: *Numerical semigroups – Apéry Set – Monomial order – Division algorithm – Gröbner Basis.*

Contenido

Introducción

La Teoría de Semigrupos Numéricos surge con el estudio de las Ecuaciones Diofánticas. En particular, con la búsqueda de soluciones naturales de ecuaciones de la forma $a_1x_1 + \cdots + a_nx_n = b$, donde $a_1, \ldots, a_n, b \in \mathbb{N}$. Ferninand Fröbenius, matemático alemán, observó que si $a_1, \ldots, a_n$ son primos entre sí, esta ecuación tiene soluciones para todo valor de b suficientemente grande. Además, dedicó parte de sus investigaciones a averiguar cuál es el mayor valor que puede tomar b para que la ecuación no tenga soluciones. Cuando $n = 2$, este problema fue resuelto por diversos matemáticos, entre ellos James Sylvester en 1884 [7] y desde entonces se bautizó esta cuestión como el problema de Fröbenius.

Por otra parte, la Teoría de Bases de Gröbner, de más reciente creación, nace en 1965 en el campo del Álgebra Computacional de manos de Bruno Buchberger y con el objetivo de resolver sistemas de ecuaciones polinomiales. En su Tesis Doctoral [1], el autor establece el concepto de Base de Gröbner como un sistema generador de un ideal en el anillo de polinomios con propiedades deseables. Además, diseña un algoritmo para computarlas.

El fin último de esta memoria es introducir al lector tanto en la Teoría de Semigrupos Numéricos como en la Teoría de Bases de Gröbner así como mostrar las interacciones existentes entre estas. Se encuentra dividida en tres capítulos y un apéndice.

El primer capítulo trata con profundidad la estructura de semigrupo numérico y se presentan varios problemas relacionados con esta estructura como son: el problema de pertenencia a un semigrupo, el cálculo de sistemas generadores y el cálculo del número de Fröbenius y del tipo del semigrupo. Tras esto, se introduce el objeto principal de este capítulo: el conjunto de Apéry. Veremos cómo el conocimiento de este conjunto resuelve todos los problemas anteriores.

El capítulo está inspirado en [3] y [6] si bien en este trabajo se estudian los semigrupos desde una perspectiva diferente, explotando el orden parcial sobre $\mathbb{Z}$ inducido por un semigrupo numérico.

En el segundo capítulo se estudia la teoría clásica de Bases de Gröbner. La referencia principal es [2]. Sin embargo, en esta memoria se toma como punto de partida el Teorema de la Base de Hilbert, lo cual permite presentar la teoría de forma más concisa. Comenzamos introduciendo la noción de orden monomial y se generaliza la división de polinomios al caso de varias variables, para posteriormente presentar un algoritmo de cálculo de bases de Gröbner de un ideal y tratar diversas aplicaciones de estas.

En el tercer capítulo se conectan las dos teorías anteriores. Afrontamos el problema de pertenencia a un semigrupo numérico y el cálculo del conjunto de Apéry con respecto a un elemento del semigrupo. Estos problemas han sido estudiados en [5], aunque en esta memoria se presentan pruebas elementales empleando propiedades específicas de los ideales monomiales y binomiales.

Por último, en el apéndice se presenta una implementación de dos rutinas en lenguaje `Singular` [4]: la primera de ellas, `PerteneceSemig` permite determinar si un número natural pertenece o no a un semigrupo numérico, dados sus generadores. La segunda, llamada `Apery` computa el conjunto de Apéry de un semigrupo numérico respecto a uno de sus elementos.

1

Semigrupos numéricos

En este primer capítulo introduciremos los conceptos más básicos de la teoría de monoides. Posteriormente, nos centraremos en la estructura de interés de este trabajo: el semigrupo numérico. Estableceremos una relación de orden parcial en este tipo de monoides que nos permitirá estudiar con sencillez los sistemas de generadores minimales así como sus elementos más notables.

1.1. Monoides y homomorfismos

En primer lugar se presenta una serie de definiciones esenciales para conocer la estructura con la que se tratará a lo largo de este trabajo.

Definición 1.1. *Sea S un conjunto y $+$ una ley de composición interna. Diremos que el par $(S,+)$ es un monoide si se verifican las siguientes propiedades:*

1. ***Propiedad asociativa**: $\forall x,y,z \in S$, se tiene que $x+(y+z)=(x+y)+z$.*
2. ***Existencia de elemento neutro**: $\exists e \in S$ tal que $\forall m \in S$, se tiene que $e+m=m+e=m$. Al elemento neutro de S lo denotaremos por 0_S o simplemente 0 cuando no haya lugar a confusión.*

*Si además $(S,+)$ verifica la propiedad **conmutativa**, diremos que es un monoide abeliano.*

Definición 1.2. *Sea $(S,+)$ un monoide y T un subconjunto de S. Diremos que T es un submonoide de S si $(T,+)$ es nuevamente un monoide y $0_S \in T$.*

Los submonoides poseen las propiedades habituales de las subestructuras algebraicas (como subgrupos e ideales), en tanto que la intersección de submonoides resulta ser un submonoide y sin embargo la unión de estos no conserva necesariamente la estructura de monoide.

Nota:. Denotaremos $\lambda a = a + \overset{\lambda}{\cdots} + a$ para $\lambda \in \mathbb{N}$, $a \in S$.

Definición 1.3. *Sea S un monoide y A un subconjunto de S. Se define el submonoide de S generado por A, denotado por $\langle A \rangle$ como sigue:*

$$\langle A \rangle = \{\lambda_1 a_1 + \cdots + \lambda_n a_n : \lambda_i \in \mathbb{N}, a_i \in A, 1 \leq i \leq n\}$$

En este caso, diremos que A es sistema generador de S. Además, si A tiene un número finito de elementos, diremos que $\langle A \rangle$ está finitamente generado.

Una vez presentada esta estructura, es natural definir los morfismos que las relacionan. Por ello, se presenta a continuación la definición de homomorfismo de monoides.

Definición 1.4. *Sean $(S, +)$ y $(T, +)$ monoides y $f : S \to T$ una aplicación entre ellos. Diremos que f es un homomorfismo de monoides si se verifica que:*

1. $f(x + y) = f(x) + f(y)\ \forall x, y \in S$
2. $f(0_S) = 0_T$

De la manera usual, diremos que este homomorfismo será un isomorfismo si es biyectivo. De darse esto, escribiremos $S \cong T$.

1.2. Semigrupos numéricos

En esta memoria siempre trabajaremos con submonoides S de $(\mathbb{N}, +)$, los números naturales con la operación suma usual. Por tanto, dicho submonoides serán abelianos.

A continuación presentamos el concepto de semigrupo numérico, el objeto central de este trabajo:

Definición 1.5. *Sea S un submonoide de $\mathbb{N}$, diremos que S es un semigrupo numérico si $\mathbb{N} - S$ es finito.*

Observación 1.6. Cuando describamos un semigrupo numérico S, como $\mathbb{N} - S$ es finito, a partir de un cierto elemento en adelante todos los números naturales pertenecerán a S. Con el fin de compactar la notación, escribiremos $\to$ cuando ocurra esto. Por ejemplo, en

$$S = \{0, 5, 7, 9, 10, 12, 14, \to\}$$

están todos los números naturales mayores que 14.

Vamos a caracterizar los semigrupos numéricos como aquellos submonoides de los naturales finitamente generados por un conjunto de enteros primos entre sí.

Proposición 1.7. *Sea $A \subseteq \mathbb{N}$ finito. Entonces,*

$$\langle A\rangle \text{ semigrupo numérico} \iff mcd(A) = 1.$$

Demostración. " $\Rightarrow$ "Procedemos por contrarrecíproco y reducción al absurdo. Denotamos $d \coloneqq mcd(A)$ y suponemos que $d \neq 1$. Además, afirmamos que $A \subseteq \langle d\rangle$. En efecto, si $x \in A$ como d es el máximo común divisor de A, entonces $d \mid x$ y por tanto $x \in \langle d\rangle$. De esta inclusión deducimos tomando complementarios que $\mathbb{N} - \langle A\rangle \supseteq \mathbb{N} - \langle d\rangle$. Supongamos ahora que $d \neq 1$. Entonces, $\mathbb{N} - \langle d\rangle = \mathbb{N} - \{\alpha d : \alpha \in \mathbb{N}\}$ que es claramente un conjunto infinito. Tendríamos entonces por la última inclusión que un conjunto finito tiene un subconjunto infinito, lo cual es absurdo. Por tanto, $d = 1$.

" $\Leftarrow$ " Dado que A es finito, podemos escribir $A = \{a_1, \ldots, a_n\}$ donde $a_1 < \ldots < a_n$. Por hipótesis $mcd(A) = 1$, luego por la identidad de Bézout, $1 = \alpha_1 a_1 + \cdots + \alpha_n a_n$ con $\alpha_i \in \mathbb{Z}, 1 \leq i \leq n$.

Tenemos que ver que $\mathbb{N} - \langle A\rangle$ es finito, lo que equivale a que exista un M tal que $\forall x > M, x \in \langle A\rangle$. Tomamos $M = |a_1\alpha_1|\, a_1 + \cdots + |a_1\alpha_n|\, a_n$. Claramente $M \in \langle A\rangle$ pues $|a_1\alpha_i|\, a_i \in \mathbb{N}$ y $a_i \in A$ para $1 \leq i \leq n$. Veamos que $M + k \in \langle A\rangle$ para $1 \leq k \leq a_1 - 1$. Por la identidad de Bézout, $k = k\alpha_1 a_1 + \cdots + k\alpha_n a_n$. Por tanto, $M + k = (|a_1\alpha_1| + k\alpha_1)\, a_1 + \cdots + (|a_1\alpha_n| + k\alpha_n)\, a_n$ que claramente pertenece a $\langle A\rangle$.

Por último, si tenemos que $k \geq a_1$, podemos realizar la división entre a_1 y escribir $k = qa_1 + r$, con $0 \leq r < a_1$. Entonces, $M + k = M + qa_1 + r = (M + r) + qa_1$ que resulta ser un elemento de $\langle A\rangle$. □

Teorema 1.8 (Caracterización de semigrupos numéricos). *Sea S un submonoide de $\mathbb{N}$. Entonces,*

$$S \text{ semigrupo numérico} \iff \exists A \subseteq \mathbb{N} \text{ finito tal que } S = \langle A\rangle \text{ y } mcd(A) = 1.$$

Demostración. " $\Leftarrow$ " Directo de la Proposición 1.7.

" $\Rightarrow$ " Como S es semigrupo numérico, $\mathbb{N} - S$ es finito, luego existe $M > 2$ tal que $\forall x \geq M$, $x \in S$. Sea $A \coloneqq \{x \in S : x < M\} \sqcup \{M, M + 1, \ldots, 2M - 1\}$. Cada uno de los conjuntos contemplados en la unión es finito, y $mcd(A) = 1$ pues $mcd(M, M + 1) = 1$. Queda demostrar que $\langle A\rangle = S$.
" $\subseteq$ " Trivial, pues si $A \subseteq S$, es claro que $\langle A\rangle \subseteq S$.
" $\supseteq$ " Sea $x \in S$. Si $x < M$ es evidente que $x \in A \subseteq \langle A\rangle$. Supongamos ahora que $x \geq M$. Podemos entonces realizar la división euclídea entre de x entre M y escribir $x = qM + r$ con $q \geq 1$ y $0 \leq r < M$. Entonces, tenemos que $x = qM + r = (q - 1)M + (M + r)$ y como $M \in A$ y $M + r \in A$, entonces $x \in A$ y consecuentemente $x \in \langle A\rangle$. □

En esta memoria centramos nuestra atención en los semigrupos numéricos. No obstante, como muestra la siguiente proposición, en realidad estamos estudiando cualquier submonoide de $(\mathbb{N}, +)$ pues todo submonoide de esta forma es isomorfo a un semigrupo numérico.

Proposición 1.9. *Sea S un submonoide de $\mathbb{N}$, $S \neq \{0\}$. Entonces, S es isomorfo a un semigrupo numérico.*

Demostración. Consideramos S submonoide de $\mathbb{N}$ con $S \neq \{0\}$. Además, definimos el conjunto $G = \{x - y : x, y \in S\} \subseteq \mathbb{Z}$.

Si tomamos $z_1, z_2 \in G$ tenemos que $z_i = x_i - y_i$, con $x_i, y_i \in S$, $i \in \{1, 2\}$. Así, $z_1 - z_2 = x_1 + y_2 - (x_2 + y_1) \in G$. Por el teorema de caracterización de subgrupos tenemos que G es subgrupo de $\mathbb{Z}$ y como $\mathbb{Z}$ es cíclico, G también lo es. Por tanto, podemos escribir $G = d\mathbb{Z}$ con $d \in \mathbb{N}$. En particular, como $S \neq \{0\}$, entonces $H \neq \{0\}$ y por tanto $d \geq 1$.

Sea $M = \{s/d : s \in S\}$. Claramente M es un submonoide de $\mathbb{N}$. Definimos a continuación la correspondencia entre monoides $f : S \longrightarrow M$ donde $f(s) = s/d$. Es sencillo comprobar que, en efecto f es un isomorfismo de monoides.

Veamos que M es un semigrupo numérico. Como $d \in M$, $d = x - y$ con $x, y \in S$ luego $1 = \frac{x}{d} - \frac{y}{d}$ con $x/d, y/d \in M$. Así, tenemos que $\langle x/d, y/d \rangle \subseteq M$ y en consecuencia $\mathbb{N} - M \subseteq \mathbb{N} - \langle x/d, y/d \rangle$. Por la proposición 1.7 y como $mcd(x/d, y/d) = 1$ se tiene que $\mathbb{N} - \langle x/d, y/d \rangle$ es finito luego $\mathbb{N} - M$ también lo es y concluimos que M es semigrupo numérico. □

Corolario 1.10. *Todo submonoide de $\mathbb{N}$ está finitamente generado.*

Demostración. Sea S un submonoide de $\mathbb{N}$. Si $S = \{0\}$, entonces $S = \langle 0 \rangle$. En caso contrario, por la Proposición 1.9, existe un semigrupo numérico M y un $d \in \mathbb{Z}^+$ tal que $f : S \longmapsto M$ definido por $f(s) = s/d$ es isomorfismo de monoides. Como M es semigrupo numérico, en virtud del Teorema 1.8, tenemos que $M = \langle a_1, \ldots, a_n \rangle$ luego es evidente que $S = \langle da_1, \ldots, da_n \rangle$. □

1.3. El orden parcial inducido por un semigrupo numérico

Vamos a estudiar cómo todo semigrupo numérico S dota a $\mathbb{Z}$ de una estructura de orden parcial. En este capítulo explotaremos dicha estructura para estudiar el semigrupo en cuestión.

Definición 1.11. *Sea $A \neq \emptyset$ y $\leq$ una relación binaria en A. Diremos que $\leq$ es una relación de orden (u orden parcial) si verifica las siguientes propiedades:*

1. ***Reflexiva**: $\forall x \in A, x \leq x$.*
2. ***Antisimétrica**: $\forall x, y \in A$, si $x \leq y, y \leq x$, entonces $x = y$.*
3. ***Transitiva**: $\forall x, y, z \in A$, si $x \leq y, y \leq z$, entonces $x \leq z$.*

En caso de que $\leq$ sea, efectivamente, una relación de orden, diremos que el par $(A, \leq)$ es un conjunto (parcialmente) ordenado. Además, diremos que $(A, \leq)$ está totalmente ordenado si $\forall x, y \in A$ se tiene que $x \leq y$ o $y \leq x$.

En la siguiente proposición se recoge el orden que manejaremos en un semigrupo numérico cualquiera.

Proposición 1.12. *Sea S un semigrupo numérico. Definimos la relación binaria en $\mathbb{Z}$ siguiente:*

$$x \leq_S y \iff y - x \in S$$

La relación $\leq_S$ es relación de orden en $\mathbb{Z}$.

Demostración. Sean $x, y, z \in \mathbb{Z}$. Veamos que se verifican las propiedades necesarias para que $\leq_S$ sea un orden parcial.

1. Es claro que $x \leq_S x$ pues $x - x = 0$, y como S es un monoide, $0 \in S$.
2. Si $x \leq_S y, y \leq_S x$, tenemos que $x - y \in S, y - x \in S$. Como S es submonoide de $\mathbb{N}$, necesariamente $x - y \geq 0$, luego $y - x \leq 0$. Dado que $y - x \in S \subseteq \mathbb{N}$, esta última condición solo puede darse si $y - x = 0$ o equivalentemente si $y = x$.
3. Si $x \leq_S y$ e $y \leq_S z$, podemos afirmar que $y - x \in S$ y $z - y \in S$. Además, como $+$ es ley de composicion interna, $(y - x) + (z - y) = z - x \in S$ luego por la definición de la relación, $x \leq_S z$.

Así, concluimos que $\leq_S$ es un orden en $\mathbb{Z}$. □

Observación 1.13. Si $(A, \leq)$ es un conjunto ordenado y $B \subseteq A$, entonces $(B, \leq)$ es también un conjunto ordenado. Esto nos permitirá aplicar la relación de la Proposición 1.12 a subconjuntos de $\mathbb{Z}$.

Dentro de los conjuntos ordenados existe una serie de elementos particularmente relevantes. Por ello, introducimos una serie de definiciones que serán necesarias a posteriori.

Definición 1.14. *Sea $(P, \leq)$ un conjunto (parcialmente) ordenado y sea $m \in P$. Diremos que:*

- *m es **máximo** en P si para todo $x \in P$, se tiene que $x \leq m$.*
- *m es **mínimo** en P si para todo $x \in P$, se tiene que $m \leq x$.*
- *m es **maximal** en P si de tener que $x \in P$ y $m \leq x$, entonces $m = x$.*

- m *es* ***minimal*** *en* P *si de tener que* $x \in P$ *y* $x \leq m$, *entonces* $m = x$.

Si S es un semigrupo numérico, podemos afirmar que $(S, \leq_S)$ tiene a 0 por mínimo. Denotando $S^* = S - \{0\}$, vamos a demostrar que los elementos minimales de $(S^*, \leq_S)$ conforman el único sistema minimal de generadores de S.

Lema 1.15. *Sea* S *un semigrupo numérico y* $x \in S$. *Entonces,*

$$x \text{ es no minimal en } (S, \leq_S) \iff x = y + z, \text{ con } y, z \in S^*.$$

Demostración. Supongamos que $x \in S$ es no minimal. De esta hipótesis, tenemos que $\exists\ y \in S^*$, $y \neq x$ tal que $y \leq_S x$, luego por definición $x - y \in S$. Llamando $z \coloneqq y - x$ es evidente que $x = y + z$. Además, podemos afirmar que $y, z \neq 0$ pues de ser alguno de ellos igual a cero, tendríamos que $x = y$ o $x = z$, lo cual no es posible.

Consideramos ahora $x, y, z \in S^*$ tal que $x = y + z$. Como S está parcialmente ordenado y podemos escribir x de la forma anterior, tenemos que $y \leq_S x$. Además, podemos afirmar que $y \neq x$, pues en caso contrario obtendríamos que $z = 0$, en contra de lo supuesto. Así, hemos encontrado $y \neq x$ menor que x para $\leq_S$, luego x es no minimal. □

Este lema nos sitúa en condiciones de caracterizar cuál es el sistema minimal de generadores de un semigrupo numérico arbitrario.

Proposición 1.16. *El único sistema minimal de generadores de* S *está formado por los elementos minimales de* $(S^*, \leq_S)$. *Además, dicho sistema es finito y tiene como mucho* a_1 *elementos. siendo* $a_1 \coloneqq min(S^*)$.

Demostración. Definimos $H \coloneqq \{x \in S^* : x \text{ es minimal}\}$. Vamos a demostrar que $\langle H \rangle = \mathrm{S}$.

" $\subseteq$ " Es claro que $H \subseteq S$ luego $\langle H \rangle \subseteq S$.
" $\supseteq$ " Por inducción. Consideramos $S_n \coloneqq \{x \in S : x \leq n\}$. Si $n = 0$, es evidente que $S_n = \{0\} \subseteq \langle H \rangle$. Supongamos que $S_n \subseteq \langle H \rangle$ y veamos que $S_{n+1} \subseteq \langle H \rangle$.

Sea $x \in S_{n+1}$. Entonces, $x \in S$ y $x \leq n + 1$. Podemos ahora distinguir dos casos: si $x \leq n$, automáticamente estaría en S_n y por la hipótesis de inducción también en $\langle H \rangle$. Por otra parte, si $x = n + 1$ se presentan dos nuevos casos:

- Si x es minimal, $x \in H$ por definición luego $x \in \langle H \rangle$.
- Si x no es minimal, por el Lema 1.15, existen $y, z \in S^*$ tal que $x = y + z$. Además, $x = n + 1$ luego $x = n + 1 = y + z$ y en consecuencia tenemos que $y, z \in S$ e $y, z \leq n$. Por tanto, $y, z \in S_n \subseteq \langle H \rangle$ y por tanto $x = y + z \in \langle H \rangle$.

Así, hemos probado que $S_{n+1} \subseteq \langle H \rangle$. Además, si $x \in S$ entonces es claro que $x \in S_x \subseteq \langle H \rangle$, quedando así demostrada la inclusión y por lo tanto la igualdad.

Veamos la unicidad del sistema generador minimal. Sea T otro sistema generador minimal de S y sea $x \in H$. La siguiente cadena de inclusiones es evidente: $H \subseteq S \subseteq \langle T \rangle$, luego $x \in \langle T \rangle$. Si $x \in T$ ya estaría. Supongamos que $x \notin T$, dado que si está en el generado por él, podemos afirmar que existen $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^+$ y $t_1, \ldots t_n \in T$ tales que:

$$x = \alpha_1 t_1 + \cdots + \alpha_n t_n$$

Podemos reescribir x de la siguiente manera:

$$x = t_1 + \big((\alpha_1 - 1)t_1 + \alpha_2 t_2 + \cdots + \alpha_n t_n\big)$$

Observamos que $t_1 \in T \subseteq \langle T \rangle \subseteq S$ y que el segundo sumando está en $\langle T \rangle \subseteq S$ y además es distinto de cero, pues en caso contrario $x \in T$ en contra de lo supuesto. Obtenida esta escritura de x, en virtud del Lema 1.15, x es no minimal, lo cual es absurdo dado que inicialmente supusimos que $x \in H$. Por tanto, $H \subseteq T$.

Supongamos que H tiene más de a_1 elementos. En ese caso, existen $a, b \in H$ tales que $a \equiv b \pmod{n}$. Así, obtenemos que $a = b + \lambda a_1$ con $\lambda \in \mathbb{N}$ y además cada uno de estos sumandos está en S^*, luego nuevamente por el Lema anterior, a es no minimal, lo que es una contradicción. Por tanto, H es finito y tiene como mucho a_1 elementos. □

Nota:. A partir de ahora nombraremos $S = \langle a_1, \ldots, a_n \rangle$ con $a_1 < \cdots < a_n$ su único sistema minimal de generadores.

1.4. El conjunto de Apéry y elementos notables asociados a semigrupos numéricos

Vamos a estudiar algunos de los conjuntos notables asociados a un semigrupo numérico. El primero de ellos es el conjunto de Apéry, a partir del cual podremos obtener una gran cantidad de información sobre los semigrupos numéricos.

Definición 1.17. *Sean S un semigrupo numérico y $n \in S^*$. Se define el conjunto de Apéry de S respecto a m, denotado por $Ap(S, m)$ como sigue:*

$$Ap(S, m) \coloneqq \{s \in S : s - m \notin S\}$$

Ejemplo 1.18. Sea $S = \langle 5, 7, 9 \rangle = \{0, 5, 7, 9, 10, 12, 14, \rightarrow\}$. Vamos a calcular $Ap(S, 5)$ y $Ap(S, 7)$.

$$Ap(S,5) = \{s \in S : s-5 \notin S\} = \{0,7,9,16,18\}$$
$$Ap(S,7) = \{s \in S : s-7 \notin S\} = \{0,5,7,9,10,15,18,20\}$$

A continuación recogemos en un lema una descripción del conjunto de Apéry empleando congruencias.

Lema 1.19. *Sean S un semigrupo numérico y $m \in S^*$ y sea $w(i)$ el menor elemento de S congruente con i módulo m. Entonces,*

$$Ap(S,m) = \{0 = w(0), w(1), \cdots, w(m-1)\}$$

Demostración. " $\supseteq$ " Sea $i \in \{0, \cdots, m-1\}$. Entonces, por definición $w(i) \in S$ y $w(i) \equiv i \pmod{m}$. Podemos afirmar que $w(i) - m \notin S$ pues en caso contrario, tendríamos que $w(i) - m \equiv i \pmod{m}$ y además $w(i) - m < w(i)$, lo cual contradice la definición de $w(i)$. Entonces, por definición del conjunto de Apéry, $w(i) \in Ap(S,m)$ y en consecuencia $\#Ap(S,m) \geq \#\{w(0), \cdots, w(n-m)\} = m$.

Veamos que $\#Ap(S,m) \leq m$. En efecto, si $a, b \in Ap(S,m)$ con $a > b$, no puede verificarse que $a \equiv b \pmod{m}$ pues de darse, entonces $a = km + b$ donde $k > 0$ y consecuentemente, $a - m = (k-1)m + b \in S$ lo cual es absurdo puesto que $a \in Ap(S,m)$.

Por tanto, en $Ap(S,m)$ hay exactamente m elementos y combinando esto con la inclusión anterior, tenemos la igualdad de conjuntos. □

.

Lema 1.20. *Sea S un semigrupo numérico y $m \in S^*$. Para todo $s \in S$ existe un único par $(k,w) \in \mathbb{Z} \times Ap(S,m)$ tal que $s = km + w$. Además, $s \in S$ si y solo si $k \in \mathbb{N}$.*

Demostración. Veamos la existencia. Sean $s \in \mathbb{Z}$, $i \in \{0, \ldots, m-1\}$ tal que $s \equiv i \pmod{m}$. Por la definición de $Ap(S,m)$, tenemos que $s \equiv w(i) \pmod{m}$ y en consecuencia $s = km + w(i)$.

En cuanto a la unicidad, supongamos que tenemos $(k_1, w_1), (k_2, w_2) \in \mathbb{Z} \times Ap(S,m)$ tales que $s = k_1 m + w_1(i) = k_2 m + w_2(i)$. Es claro que $w_1 \equiv w_2 \pmod{m}$. Esto implica que $w_1 = w_2$ y de aquí, es inmediato que $k_1 = k_2$ luego $(k_1, w_1) = (k_2, w_2)$.

Veamos la última equivalencia. Si tenemos $s = km + w$ con $k \in \mathbb{N}$, es claro que $s \in S$ pues $km \in S$ y $w \in S$. En cuanto al recíproco, si $k \notin \mathbb{N}$, entonces $k < 0$ luego $s = kn + w < w$ y de la definición de w se tiene que $s \notin S$. □

Para terminar esta sección, incluimos un corolario que es consecuencia directa del Lema 1.20.

Corolario 1.21. *Si S es un semigrupo numérico, $(Ap(S,m) - \{0\}) \cup \{m\}$ es un sistema generador de S con m generadores.*

1.5. Números de Fröbenius y de pseudo-Fröbenius. Huecos y tipo de un semigrupo numérico.

Definición 1.22. *Sea S un semigrupo numérico. Se define el número de Fröbenius de S, denotado $F(S)$ de la siguiente manera:*

$$F(S) \coloneqq máx(\mathbb{Z} - S)$$

Definición 1.23. *Sea S un semigrupo numérico, se define el conjunto de huecos de S como aquellos elementos de $\mathbb{N}$ que no están en el semigrupo, esto es, $G(S) \coloneqq \mathbb{N} - S$. Dicho conjunto es finito pues S es semigrupo numérico. Además, a su cardinal lo llamamos número de huecos de S y lo denotaremos como $g(S)$.*

Ejemplo 1.24. En $S = \{0, 2, 4, 5, \rightarrow\}$, tenemos que el conjunto de huecos es $G(S) = \{1, 3\}$, luego $g(S) = 2$. Su número de Fröbenius es $F(S) = 3$.

Proposición 1.25 (Fórmulas de Selmer). *Sea S un semigrupo numérico y $m \in S^*$. Entonces:*

1. $F(S) = máx(Ap(S, m)) - m$.
2. $g(S) = \frac{1}{m}\left(\sum_{w \in Ap(S,m)} w\right) - \frac{m-1}{2}$.

Demostración. Sea $F = máx(Ap(S, m)) - m$. Vamos a demostrar que cualquier número mayor que F está en el semigrupo. Para ello, tomamos $x > F$. Entonces, tenemos que $x + m > máx(Ap(S, n))$. Por el Lema 1.20, existe un único $(k, i) \in \mathbb{Z} \times Ap(S, m)$ tal que $x + m = km + i$. Consideremos ahora $i \in Ap(S, m) : w(i) \equiv i \pmod{m}$. Por la relación de congruencia, llegamos a que $w(i) = km + i$ y en consecuencia $x + m = km + w(i)$, luego $x = (k - 1)m + w(i)$ que es suma de elementos de S, por lo que podemos afirmar que $x \in S$.

Como $F = máx(Ap(S, n)) - m \notin S$ y si $x > F$ entonces $x \in S$, podemos afirmar que F es el número de Fröbenius de S.

Para la segunda propiedad, consideremos $w \in Ap(S, m) \subseteq S$. Entonces, por el Lema 1.20 podemos escribir $w = k_i m + i$, donde $(k, i) \in \mathbb{Z} \times Ap(S, m)$. Por ello, el conjunto de Apéry admite la siguiente escritura:

$$Ap(S, m) = \{0, k_1 m + 1, k_2 m + 2, \cdots, k_{m-1} m + (m - 1)\}$$

Ahora bien, si $x \in \mathbb{N}$, $x \equiv i \pmod{m}$ es cierto que para todo $x \in S$, podemos expresar $x = w(i) + \lambda m$ con $\lambda \geq 0$.

Definimos $G_i(S) = \{x = w(i) + \mu m, \mu < 0, x \geq 0\}$. Podemos entonces caracterizar los huecos de S de la siguiente manera:

$$\begin{aligned} G(S) &= \{x \in \mathbb{N} : x = w(i) + \mu m, \mu < 0, i \in \{0, \dots, m-1\}\} \\ &= \bigsqcup_{i=0}^{n-1} \{x = w(i) + \mu m, \mu < 0, x \geq 0\} \\ &= \bigsqcup_{i=0}^{n-1} G_i(S) \end{aligned}$$

Nótese que la unión disjunta es consecuencia de que $w(i) \in Ap(S,m)$, pues no puede haber dos $w(i) \equiv i \pmod m$ distintos. Además, esto nos permite afirmar la siguiente cadena de igualdades referente al cardinal de dicha unión.

$$\begin{aligned} g(S) =& \#\left(\bigsqcup_{i=0}^{m-1} G_i(S)\right) = \sum_{i=0}^{m-1} \#G_i(S) = \sum_{i=0}^{m-1} \left\lfloor \frac{w(i)}{m} \right\rfloor \\ =& \sum_{i=0}^{m-1} \frac{w(i)-i}{m} = \frac{1}{m}\sum_{i=0}^{m-1} w(i) - \frac{1}{m}\sum_{i=0}^{m-1} i \\ =& \frac{1}{m}\sum_{i=0}^{m-1} w(i) - \frac{m-1}{2} = \frac{1}{m}\left(\sum\nolimits_{w \in Ap(S,m)} w\right) - \frac{m-1}{2} \end{aligned}$$

Quedan así demostradas las dos fórmulas. □

Lema 1.26. *Sea S un semigrupo numérico. Entonces:*

$$g(S) \geq \frac{F(S)+1}{2}$$

Demostración. Definimos el conjunto $N(S) = \{s \in S : s \leq F(S)\}$ y denotamos su cardinal por $n(S)$. Definimos la siguiente aplicación:

$$\begin{aligned} h : N(S) &\longrightarrow G(S) \\ s &\longmapsto F(S) - s \end{aligned}$$

Está bien definida, puesto que si $s \in N(S)$, $h(s) = F(S) - s \notin S$ pues de lo contrario, dado que S es un monoide se daría que $(F(S) - s) + s = F(S) \in S$ en contra de la definición de $F(S)$, luego $h(s) \in G(S)$. Es sencillo comprobar además, que h es inyectiva.

Por la inyectividad de h, tenemos que $\#G(S) \geq \#N(S)$ luego $g(S) \geq n(S)$. Además, todos los elementos de S más pequeños que $F(S)$ están en $N(S)$ o en $G(S)$, por lo que en definitiva, $G(S) \bigsqcup N(S) = \{0, \cdots, F(S)\}$. Considerando el hecho de que la unión es disjunta, concluimos que $g(S) + n(S) = F(S) + 1$. Así, valiéndonos de la primera desigualdad y sumando $g(S)$ a ambos lados, obtenemos que $2g(S) \geq F(S) + 1$ luego $g(S) \geq \frac{F(S)+1}{2}$. □

Definición 1.27. *Sea S semigrupo numérico y $x \in \mathbb{Z}$. Diremos que x es un número de pseudo-Fröbenius si verifica las siguientes propiedades:*

1. $x \notin S$.
2. $x + s \in S \ \forall s \in S^*$

Al conjunto de números de pseudo-Fröbenius se le denota por $PF(S)$ y su cardinal es denominado tipo del semigrupo y lo denotamos por tipo(S).

Observación 1.28. Es claro que $F(S) \in PF(S)$ pues se trata del mayor entero positivo que no está en el semigrupo S.

Proposición 1.29. *Sea S un semigrupo numérico. Entonces:*

1. $PF(S) = Maximales_{\leq_S}(\mathbb{Z} - S)$.
2. $x \in \mathbb{Z} - S \iff f - x \in S$ *para algún* $f \in PF(S)$.

Demostración. Comenzamos con 1.
" $\subseteq$ " Tomamos $x \in PF(S)$ y supongamos que no es maximal. Entonces, existe $y \in \mathbb{Z} - S$ tal que $y \neq x, x \leq_S y$. Por la relación de orden establecida, tenemos que $y - x \in S$. Llamamos ahora $s_0 = y - x$. De aquí, claramente $y = x + s_0$. Además, como $x \in PF(S)$, $x + s \in S \ \forall s \in S^*$. En particular es válido para $s = s_0$. Llegamos así a un absurdo dado que y pertenecería a $S \cap (\mathbb{Z} - S) = \emptyset$, luego $x \in Maximales_{\leq_S}(\mathbb{Z} - S)$.

" $\supseteq$ " Por reducción al absurdo. Supongamos que $x \in Maximales_{\leq_S}(\mathbb{Z} - S)$ y que $x \notin PF(S)$, es decir, que existe $s_0 \in S^*$ tal que $x + s_0 \notin S$. Es evidente que $(x + s_0) - x = s_0 \in S$ luego podemos afirmar que $x \leq_S x + s_0$. Además, estos dos elementos son distintos puesto que $s_0 \neq 0$. En consecuencia, es absurdo que $x \leq_S x + s_0$ dada la maximalidad de x. Por tanto, $x \in PF(S)$.

Veamos a continuación 2.
" $\Rightarrow$ " Sea $x \in \mathbb{Z} - S$. Si x un número de pseudo-Fröbenius, bastaría tomar $f = x$ puesto que $f - x = x - x = 0 \in S$. Si no lo fuera, existiría $y \neq x$ maximal, luego $x \leq_S y$. Tomando en este caso $f = y$ y teniendo en cuenta el orden, tendríamos que $y - x = f - x \in S$ y ya estaría.

" $\Leftarrow$ " Sea $f \in PF(S) : f - x \in S$. Supongamos además que $x \in S$. Por hipótesis y dado que la suma es ley de composición interna, obtenemos que $(f - x) + x = f \in S$, lo cual es absurdo en virtud de la primera hipótesis. De aquí, concluimos que $x \notin S$ y por tanto $x \in \mathbb{Z} - S$. □

Proposición 1.30. *Sea S semigrupo numérico y $m \in S^*$. Entonces:*

$$PF(S) = \{w - m : w \in Maximales_{\leq_S}(Ap(S, m))\}$$

Demostración. " $\subseteq$ " En primer lugar, sea $x \in PF(S)$. Por definición $x \notin S$ y dado que $m \in S^*$, tenemos que $x + m \in S$. Esto es equivalente a que $x+m \in Ap(S,n)$, puesto que $(x+m)-m = x \notin S$. Tomamos ahora $w \in Ap(S,m)$ verificando que $x+m \leq_S w$. Entonces, $w-(x+m) = w-x-m \in S$. Llamando $s := w-x-m$, tenemos que $w-m = x+s$ para cierto $s \in S$. Esto implica que $s = 0$ pues en caso contrario, tendríamos que $x+s = w-m \in S \cap (\mathbb{Z}-S)$. Por tanto, podemos afirmar que $x = w-m$. Además, de suponer que $x+m \leq_S w$ hemos obtenido que $w = x+m$ y en consecuencia, $x+m \in Maximales_{\leq_S}(Ap(S,m))$ que implica que $w \in Maximales_{\leq_S}(Ap(S,m))$.

" $\supseteq$ " Sea $w \in Maximales_{\leq_S}(Ap(S,m))$. Entonces, en particular $w \in Ap(S,m)$, luego $w-m$ no es un elemento de S. Supongamos ahora que existe $s_0 \in S^*$ tal que $(w-m)+s_0 \notin S$. Es claro que en ese caso, $w+s_0 \in Ap(S,m)$. Además, dado que s_0 es no nulo, que $w+s_0 \neq w$ y que $w \leq_S w+s_0$ llegamos a un absurdo por la maximalidad de w. □

En el siguiente corolario recogemos una cota superior para el tipo de un semigrupo numérico.

Corolario 1.31. *Sea $S = \langle a_1, \ldots, a_n \rangle$ un semigrupo numérico. Entonces,*

$$1 \leq tipo(S) \leq a_1 - 1$$

Demostración. La desigualdad $1 \leq tipo(S)$ es evidente ya que $F(S) \in PF(S)$. Por el Lema 1.19 tenemos que $\#Ap(S,n) = n$, $\forall n \in S^*$. Además, la Proposición 1.30 nos permite afirmar, puesto que 0 no es un elemento maximal de este conjunto, que:

$$tipo(S) = \#PF(S) = \#Maximales_{\leq_S}(Ap(S,n)) \leq n-1$$

Como ya sabemos, $a_1 \in S^*$ luego tiene sentido considerar el conjunto $Ap(S,a_1)$, que sabemos que tiene exactamente a_1 elementos. Concluimos entonces que

$$tipo(S) = \#Maximales_{\leq_S}(Ap(S,a_1)) \leq a_1 - 1 \qquad \square$$

Para finalizar este capítulo, presentamos un ejemplo del estudio particular de un semigrupo numérico.

Ejemplo 1.32. Sea $S = \langle 5,7,9,11,13 \rangle$. Vamos a calcular diferentes elementos notables de dicho semigrupo. En primer lugar determinamos explícitamente los elementos de S:

$$S = \langle 5,7,9,11,13 \rangle = \{0,5,7,9,10,\rightarrow\}$$

Es fácil comprobar que $A = \{5,7,9,11,13\}$ es el sistema generador minimal de S. Dado que ninguno de los elementos de A es suma de dos elementos de S^*, en virtud del Lema 1.15, los elementos de A son minimales en $(S^*, \leq_S)$ y de la

Proposición 1.16, deducimos que A es, en efecto, el sistema generador minimal de S.

Conocido S, podemos afirmar que el conjunto de huecos de S es $G(S) = \mathbb{N} - S = \{1, 2, 3, 4, 6, 8\}$. Por tanto, el número de huecos es $g(S) = 6$ y podemos afirmar que $F(S) = 8$.

Atendiendo a la Definición 1.27, el conjunto de números de pseudo-Fröbenius es $PF(S) = \{2, 4, 6, 8\}$, luego $tipo(S) = 4$.

Hallamos $Ap(S, 9)$, $Ap(S, 13)$ y sus respectivos diagramas de orden para así detectar sus elementos maximales.

$$Ap(S, 9) = \{s \in S : s - 9 \notin S\} = \{0, 5, 7, 10, 11, 12, 13, 15, 17\}$$
$$Ap(S, 13) = \{s \in S : s - 13 \notin S\} = \{0, 5, 7, 9, 10, 11, 12, 14, 15, 16, 17, 19, 21\}$$

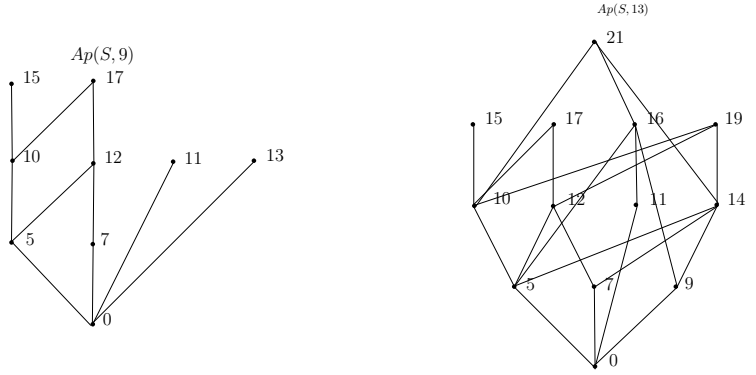

Figura 1.1: Diagramas de $Ap(S, 9)$ y $Ap(S, 13)$.

Observamos que los elementos maximales son aquellos que ocupan los extremos de los diagramas, es decir, $Maximales_{\leq_S}(Ap(S, 9)) = \{11, 13, 15, 17\}$ y $Maximales_{\leq_S}(Ap(S, 13)) = \{15, 17, 19, 21\}$.

Por último, comprobamos que hallando $PF(S)$ mediante la Proposición 1.30 el resultado coincide con el anteriormente calculado. En efecto,

$$PF(S) = \{w - 9 : w \in Maximales_{\leq_S}(Ap(S, 9))\} = \{2, 4, 6, 8\}.$$
$$PF(S) = \{w - 13 : w \in Maximales_{\leq_S}(Ap(S, 13))\} = \{2, 4, 6, 8\}.$$

2

Bases de Gröbner

En este capítulo vamos a estudiar los ideales del anillo de polinomios $\mathbb{K}[x_1, \ldots, x_n]$, donde $\mathbb{K}$ es un cuerpo. Cuando se pretende comprender los ideales polinómicos, surgen diversas problemáticas.

- **Problema de pertenencia:** Dado $f \in \mathbb{K}[x_1, \ldots, x_n]$ y $\mathfrak{I} = \langle f_1, \ldots, f_s \rangle$, ¿$f$ pertenece a $\mathfrak{I}$? Cuando tenemos $n = 1$, dado que $\mathbb{K}[x]$ es un dominio euclídeo, es sencillo responder a la pregunta mediante la división euclídea. Sin embargo, cuando el número de variables es mayor o igual que dos, $\mathbb{K}[x_1, \ldots, x_n]$ no es un dominio euclídeo y en consecuencia aumenta la complejidad para dar una respuesta.
- **Problema de eliminación:** Dado $\mathfrak{I}$ un ideal de $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, se pretende calcular un sistema generador del ideal $\mathfrak{J} \cap \mathbb{K}[x_1, \ldots, x_n]$.
- **Cálculo de la dimensión de** $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$: Consideramos el anillo cociente $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$, el cual admite estructura de $\mathbb{K}$-espacio vectorial. Nos interesa calcular una base y hallar su dimensión.

Será de especial interes en este trabajo el problema de pertenencia a ideales del anillo de polinomios, si bien todos estos problemas los resolveremos empleando bases de Gröbner. Se hará uso en repetidas ocasiones del Teorema de la Base de Hilbert, el cual presentamos a continuación.

Teorema 2.1 (de la Base de Hilbert). *Sea $\mathfrak{I}$ un ideal de $\mathbb{K}[x_1, \ldots, x_n]$. Si $\mathfrak{I} = \langle f_i : i \in I \rangle$, entonces existen $i_1, \ldots, i_r \in I$ tales que $\mathfrak{I} = \langle f_{i_1}, \ldots, f_{i_r} \rangle$*

En particular, el Teorema de la Base de Hilbert afirma que el anillo $\mathbb{K}[x_1, \ldots, x_n]$ es noetheriano y por tanto toda cadena creciente de ideales se estabiliza.

2.1. Órdenes monomiales

Definición 2.2. *Un monomio en $\mathbb{K}[x_1, \ldots, x_n]$ es un producto de la forma*

$$x^\alpha \coloneqq x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

siendo $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. *El valor* $|\alpha| \coloneqq \alpha_1 + \cdots + \alpha_n$ *es el grado del monomio.*

Para el desarrollo de este capítulo es necesario introducir una noción de orden total sobre los monomios. Este concepto generaliza el orden inducido por el grado en el anillo de polinomios en una variable. Por ello, presentamos la siguiente definición:

Definición 2.3. *Un orden monomial en* $\mathbb{K}[x_1, \ldots, x_n]$ *es una relación binaria* " $\geq$ " *en el conjunto de monomios* $M = \{x^\alpha : \alpha \in \mathbb{N}^n\}$ *verificando:*

1. " $\geq$ " *es orden total en* M.
2. *Si* $x^\alpha, x^\beta, x^\gamma \in M$ *tal que* $x^\alpha \geq x^\beta$ *entonces* $x^\alpha x^\gamma \geq x^\beta x^\gamma$ *(compatibilidad con el producto de monomios).*
3. $x^\alpha \geq x^{(0,\ldots,0)} = 1$ *para todo* $x^\alpha \in M$.

Dado un orden monomial " $\geq$ "*, escribiremos* $x^\alpha > x^\beta$ *si* $x^\alpha \geq x^\beta$ *y* $x^\alpha \neq x^\beta$.

De manera equivalente, los órdenes monomiales pueden ser tratados como relaciones binarias " $\geq$ " *en* $\mathbb{N}^n$ *verificando las siguientes propiedades:*

1. " $\geq$ " *es orden total en* $\mathbb{N}^n$.
2. *Si* $\alpha, \beta, \gamma \in \mathbb{N}^n$*, entonces* $\alpha + \gamma \geq \beta + \gamma$ *(compatibilidad con la suma de* $\mathbb{N}^n$*).*
3. $\alpha \geq (0, \ldots, 0)$ *para todo* $\alpha \in \mathbb{N}^n$.

Observación 2.4. Cuando se presenta la Teoría de bases de Grobner en contextos más generales (como el anillo de polinomios en infinitas variables) se exige que el orden monomial " $\geq$ " sea un buen orden, es decir, que toda cadena decreciente de monomios ordenados tenga mínimo. En nuestro caso, esta condición se verifica automáticamente en virtud del Teorema 2.1 pues si tenemos una cadena de monomios $x^{\alpha_1} \geq x^{\alpha_2} \geq x^{\alpha_3} \geq \cdots$ se obtiene una cadena de ideales $I_1 = \langle x^{\alpha_1} \rangle \subseteq I_2 = \langle x^{\alpha_1}, x^{\alpha_2} \rangle \subseteq I_3 = \langle x^{\alpha_1}, x^{\alpha_2}, x^{\alpha_3} \rangle \cdots$. Por el Teorema de la Base de Hilbert, esta cadena ascendente de ideales se estabiliza, es decir, existe k tal que $\forall l \geq k$, $I_k = I_l$. Vamos a ver que el mínimo de $x^{\alpha_1} \geq x^{\alpha_2} \geq x^{\alpha_3} \geq \cdots$ es x^{α_k}. Sea $l \in \mathbb{Z}^+$. Si $l < k$ entonces $x^{\alpha_l} \geq x^{\alpha_k}$. Si $l \geq k$ como $I_k = I_l$, se tiene que $x^{\alpha_l} \in I_k$. En virtud del Lema 2.16 (que demostraremos posteriormente), existe $i \in \{1, \ldots, k\}$ tal que $x^{\alpha_i} \mid x^{\alpha_l}$, luego existe x^β tal que $x^{\alpha_l} = x^{\alpha_i} x^\beta$. Como consecuencia de 3 en la Definición 2.3, se tiene que $x^\beta \geq 1$ luego $x^{\alpha_i} x^\beta \geq x^{\alpha_i}$. Finalmente, por 2 de la misma definición, se obtiene que $x^{\alpha_l} = x^{\alpha_i} x^\beta \geq x^{\alpha_i} \geq x^{\alpha_k}$ y x^{α_k} es el mínimo.

Presentamos a continuación diversos ejemplos de órdenes monomiales.

Definición 2.5 (Orden lexicográfico). *Sean dos n-tuplas* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *y* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. *Diremos que* $\alpha >_{lex} \beta$ *si la primera entrada no nula de* $\alpha - \beta$ *por la izquierda es positiva. Si* $\alpha >_{lex} \beta$, *escribiremos* $x^\alpha >_{lex} x^\beta$.

Definición 2.6 (Orden lexicográfico graduado). *Sean* $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. *Diremos que* $\alpha >_{grlex} \beta$ *si* $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ *o* $|\alpha| = |\beta|$ *y* $\alpha >_{lex} \beta$.

Definición 2.7 (Orden lexicográfico inverso graduado). *Sean dos n-tuplas* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *y* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. *Diremos que* $\alpha >_{grevlex} \beta$ *si* $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ *o* $|\alpha| = |\beta|$ *y la primera entrada no nula por la derecha de* $\alpha - \beta$ *es negativa.*

Proposición 2.8. *Los órdenes lexicográfico, lexicográfico graduado y lexicográfico inverso graduado son órdenes monomiales.*

Demostración. Que $>_{lex}$ es un orden total es directo de la definición y de que $\mathbb{N}^n$ está totalmente ordenado. Sean $\alpha, \beta, \gamma \in \mathbb{N}^n$, veamos que la suma es compatible con el orden lexicográfico.

Supongamos que $\alpha >_{lex} \beta$. De aquí, la primera entrada no nula de $\alpha - \beta$ es positiva. Consideramos ahora $\alpha + \gamma$ y $\beta + \gamma \in \mathbb{N}^n$. Claramente, $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, cuya primera entrada no nula es positiva. Por tanto, tenemos que $\alpha + \gamma >_{lex} \beta + \gamma$.

Para $>_{grlex}$ y $>_{grevlex}$ el razonamiento es análogo. □

Definición 2.9. *Sea* $f = \sum a_\alpha x^\alpha$ *un polinomio no nulo en* $\mathbb{K}[x_1, \ldots, x_n]$ *y sea* " $\geq$ " *un orden monomial. Se definen:*

- *Multigrado de* f *como* $mdeg(f) \coloneqq máx_{\geq}\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$
- *Coeficiente principal de* f *es* $LC(f) = a_{mdeg(f)} \in \mathbb{K}$.
- *Monomio principal de* f *es* $LM(f) = x^{mdeg(f)}$.
- *Término principal de* f *es* $LT(f) = LC(f) \cdot LM(f) = a_{mdeg(f)} x^{mdeg(f)}$.

El multigrado de un polinomio presenta un comportamiento similar al del grado en polinomios de una única variable. Recogemos dicho comportamiento en la siguiente proposición cuya prueba es evidente.

Proposición 2.10. *Sean* $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ *polinomios no nulos. Entonces:*

1. $mdeg(f \cdot g) = mdeg(f) + mdeg(g)$.
2. *Si* $f + g \neq 0$, $mdeg(f + g) \leq máx\,(mdeg(f), mdeg(g))$. *En particular, si* $mdeg(f) \neq mdeg(g)$, *se da la igualdad.*

2.2. Algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$

Como ya se ha mencionado, el anillo $\mathbb{K}[x]$ donde $\mathbb{K}$ es un cuerpo es un dominio euclídeo. Por tanto, podemos definir sobre él una función euclídea y un algoritmo de división de polinomios con una variable. Sin embargo, al aumentar el número de variables esta propiedad desaparece. El objetivo de esta sección es generalizar a $\mathbb{K}[x_1, \ldots, x_n]$ el algoritmo de división empleado en $\mathbb{K}[x]$. Esto es, dados $f, f_1, \ldots, f_s$, se pretende diseñar un algoritmo que permita obtener la siguiente escritura del polinomio f:

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

donde $q_i \in \mathbb{K}[x_1, \ldots, x_n]$ para $1 \leq i \leq s$ y $r \in \mathbb{K}[x_1, \ldots, x_n]$ satifaciendo ciertas propiedades.

Teorema 2.11 (Algoritmo de división). *Fijado un orden monomial " $\geq$ " en $\mathbb{N}^n$ y sea $F = (f_1, \ldots, f_s)$ una s-tupla ordenada de polinomios de $\mathbb{K}[x_1, \ldots, x_n]$. Entonces, todo $f \in \mathbb{K}[x_1, \ldots, x_n]$ se puede expresar como:*

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

con $q_i \in \mathbb{K}[x_1, \ldots, x_n]$ para $1 \leq i \leq s$, $r \in \mathbb{K}[x_1, \ldots, x_n]$ y $r = 0$ o bien r combinación lineal de monomios de $\mathbb{K}[x_1, \ldots, x_n]$ ninguno de ellos divisible por $LT(f_i)$ para $1 \leq i \leq s$. Además, si $q_i, f_i \neq 0$, entonces $mdeg(f) \geq mdeg(q_i f_i)$.

Demostración. Sean " $\geq$ " un orden monomial y $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Se pretende realizar la división de f entre $f_1, \ldots, f_s$, esto es, obtener una expresión de f como $f = q_1 f_1 + \cdots + q_s f_s + r$. La división termina si bien $r = 0$ o $x^\alpha \nmid LT(f_i)$, con $1 \leq i \leq s$.

Se propone el siguiente algoritmo para la realización de la división:

Algoritmo 1: Algoritmo de división.

Entrada: $f, f_1, \ldots, f_s$ polinomios de $\mathbb{K}[x_1, \ldots, x_n]$
Salida: $q_1, \ldots, q_s$ y resto r.
Inicialización: $f^{(0)} := f, r^{(0)} = 0, q_1 = \cdots = q_s = 0$.
repetir
  si *existe* $j = min\{k : LT(f_k) \mid LT(f^{(i)})\}$. **entonces**
    $f^{(i+1)} = f^{(i)} - \frac{LT(f^{(i)})}{LT(f_j)} f_j$
    $r^{(i+1)} = r^{(i)}$
    $q_j^{(i+1)} = q_j^{(i)} + LT(f^{(i)})/LT(f_j)$
    $q_k^{(i+1)} = q_k^{(i)} \forall k \neq j$
  fin
  en otro caso
    $f^{(i+1)} = f^{(i)} - LT(f^{(i)})$
    $r^{(i+1)} = r^{(i)} + LT(f^{(i)})$
    $q_k^{(i+1)} = q_k^{(i)}$
  fin
  $i := i + 1$
hasta que $f^{(i)} = 0$;
devolver $q_1^{(i)}, \ldots, q_s^{(i)}, r^{(i)}$

Esencialmente ha de demostrarse que este algoritmo termina en un número finito de pasos. En efecto, en cualquiera de los dos casos (existencia o no del j especificado), es claro que $LT(f^{(i)}) > LT(f^{(i+1)})$ puesto que la construcción del dividendo en cada etapa conlleva una cancelación de monomios o términos principales. Por otra parte, estamos considerando un orden monomial en un anillo noetheriano. Por tanto, se trata de un buen orden y en consecuencia la cadena $LT(f^{(i)}) > LT(f^{(i+1)}) > LT(f^{(i+2)}) > \cdots$ tiene mínimo, lo cual nos garantiza que el proceso termina. □

Nota:. Al polinomio r del teorema anterior se le denomina un resto de la division de f entre F.

Ejemplo 2.12. Vamos a realizar la división de $f = xy^2 - x$ entre $f_1 = xy + 1$ y $f_2 = y^2 - 1$ considerando como orden monomial $>_{lex}$ y siguiendo el algoritmo del Teorema 2.11.

Se tiene que $LT(f) = xy^2$ y $LT(f_1)$ divide a $LT(f)$. Así, $f^{(1)} = f - y \cdot f_1 = -x - y$. Ahora, $LT(f^{(1)}) = -x$ y $LT(f_1)$ ni $LT(f_2)$ dividen a $LT(f^{(1)})$ luego $r_1 = -x$ pasa al resto.

Tenemos que $f^{(2)} = f^{(1)} - r_1 = -y$ y $LT(f_1)$ ni $LT(f_2)$ dividen a $LT(f^{(2)})$, luego $r_2 = -y$ pasaría al resto y tendríamos que $r = r_1 + r_2 = -x - y$ es un

resto de la división, obteniendo $f = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$.

Veamos a continuación qué ocurre si alteramos el orden de los polinomios f_1 y f_2. Es decir, dividiremos en primer lugar por f_2 y luego por f_1. Se tiene que $LT(f) = xy^2$ y $LT(f) \mid LT(f_2)$ luego $f^{(1)} = f - x \cdot f_2 = 0$ y habría finalizado la división. Así, $f = x \cdot (y^2 - 1) + 0 \cdot (xy + 1)$.

Al considerar los dos divisores $F_1 = (f_1, f_2)$ y $F_2 = (f_2, f_1)$ se han obtenidos restos diferentes. De aquí deducimos en primer lugar que el resto no queda caracterizado por la condición de que sus términos no sean divisibles por $LT(f_i), 1 \leq i \leq s$. Además, queda patente que el orden en el que se realiza la división es determinante, pues en el caso en el que el resto de la división es cero queda resuelto el problema de pertenencia de forma explícita mientras que en el otro no podemos concluir la pertenencia o no a priori de f al ideal generado por f_1 y f_2.

En cualquier caso, presentamos una condición suficiente para la pertenencia de f al ideal considerado en el siguiente corolario.

Corolario 2.13. *Sean $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ y $F = (f_1, \ldots, f_s)$. Si tras la división de f entre F se obtiene que el resto es cero, entonces $f \in \langle f_1, \ldots, f_s \rangle$.*

2.3. Ideales monomiales

Definición 2.14. *Un ideal $\mathfrak{I}$ de $\mathbb{K}[x_1, \ldots, x_n]$ se dice ideal monomial si existe un subconjunto $A \subseteq \mathbb{N}^n$ posiblemente infinito tal que $\mathfrak{I} = \langle x^\alpha : \alpha \in A \rangle$.*

Ejemplo 2.15. El ideal $\mathfrak{I} = \langle x^4 + y^2, x^2 \rangle$ de $\mathbb{K}[x, y]$ es un ideal monomial. Es claro que $\langle x^4 + y^2, x^2 \rangle = \langle x^2, y^2 \rangle$ luego tenemos un sistema generador de $\mathfrak{I}$ conformado por monomios.

Lema 2.16. *Sea $\mathfrak{I} = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial. Entonces. el monomio x^β pertenece a $\mathfrak{I}$ si y solo si x^β es divisible por x^α para algún $\alpha \in A$.*

Demostración. " $\Leftarrow$ " Sea $\alpha \in A$ tal que x^β es divisible por x^α, con $x^\alpha, x^\beta \in \mathbb{K}[x_1, \ldots, x_n]$. Por hipótesis, $x^\beta = p x^\alpha$ para $p \in \mathbb{K}[x_1, \ldots, x_n]$. Como $\mathfrak{I}$ es un ideal, es evidente que $x^\beta \in \mathfrak{I}$.

" $\Rightarrow$ " Sea $x^\beta \in \mathfrak{I}$. Entonces, se tiene que $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ para $h_i \in \mathbb{K}[x_1, \ldots, x_n], 1 \leq i \leq s$. Podemos expandir esta expresión y obtenemos

$$x^\beta = x^{\alpha(1)} \left(c_{1,1} x^{\beta_{1,1}} + \cdots c_{1,s} x^{\beta_{1,s}} \right) + \cdots + x^{\alpha(s)} \left(c_{s,1} x^{\beta_{s,1}} + \cdots + c_{s,s} x^{\beta_{s,s}} \right).$$

Cada uno de los términos de la segunda expresión es divisible por cierto $x^{\alpha(i)}$. Como dicha expresión es igual a x^β, concluimos que x^β es divisible por x^α para cierto $\alpha \in A$. □

Lema 2.17. *Sea $\mathfrak{I}$ un ideal monomial y $f \in \mathbb{K}[x_1, \ldots, x_n]$. Las siguientes afirmaciones son equivalentes:*

1. *$f \in \mathfrak{I}$.*
2. *Todos los términos de f pertenecen a $\mathfrak{I}$.*
3. *f es $\mathbb{K}$-combinación lineal de monomios de $\mathfrak{I}$.*

Demostración. La cadena de implicaciones 3 $\implies$ 2 $\implies$ 1 es trivial, así como 2 $\implies$ 3 en virtud del Lema 2.16. Veamos que 1 $\implies$ 2.

Sea $f \in \mathfrak{I}$. Como $\mathfrak{I}$ es monomial, tenemos que $f = \sum_{\alpha \in A} h_\alpha x^\alpha$ con $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n], x^\alpha \in \mathfrak{I}$. Como h_α es un polinomio, es suma de monomios luego podemos reescribir esta expresión como $f = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}$. Por tanto, hemos escrito f como suma de monomios de $\mathfrak{I}$ que además son divisibles por $x^{\alpha(i)}$ para cierto $\alpha(i) \in A$. En virtud del Lema 2.16 cada uno de los monomios de f pertenece a $\mathfrak{I}$. □

A partir de este resultado obtenemos un corolario que implica una condición necesaria y suficiente de igualdad para ideales monomiales.

Corolario 2.18. *Dos ideales monomiales $\mathfrak{I}, \mathfrak{K}$ son iguales si y solo si contienen los mismos monomios.*

Demostración. Sean $\mathfrak{I}, \mathfrak{K}$ dos ideales monomiales de $\mathbb{K}[x_1, \ldots, x_n]$.
" $\Rightarrow$ " Es evidente pues si $\mathfrak{I} = \mathfrak{K}$, todo monomio de $\mathfrak{I}$ pertenece a $\mathfrak{K}$ y viceversa.
" $\Leftarrow$ " Supongamos que $\mathfrak{I}, \mathfrak{K}$ contienen los mismos monomios. Veamos que $\mathfrak{I} = \mathfrak{K}$.

" $\subseteq$ " Sea $f \in \mathfrak{I}$. Como f es un polinomio de $\mathfrak{I}$, por el Lema 2.17 todos los términos de f pertenecen a $\mathfrak{I}$. En particular dichos términos son monomios de $\mathfrak{I}$ multiplicados por una constante luego por hipótesis, son también monomios de $\mathfrak{K}$.
" $\supseteq$ " El razonamiento es totalmente análogo tomando $f \in \mathfrak{K}$. □

Sabemos por el Teorema 2.1 enunciado al inicio del capítulo que todo ideal del anillo de polinomios está finitamente generado. Presentamos a continuación una proposición y una definición de un sistema generador notable de los ideales monomiales.

Definición 2.19. *Sea $\mathfrak{I} = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ un ideal monomial. Diremos que su sistema generador es una base mínima si verifica que $x^{\alpha(i)} \nmid x^{\alpha(j)}$ para todo $i \neq j$.*

Proposición 2.20. *La base mínima de un ideal monomial existe y es única.*

Demostración. Veamos la existencia. Sea $\mathfrak{I} = \langle x^{\alpha(1)}, \ldots, x^{\alpha(k)} \rangle$ un ideal monomial. Supongamos que existen $i_0, j_0 \in \{1, \cdots, k\}$ tal que $x^{\alpha(i_0)} \mid x^{\alpha(j_0)}$. Entonces, $x^{\alpha(i_0)} = p x^{\alpha(j_0)}$ con $p \in \mathbb{K}[x_1, \ldots, x_n]$. Podemos eliminar por tanto el monomio $x^{\alpha(i_0)}$ del sistema generador y el conjunto resultante seguiría siendo un sistema generador del ideal.

Si repetimos este proceso un número finito de veces, obtendremos un sistema generador $\{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\}$ con $s \leq k$ verificando que $x^{\alpha(i)} \nmid x^{\alpha(j)}$ $\forall i \neq j$.

Vamos a demostrar la unicidad. Supongamos que $\{x^{\beta(1)}, \ldots, x^{\beta(s)}\}$ es otra base mínima de $\mathfrak{I}$. Entonces, como $x^{\alpha(i)}, x^{\beta(i)} \in \mathfrak{I}$, por el Lema 2.16, tenemos que $x^{\beta(i)} \mid x^{\alpha(1)}$ y $x^{\alpha(j)} \mid x^{\beta(i)}$. De estas dos condiciones, tenemos que $x^{\alpha(j)} \mid x^{\alpha(1)}$ y como la base es mínima se tiene que $\alpha(j) = \alpha(1)$ y $\beta(i) = \alpha(1)$.

Por otra parte, podemos afirmar que $x_1^{a_1} \cdots x_n^{a_n} \mid x_1^{b_1} \cdots x_n^{b_n}$ si y solo si $a_i \leq b_i$ $\forall i$ y que $x_1^{b_1} \cdots x_n^{b_n} \mid x_1^{a_1} \cdots x_n^{a_n}$ si y solo si $b_i \leq a_i$ $\forall i$ y en consecuencia $a_i = b_i$. Aplicando esto al razonamiento anterior, tenemos que $\alpha(i) = \beta(i)$ y queda demostrada la unicidad. □

2.4. Bases de Gröbner

En esta sección vamos a tratar sistemas generadores de ideales en el anillo de polinomios. En particular vamos a centrarnos en un tipo de sistema generador con propiedades deseables para el estudio y resolución del problema de pertenencia.

Definición 2.21. *Sea $\mathfrak{I}$ un ideal no nulo de $\mathbb{K}[x_1, \ldots, x_n]$ y fijado un orden monomial en el anillo de polinomios. Denotamos por $\langle LM(\mathfrak{I}) \rangle$ al siguiente ideal de $\mathbb{K}[x_1, \ldots, x_n]$:*

$$\langle LM(\mathfrak{I}) \rangle = \langle LM(f) : f \in \mathfrak{I} - \{0\} \rangle$$

Observación 2.22. De manera análoga a $\langle LM(\mathfrak{I}) \rangle$, se puede definir el ideal de $\mathbb{K}[x_1, \ldots, x_n]$ siguiente:

$$\langle LT(\mathfrak{I}) \rangle = \langle x^\alpha : \exists f \in \mathfrak{I} - \{0\} \wedge LT(f) = c x^\alpha \rangle$$

Como $\mathbb{K}$ es un cuerpo, es claro que $\langle LM(\mathfrak{I}) \rangle = \langle LT(\mathfrak{I}) \rangle$, aunque en general esto no es cierto para cualquier anillo.

Proposición 2.23. *Sea $\mathfrak{I}$ un ideal no nulo de $\mathbb{K}[x_1, \ldots, x_n]$. Entonces:*

1. *$\langle LM(\mathfrak{I}) \rangle$ es un ideal monomial.*
2. *Existen $g_1, \ldots, g_t \in \mathfrak{I}$ tal que $\langle LM(\mathfrak{I}) \rangle = \langle LM(g_1), \ldots, LM(g_t) \rangle$.*

Demostración. La prueba de 1 es evidente, puesto que por definición $\langle LM(\mathfrak{I})\rangle$ está generado por monomios y en consecuencia es un ideal monomial. Que 2 se cumple es también consecuencia directa del Teorema de la base de Hilbert. □

Con todos estos resultados nos encontramos en condiciones de definir el sistema generador de los ideales del anillo de polinomios que nos permitirá resolver el problema de pertenencia.

Definición 2.24 (Base de Gröbner). *Fijado un orden monomial* " $\geq$ " *en* $\mathbb{K}[x_1,\ldots,x_n]$*, un subconjunto* $G = \{g_1,\ldots,g_t\}$ *de un ideal* $\mathfrak{I} \subseteq \mathbb{K}[x_1,\ldots,x_n]$*,* $\mathfrak{I} \neq \{0\}$ *se denomina base de Gröbner de* $\mathfrak{I}$ *respecto de* " $\geq$ " *si* $\langle LM(\mathfrak{I})\rangle = \langle LM(g_1),\ldots,LM(g_t)\rangle$.

Por convenio, $\langle\emptyset\rangle = \{0\}$ y consideramos $\emptyset$ la base de Gröbner del ideal $\{0\}$.

Proposición 2.25. *Fijado un orden monomial, todo ideal* $\mathfrak{I} \subseteq \mathbb{K}[x_1,\ldots,x_n]$ *admite una base de Gröbner. Es más, toda base de Gröbner de* $\mathfrak{I}$ *es un sistema generador del ideal.*

Demostración. Sea $\mathfrak{I}$ un ideal de $\mathbb{K}[x_1,\ldots,x_n]$. Si $\mathfrak{I} = \{0\}$, su base de Gröbner es $\emptyset$. Supongamos que $\mathfrak{I} \neq \{0\}$. De la Proposición 2.23 tenemos que existen $g_1,\ldots,g_t \in \mathfrak{I}$ tal que $\langle LM(\mathfrak{I})\rangle = \langle LM(g_1),\ldots,LM(g_t)\rangle$. Así, tenemos que $G = \{g_1,\ldots,g_t\}$ es una base de Gröbner de $\mathfrak{I}$ por definición.

Veamos ahora que en efecto, $\mathfrak{I} = \langle g_1,\ldots,g_t\rangle$.

" $\supseteq$ " Es trivial, puesto que $\{g_1,\ldots,g_t\} \subseteq \mathfrak{I}$.
" $\subseteq$ " Sea $f \in \mathfrak{J}$. Fijado un orden monomial, podemos realizar la división de f entre $(g_1,\ldots,g_t)$ luego $f = q_1g_1 + \cdots + q_tg_t + r$ y ninguno de los términos de r es divisible por $LT(g_i), 1 \leq i \leq t$. Vamos a demostrar que $r = 0$. Nótese que de la expresión anterior de f obtenemos que $r = f - q_1g_1 - \cdots - q_tg_t \in \mathfrak{J}$. Supongamos que $r \neq 0$. Entonces, se tiene que $LT(r) \in \langle LT(\mathfrak{I})\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$. Como $\langle LT(\mathfrak{I})\rangle$ es monomial, en virtud del Lema 2.16 existe $g_i \in G$ tal que $LT(r)$ es divisible por $LT(g_i)$ lo cual es absurdo puesto que r es el resto de la división.

Por tanto, $r = 0$ y $f = q_1g_1 + \cdots + q_tg_t$ y en consecuencia $f \in \langle g_1,\ldots,g_t\rangle$. □

2.5. Propiedades de las bases de Gröbner

En esta sección se pretende estudiar las propiedades de las bases de Gröbner, obtener un método para detectar cuándo el sistema generador de un ideal es una base de Gröbner así como un método para su cálculo. En primer lugar, vamos a demostrar que el resto de la división está determinado de forma única cuando se divide entre una base de Gröbner.

Proposición 2.26. *Sea $\mathfrak{I}$ un ideal de $\mathbb{K}[x_1,\ldots,x_n]$. Dado $f \in \mathbb{K}[x_1,\ldots,x_n]$ y fijado un orden monomial, existe un único $r \in \mathbb{K}[x_1,\ldots,x_n]$ verificando:*

1. *Ningún término de r pertenece a $\langle LT(\mathfrak{I})\rangle$.*
2. *Existe $g \in \mathfrak{I}$ tal que $f = g + r$.*

En particular, r es el resto de la división de f entre una base de Gröbner de $\mathfrak{I}$ sin importar el orden de los elementos de dicha base al realizar la división.

Demostración. Veamos en primer lugar la existencia. Sea $f \in \mathbb{K}[x_1,\ldots,x_n]$ y $G = \{g_1,\ldots,g_t\}$ una base de Gröbner. Si efectuamos la división de f entre G, obtenemos que $f = q_1g_1 + \cdots + q_tg_t + r$ donde r satisface la primera propiedad por el propio algoritmo de la división (ver Teorema 2.11). Además, si tomamos $g \coloneqq q_1g_1 + \cdots + q_tg_t$, tenemos que $f = g + r$.

En cuanto a la unicidad, supongamos que existe r' satisfaciendo las dos propiedades. De la segunda propiedad, tenemos que $f = g + r = g' + r'$ luego $r - r' = g' - g \in \mathfrak{I}$. Supongamos que $r \neq r'$. Entonces, $LT(r - r') \in \langle LT(\mathfrak{I})\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$ y por el Lema 2.16, $LT(r - r')$ es divisible por $LT(g_i)$ para cierto g_i con $i \in \{1,\ldots,t\}$. Sin embargo, esto no es posible en virtud de la primera propiedad, luego $r = r'$. □

Corolario 2.27. *Sean $\mathfrak{I}$ un ideal de $\mathbb{K}[x_1,\ldots,x_n]$, $G = \{g_1,\ldots,g_t\}$ una base de Gröbner de $\mathfrak{I}$ y $f \in \mathbb{K}[x_1,\ldots,x_n]$. Entonces:*

$$f \in \mathfrak{I} \iff \textit{El resto de la división de } f \textit{ entre } G \textit{ es cero.}$$

Demostración. " $\Leftarrow$ " Es evidente en virtud del Corolario 2.13.

" $\Rightarrow$ " Sea $f \in \mathfrak{I}$. Es claro que $f = f + 0$ luego tenemos una escritura de f como en la Proposición 2.26. Por tanto, $r = 0$ es el resto de la división de f entre G. □

Definición 2.28. *Denotaremos por $\bar{f}^F$ al resto de la división de f entre la s-tupla $F = (f_1,\ldots,f_s)$. Si F es una base de Gröbner de $\langle f_1,\ldots,f_s\rangle$, podemos considerar F un conjunto (sin ningún orden en particular).*

Observación 2.29. Sean $f, g \in \mathbb{K}[x_1,\ldots,x_n] - \{0\}$. Si $mdeg(f) = \alpha, mdeg(g) = \beta$ y $\gamma = (\gamma_1,\ldots,\gamma_s)$ donde $\gamma_i = máx\,(\alpha_i,\beta_i)$ para cada i, se tiene que x^γ es el mínimo común múltiplo de $LM(f)$ y $LM(g)$ y escribiremos $x^\gamma = mcm\,(LM(f), LM(g))$.

Definición 2.30 (S-polinomio). *Sean $f, g \in \mathbb{K}[x_1,\ldots,x_n] - \{0\}$. Se define el S-polinomio de f y g, denotado por $S(f,g)$ como:*

$$S(f,g) \coloneqq \frac{x^\gamma}{LT(f)}f - \frac{x^\gamma}{LT(g)}g$$

Lema 2.31. *Supongamos que tenemos una suma* $\sum_{i=1}^{s} p_i$ *con* $mdeg(p_i) = \delta \in \mathbb{N}^n$ *para todo* $1 \leq i \leq n$. *Si* $mdeg(\sum_{i=1}^{s} p_i) < \delta$, *entonces* $\sum_{i=1}^{s} p_i$ *es una* $\mathbb{K}$*-combinación lineal de los S-polinomios* $S(p_j, p_l)$ *con* $1 \leq j, l \leq s$.

Demostración. Llamamos $d_i = LC(p_i)$, luego $LT(p_i) = d_i x^{\delta}$ con $1 \leq i \leq s$. De que cada polinomio tiene multigrado exactamente δ y la suma tiene multigrado estrictamente menor que δ, es claro que $\sum_{i=1}^{s} d_i = 0$ puesto que se produce cancelación en los términos principales. Por tanto, $d_s = -d_1 - \cdots - d_{s-1}$.

Consideramos ahora el S-polinomio de p_i y p_j, que toma la expresión

$$S(p_i, p_j) = \frac{x^{\gamma}}{LT(p_i)} p_i - \frac{x^{\gamma}}{LT(p_j)} p_j = \frac{1}{d_i} p_i - \frac{1}{d_j} p_j$$

De aquí, teniendo en cuenta que $d_s = -d_1 - \cdots - d_{s-1}$ se obtiene fácilmente que $\sum_{i}^{s-1} d_i S(p_i, p_j) = \sum_{i=1}^{s} p_i$. Por tanto, hemos obtenido una expresión para la suma de los polinomios p_i como $\mathbb{K}$-combinación lineal de los S-polinomios.

□

Antes de presentar una condición necesaria y suficiente para caracterizar las bases de Gröbner, requerimos dos resultados auxiliares que enunciamos y demostramos a continuación.

Lema 2.32. *Sean* $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ *y* $S(f, g)$ *su S-polinomio. Entonces,* $mdeg(S(f, g)) < \gamma$ *donde* $x^{\gamma} = mcm(LM(f), LM(g))$.

Demostración. Consideremos que $mdeg(f) = \alpha$ y $mdeg(g) = \beta$. El S-polinomio de f y g toma la expresión

$$S(f, g) = \frac{x^{\gamma}}{LT(f)} f - \frac{x^{\gamma}}{LT(g)} g = x^{\gamma - \alpha} f - x^{\gamma - \beta} g$$

Donde $x^{\gamma} = mcm(LM(f), LM(g))$. Como $\alpha, \beta \geq 0$ por definición de multigrado, es evidente que $\gamma - \alpha < \gamma$ y $\gamma - \beta < \gamma$. Además, se tiene que $mdeg(x^{\gamma - \alpha} f) = \gamma$ y $mdeg(x^{\gamma - \beta}) = \gamma$. En consecuencia,

$$mdeg(S(f, g)) = mdeg(x^{\gamma - \alpha} f - x^{\gamma - \beta} g) < \gamma$$

□

Lema 2.33. *Supongamos que* $ax^{\alpha} f$ *y* $bx^{\beta} g$ *tienen multigrado* δ. *Entonces,*

$$S(x^{\alpha} f, x^{\beta} g) = x^{\delta - \gamma} S(f, g)$$

donde $x^{\gamma} = mcm(LM(f), LM(g))$.

Demostración. Por hipótesis $ax^\alpha f$ y $bx^\beta g$ tienen multigrado δ. Podemos afirmar pues que $x^\delta = x^\alpha \cdot LT(f) = x^\beta \cdot LT(g)$. Además, se tiene que:

$$S(x^\alpha f, x^\beta g) = \frac{x^\mu}{x^\alpha LT(f)} x^\alpha g - \frac{x^\mu}{x^\beta LT(f)} x^\beta g = x^\mu \left(\frac{1}{LT(f)} f - \frac{1}{LT(g)} g \right)$$

$$S(f, g) = \frac{x^\eta}{LT(f)} f - \frac{x^\eta}{LT(g)} g$$

donde $x^\mu = mcm(x^\alpha LM(f), x^\beta LM(g))$ y $x^\eta = mcm(LM(f), LM(g))$

Si probamos que $x^\mu = x^{\delta-\gamma} \cdot x^\eta$ con $\gamma = mcm(LM(g_i), LM(g_j))$ habríamos acabado. En efecto, de que los polinomios iniciales tengan multigrado δ, tenemos que $x^\mu = x^\delta$. Por otra parte, de la expresión de $S(g_i, g_j)$ y de la definición de x^γ, es claro que $x^\eta = x^\gamma$. Por tanto, se verifica la igualdad y en consecuencia los S-polinomios considerados son iguales. □

Nos encontramos en condiciones de enunciar un resultado esencial en la teoría de bases de Gröbner, que nos permitirá caracterizar estos objetos algebraicos en términos de los S-polinomios y el algoritmo de division.

Teorema 2.34 (Criterio de Buchberger). *Sea $\mathfrak{I}$ un ideal de $\mathbb{K}[x_1, \ldots, x_n]$ y sea $G = \{g_1, \ldots, g_n\}$ un sistema generador de $\mathfrak{I}$. Fijado un orden monomial " $\geq$ ", G es base de Gröbner de $\mathfrak{I}$ si y solo si para todo $i \neq j$, el resto de dividir $S(g_i, g_j)$ entre G (en cualquier orden) es cero.*

Demostración. " $\Rightarrow$ " Como $g_i, g_j \in \mathfrak{I}$ es claro que $S(g_i, g_j) \in \mathfrak{I}$. Combinando esto con la hipótesis de que G es base de Gröbner de $\mathfrak{I}$ y en virtud del Corolario 2.27, se tiene que $\overline{S(g_i, g_j)}^G = 0$.

" $\Leftarrow$ " Sean $f \in \mathfrak{I}$, $f \neq 0$ y " $\geq$ " un orden monomial. Veamos que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$. Como $f \in \mathfrak{I}$, $f = \sum_{i=1}^t h_i g_i$ donde $h_i \in \mathbb{K}[x_1, \ldots, x_n]$. Por la Proposición 2.10, $mdeg(f) \leq máx\,(mdeg(h_i g_i : h_i g_i \neq 0))$. Denotamos $\delta = máx\,(mdeg(h_i g_i : h_i \neq 0))$ y tomamos una escritura de f tal que δ es minimal en $\mathbb{N}^n$. Se tiene pues que $mdeg(f) \leq \delta$.

Distinguimos a continuación dos casos:

- Si $mdeg(f) = \delta$ se tiene que $mdeg(f) = mdeg(g_i h_i)$ para cierto i. Entonces, $LT(f)$ es divisible por $LT(g_i)$ para cierto i y en consecuencia $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$, lo que concluiría la demostración.
- Si $mdeg(f) < \delta$ con δ minimal, podemos reescribir f como sigue:

$$f = \sum_{i=1}^t h_i g_i = \sum_{mdeg(h_i g_i) = \delta} h_i g_i + \sum_{mdeg(h_i g_i) < \delta} h_i g_i$$

$$= \sum_{mdeg(h_i g_i)=\delta} LT(h_i)g_i + \sum_{mdeg(h_i g_i)<\delta} (h_i - LT(h_i))g_i + \sum_{mdeg(h_i g_i)<\delta} h_i g_i$$

Como $mdeg(f) < \delta$, cada uno de los sumandos de esta expresión tiene también multigrado menor que δ. Además, podemos reescribir el primer sumando en términos de los S-polinomios en virtud del Lema 2.31. En efecto, $\sum_{mdeg(g_i h_i)=\delta} LT(h_i)g_i$ tiene multigrado menor que δ y si denotamos $p_i = h_i g_i$, cada uno de estos polinomios tiene multigrado exactamente δ. Por tanto, la suma es $\mathbb{K}$-combinación lineal de los $S(p_i, p_j)$.

Además, empleando el Lema 2.33, se tiene que $S(p_i, p_j) = x^{\delta-\gamma_{ij}} S(g_i, g_j)$ donde $x^{\gamma_{ij}} = mcm(LM(g_i), LM(g_j))$. Entonces, dicha suma es en particular $\mathbb{K}$-combinación lineal de $x^{\delta-\gamma_{ij}} S(g_i, g_j)$ para ciertos i, j.

Consideramos el S-polinomio de g_i y g_j, $S(g_i, g_j)$. Por hipótesis, $\overline{S(g_i, g_j)}^{G} = 0$ y en virtud del algoritmo de división, existen $A_l \in \mathbb{K}[x_1, \ldots, x_n]$ con $1 \leq l \leq t$ verificando que $S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l$ donde $mdeg(A_l g_l) \leq mdeg(S(g_i, g_j))$ si $A_l g_l \neq 0$. Multiplicando esta expresión por $x^{\delta-\gamma_{ij}}$, se tiene que $x^{\delta-\gamma_{ij}} S(g_i, g_j) = \sum_{l=1}^{t} B_l g_l$ denotando $B_l := x^{\delta-\gamma_{ij}} A_l$.

Si $B_l g_l \neq 0$, es claro que $mdeg(B_l g_l) \leq mdeg(x^{\delta-\gamma_{ij}} S(g_i, g_j)) < \delta$ y por el Lema 2.32 se obtiene que $LT(S(g_i, g_j)) < mcm(LM(g_i), LM(g_j)) = x^{\gamma_{ij}}$. De aquí, $\sum_{mdeg(h_i g_i)=\delta} LT(h_i)g_i = \sum_{l=1}^{t} \tilde{B}_l g_l$ con $mdeg(\tilde{B}_l g_l) < \delta$ si $\tilde{B}_l g_l \neq 0$.

Introduciendo esta escritura en la descomposición de f en tres sumandos, se tiene que

$$f = \sum_{l=1}^{t} \tilde{B}_l g_l + \sum_{mdeg(h_i g_i)<\delta} (h_i - LT(h_i))g_i + \sum_{mdeg(h_i g_i)<\delta} h_i g_i$$

Es decir, hemos escrito f como suma de polinomios donde cada uno de ellos tiene multigrado menor que δ, lo cual es absurdo por la minimalidad de δ establecida al inicio. En consecuencia, el caso $mdeg(f) < \delta$ no puede darse y se tiene que G es base de Gröbner de $\mathfrak{I}$. □

Teorema 2.35 (Algoritmo de Buchberger). *Sea $\mathfrak{I} = \langle f_1, \ldots, f_s \rangle$ ideal de $\mathbb{K}[x_1, \ldots, x_n]$. El siguiente algoritmo construye una base de Gröbner de $\mathfrak{I}$ en un*

número finito de pasos.

Algoritmo 2: Algoritmo de Buchberger.

Entrada: $F = (f_1, \ldots, f_s)$ *sistema generador de* $\mathfrak{I}$.
Salida: $G = (g_1, \ldots, g_t)$ *base de Gröbner de* $\mathfrak{I}$, *con* $F \subseteq G$.
$G \coloneqq F$
repetir
  $\tilde{G} \coloneqq G$. *Para cada par* $\{p, q\}$ *con* $p \neq q$ *en* $\tilde{G}$ *hallar* $r \coloneqq \overline{S(p,q)}^{\tilde{G}}$
  si $r \neq 0$ **entonces**
    $G \coloneqq G \cup \{r\}$
  fin
hasta que $G = \tilde{G}$;
devolver G

Demostración. Vamos a demostrar que el algoritmo finaliza en un número finito de pasos. Supongamos por reducción al absurdo que no es cierto. Entonces, en cada paso se construiría un conjunto G_i que contiene estrictamente a G_{i-1} de manera que se tendría la cadena

$$G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \cdots$$

donde $G_i = G_{i-1} \cup \{r\}$. Es claro entonces que $LT(r) \notin \langle LT(G_{i-1})\rangle$, lo que permite construir la siguiente cadena de ideales monomiales:

$$\langle LT(G_1)\rangle \subsetneq \langle LT(G_2)\rangle \subsetneq \langle LT(G_3)\rangle \subsetneq \cdots$$

Es decir, tendríamos una cadena ascendente de ideales monomiales del anillo $\mathbb{K}[x_1, \ldots, x_n]$ infinita. Esto es absurdo dado que $\mathbb{K}[x_1, \ldots, x_n]$ es un anillo noetheriano en virtud del Teorema 2.1, luego la cadena de ideales ha de estabilizarse y en consecuencia el algoritmo termina en un número finito de pasos.

Por otra parte, $F = \{f_1, \ldots, f_s\} \subseteq \{g_1, \ldots, g_t\} = G$ y se tiene por hipótesis que $\mathfrak{I} = \langle f_1, \ldots, f_s\rangle$. Por tanto, $\mathfrak{I} = \langle g_1, \ldots, g_t\rangle$. Finalmente, si tomamos $g_i, g_j \in G$ con $i \neq j$, podemos considerar $S(g_i, g_j) \in \mathfrak{I}$. Como $\overline{S(g_i, g_j)}^{G} = 0$ por construccion, se tiene por el Teorema 2.34 que G es base de Gröbner de $\mathfrak{I}$. □

La elección del orden monomial condiciona la forma que tienen las bases de Gröbner de un ideal. Esto es, para un mismo ideal, considerando dos órdenes monomiales diferentes en general se obtienen bases de Gröbner diferentes. A continuación mostramos un ejemplo de ello.

Ejemplo 2.36. Consideramos el anillo de polinomios $\mathbb{Q}[x, y]$ y el orden monomial lexicográfico graduado $>_{grlex}$. Sea $\mathfrak{I} = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Una base de

Gröbner de $\mathfrak{I}$ respecto de $>_{grlex}$ es $G = \{x^2, xy, 2y^2 - x\}$.

Consideremos ahora el orden monomial lexicográfico $>_{lex}$. Para el mismo ideal $\mathfrak{I}$, una base de Gröbner respecto de $>_{lex}$ es $G' = \{y^3, x - 2y^2\}$.

Por último, empleando el orden lexicográfico inverso graduado $>_{grevlex}$, una base de Gröbner de $\mathfrak{I}$ es $G'' = \{x^2, xy, -x + 2y^2\} = G$.

2.6. Aplicaciones de las bases de Gröbner

2.6.1. Ideales de eliminación

Definición 2.37. *Sea $\mathfrak{I} = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Se define el l-ésimo ideal de eliminación como el ideal de $\mathbb{K}[x_{l+1}, \ldots, x_n]$:*

$$\mathfrak{I}_l = \mathfrak{I} \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$$

.

Nótese que los polinomios de $\mathfrak{I}_l$ son aquellos polinomios de $\mathfrak{I}$ que no contienen las l primeras variables.

Teorema 2.38 (Eliminación). *Sea $\mathfrak{I} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal y G una base de Gröbner de $\mathfrak{I}$ respecto de $\geq_{lex}$ con $x_1 \geq_{lex} x_2 \geq_{lex} \cdots \geq_{lex} x_n$. Entonces, para todo $0 \leq l \leq n$, $G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$ es una base de Gröbner de $\mathfrak{I}_l$.*

Demostración. Sea $0 \leq l \leq n$. Como $G \subseteq \mathfrak{I}$, es claro que $G_l \subseteq \mathfrak{I}_l$. Solo hemos de probar que $\langle LT(\mathfrak{I}_l) \rangle = \langle LT(G_l) \rangle$.

" $\supseteq$ " Es evidente puesto que $G_l \subseteq \mathfrak{I}_l$ luego $LT(G_l) \subseteq LT(\mathfrak{I}_l)$ y en consecuencia $\langle LT(G_l) \rangle \subseteq \langle LT(\mathfrak{I}_l) \rangle$.

" $\subseteq$ " Sea $f \in \mathfrak{I}_l$ y consideremos su término principal $LT(f)$. Basta ver que $LT(f)$ es divisible por $LT(g)$ para algún $g \in G_l$. En efecto, como $f \in \mathfrak{I}$ y G es base de Gröbner de $\mathfrak{I}$, existe $g \in G$ tal que $LT(f)$ es divisible por $LT(g)$. Por otra parte, $f \in \mathfrak{I}_l$ y como $LT(g) \mid LT(f)$, se tiene que $LT(g) \in \mathbb{K}[x_{l+1}, \ldots, x_n]$.

Además, por hipótesis todo monomio en el que aparezca alguna de las variables $x_1, \ldots, x_l$ es mayor que los monomios de $\mathbb{K}[x_{l+1}, \ldots, x_n]$. Por tanto, $g \in \mathbb{K}[x_{l+1}, \ldots, x_n]$ ya que su término principal pertenece a este anillo y el resto de términos son menores. Entonces, se tiene que $g \in G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$ luego $LT(f)$ es divisible por $LT(g)$ para cierto $g \in G_l$ y se tiene la inclusión. □

2.6.2. Estudio del $\mathbb{K}$-espacio vectorial $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$

Proposición 2.39. *El anillo* $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$ *donde* $\mathfrak{I}$ *es un ideal de* $\mathbb{K}[x_1, \ldots, x_n]$ *tiene estructura de espacio vectorial.*

Demostración. A continuación se presentan las operaciones que dotan a $R = \mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$ de estructura de espacio vectorial. Como operación interna consideramos $+ : R \times R \longrightarrow R$ donde $\overline{x} + \overline{y} = \overline{x+y}$. Para la operación externa definimos $\cdot : \mathbb{K} \times R \longrightarrow R$ donde $a \cdot \overline{x} = \overline{ax}$. Es fácil comprobar que con estas operaciones $(R, +, \cdot)$ es un espacio vectorial sobre $\mathbb{K}$. □

Sabemos que todo espacio vectorial admite una base, es decir, un sistema libre y generador. El siguiente resultado establece una base de $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$ como espacio vectorial.

Proposición 2.40. *El conjunto* $\mathfrak{B} := \{\overline{x^\alpha} : x^\alpha \notin \langle LT(\mathfrak{I})\rangle\}$ *es una base de* $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}$ *como espacio vectorial.*

Demostración. Consideremos una base de Gröbner $G = \{g_1, \ldots, g_s\}$ respecto del orden monomial " $\geq$ " del ideal $\mathfrak{I}$.

Veamos en primer lugar que $\mathfrak{B}$ es sistema libre. Sean $\beta_1, \ldots, \beta_s \in \mathbb{K}$ tal que $f = \beta_1\overline{x^{\alpha_1}} + \cdots + \beta_s\overline{x^{\alpha_s}} = \overline{0}$. De aquí, se tiene que $\overline{\beta_1 x^{\alpha_1} + \cdots + \beta_s x^{\alpha_s}} = \overline{0}$. Los representantes módulo $\mathfrak{I}$ en el espacio cociente son los restos al efectuar la división entre G. Por tanto, $\overline{\beta_1 x^{\alpha_1} + \cdots + \beta_s x^{\alpha_s}} = \overline{\bar{f}^G} = \overline{0}$. De aquí se deduce que $\bar{f}^G = \overline{0}$ y en virtud del Corolario 2.27 se obtiene que $\overline{f^G} = 0$ y consecuentemente que $\beta_1 = \cdots = \beta_s = 0$.

A continuación veamos que $\mathfrak{B}$ es sistema generador. Sea $f \in \mathbb{K}[x_1, \ldots, x_n]$. Como G es base de Gröbner de $\mathfrak{I}$, se tiene que $\langle LT(\mathfrak{I})\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$. Por el Teorema 2.11, tenemos que $f = \sum_{i=1}^s h_i g_i + r$ donde $h_i, r \in \mathbb{K}[x_1, \ldots, x_n]$ donde ningún termino de r es divisible por $LT(g_i)$ para $1 \leq i \leq s$. Tomando clases módulo $\mathfrak{I}$, es claro que $\overline{f} = \overline{\sum_{i=1}^s h_i g_i + r} = \overline{r} = \overline{\bar{f}^G}$. Dado que ningún termino de r es divisible por $LT(g_i)$ y $\langle LT(\mathfrak{I})\rangle$ es un ideal monomial, podemos afirmar por el Lema 2.16 que $r \notin \langle LT(\mathfrak{I})\rangle$. Además, r es $\mathbb{K}$-combinación lineal de monomios que en particular no pertenecen a $\langle LT(\mathfrak{I})\rangle$ luego se tiene que $\mathfrak{B}$ es sistema generador. □

2.6.3. Bases de Gröbner de ideales binomiales

En este capítulo se han estudiado ampliamente los ideales monomiales en el anillo de polinomios. Se pretende determinar qué consecuencias tiene que el sistema generador de los ideales de $\mathbb{K}[x_1, \ldots, x_n]$ contenga también binomios, cuya definición introducimos a continuación.

Definición 2.41. *Un binomio en* $\mathbb{K}[x_1, \ldots, x_n]$ *es toda expresión de la forma* $x^\alpha - x^\beta$*, donde* x^α *y* x^β *son monomios. A todo ideal generado por binomios se le denomina ideal binomial.*

Lema 2.42. *Si la entrada del algoritmo de Buchberger descrito en el Teorema 2.35 es un conjunto de binomios, la salida también es un conjunto de binomios. Si la entrada contiene monomios y binomios, la salida contiene monomios y binomios.*

Demostración. Vamos a demostrar en primer lugar que el S-polinomio de dos monomios es cero, que el de un monomio y un binomio es un monomio y que el de dos binomios es nuevamente un binomio o cero. Sea " $\geq$ " un orden monomial. En efecto,

$$S(x^\alpha, x^\beta) = \frac{x^\gamma}{LT(x^\alpha)} x^\alpha - \frac{x^\gamma}{LT(x^\beta)} x^\beta = x^\gamma - x^\gamma = 0$$

donde $x^\gamma = mcm\left(x^\alpha, x^\beta\right)$.

$$S(x^\alpha, x^\beta - x^\gamma) = \frac{x^\delta}{LT(x^\alpha)} x^\alpha - \frac{x^\delta}{LT(x^\beta - x^\gamma)} x^\beta - x^\gamma = x^{\delta-\gamma+\beta}$$

donde $x^\delta = mcm\left(x^\alpha, x^\beta - x^\gamma\right)$ y $x^\beta \geq x^\gamma$

$$\begin{aligned} S(x^\alpha - x^\beta, x^\gamma - x^\delta) &= \frac{x^\varepsilon}{LT(x^\alpha - x^\beta)} \left(x^\alpha - x^\beta\right) - \frac{x^\varepsilon}{LT(x^\gamma - x^\delta)} \left(x^\gamma - x^\delta\right) \\ &= x^{\varepsilon-\gamma+\delta} - x^{\varepsilon-\alpha+\delta} \end{aligned}$$

donde $x^\varepsilon = mcm(x^\alpha - x^\beta, x^\gamma - x^\delta)$ y $x^\alpha \geq x^\beta, x^\gamma \geq x^\delta$.

Queda estudiar qué ocurre con el resto de la división. Supongamos que queremos dividir un monomio x^α entre $F = \{f_1, \ldots, f_s\}$ con f_i monomios o binomios. Si $LT(f_i) \nmid x^\alpha, \forall i$ se tiene que el resto de la división es $r = x^\alpha$. En caso contrario, sea $i = min\{j : LT(f_j) \mid x^\alpha\}$. Distinguimos dos casos:

1. Si f_i es un monomio tenemos que $x^\alpha - x^{\alpha-\beta} x^\beta = 0$ luego $\overline{x^\alpha}^F = \overline{0}^F = 0$.
2. Si f_i es un binomio, $x^\alpha - x^{\alpha-\beta}(x^\beta - x^\gamma) = x^{\alpha-\beta+\gamma}$ luego $\overline{x^\alpha}^F = \overline{x^{\alpha-\beta+\gamma}}^F$ que es un monomio.

Por tanto, al dividir un monomio el resto obtenido es cero o un monomio.

Supongamos que queremos dividir un binomio $x^\alpha - x^\beta$ entre $F = \{f_1, \ldots, f_s\}$ con f_i monomios o binomios y $x^\alpha \geq x^\beta$ para cierto orden monomial. Nuevamente, si $LT(f_i) \nmid x^\alpha, \forall i$ tenemos que el resto de la division es $r = x^\alpha - \overline{x^\beta}^F$. Claramente x^α es un monomio y aplicando el razonamiento anterior, $\overline{x^\beta}^F$ es un

cero o un monomio, luego el resto es un monomio o un binomio, respectivamente.

En caso contrario, sea $i = min\{j : LT(f_j) \mid x^\alpha\}$. Se distinguen dos casos:

1. Si $f_i = x^\gamma$, tenemos que $x^\alpha - x^\beta - x^{\alpha-\gamma}x^\gamma = -x^\beta$ y en consecuencia $\overline{f_i}^F = \overline{-x^\beta}^F$ y como x^β es un monomio, el resto es cero o un monomio.
2. Si $f_i = x^\gamma - x^\delta$ es un binomio, $x^\alpha - x^\beta - x^{\alpha-\gamma}\left(x^\gamma - x^\delta\right) = -x^\beta + x^{\alpha-\gamma+\delta}$ y por tanto $\overline{f_i}^F = \overline{x^{\alpha-\gamma+\delta}}^F$. Como se efectúa el resto de un monomio, este es cero o un monomio. □

3

Estudio de semigrupos numéricos mediante bases de Gröbner

En este tercer capítulo conectaremos la Teoría de Semigrupos numéricos y la Teoría de Bases de Gröbner estudiada en los capítulos anteriores. Traduciremos el problema de pertenencia a un semigrupo numérico en términos del resto de una división. Introduciremos una nueva graduación de los monomios y empleando Bases de Gröbner, estableceremos una biyección entre el conjunto de Apéry de un elemento del semigrupo y las bases del anillo cociente visto como espacio vectorial. Empleando dicha biyección calcularemos el conjunto de Apéry.

3.1. El problema de pertenencia a un semigrupo

Sean $S = \langle a_1, \ldots, a_n \rangle$ un semigrupo numérico y $b \in \mathbb{N}$. El problema de pertenencia a S consiste en determinar si $b \in S$, es decir, si existen $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ tales que $b = \sum_{i=1}^{n} \alpha_i a_i$.

Con el fin de resolver este problema, asociamos a S un ideal que denotaremos por $\mathfrak{J}_S \subseteq \mathbb{K}[x_1, \ldots, x_n, t]$ definido como

$$\mathfrak{J}_S = \langle x_1 - t^{a_1}, \ldots, x_n - t^{a_n} \rangle$$

Es claro que $\mathfrak{J}_S$ es un ideal binomial, puesto que sus generadores son binomios de $\mathbb{K}[x_1, \ldots, x_n, t]$. Como se ha ilustrado en el capítulo interior, determinar la pertenencia en un ideal no monomial no es trivial. No obstante, el siguiente resultado muestra un criterio para verificar si un binomio pertenece al ideal $\mathfrak{J}_S$ citado anteriormente.

Lema 3.1 (Pertenencia de binomios al ideal $\mathfrak{J}_S$).

$$x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha} - x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta} \in \mathfrak{J}_S \iff \sum_{i=1}^{n}\alpha_i a_i + \alpha = \sum_{i=1}^{n}\beta_i a_i + \beta$$

Demostración. Sea $\varphi : \mathbb{K}[x_1,\ldots,x_n,t] \longmapsto \mathbb{K}[s]$ el único homomorfismo de anillos tal que $\varphi(x_i) = s^{a_i}$, $\varphi(t) = s$ y $\varphi|_{\mathbb{K}} = id_{\mathbb{K}}$. Veamos la doble implicación:

" $\Rightarrow$ ") Sea $F = x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha} - x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta} \in \mathfrak{J}_S$. Por pertenecer a $\mathfrak{J}_S$, existen $f_1,\ldots,f_n$ tales que $F = \sum_{i=1}^{n} f_i\,(x_i - t^{a_i})$. Aplicando el homomorfismo φ, se tiene que:

$$\varphi(F) = \sum_{i=1}^{n}\varphi(f_i)\,(\varphi(x_i) - \varphi(t^{a_i})) = \sum_{i=1}^{n}\varphi(f_i)\,(s^{a_i} - s^{a_i}) = 0$$

Por tanto, $\varphi(F) = 0$ luego $\varphi(x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha}) = \varphi(x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta})$. Nuevamente, de que φ sea homomorfismo de anillos se tiene que $\varphi(x_1^{\alpha_1})\cdots\varphi(x_n^{\alpha_n})\varphi(t^{\alpha}) = \varphi(x_1^{\beta_1})\cdots\varphi(x_n^{\beta_n})\varphi(t^{\beta})$ luego $s^{\sum_{i=1}^{n}\alpha_i a_i+\alpha} = s^{\sum_{i=1}^{n}\beta_i a_i+\beta}$ y en consecuencia $\sum_{i=1}^{n}\alpha_i a_i + \alpha = \sum_{i=1}^{n}\beta_i a_i + \beta$.

" $\Leftarrow$ ") Sean $m_1 = x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha}$ y $m_2 = x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta}$ monomios tales que $\sum_{i=1}^{n}\alpha_i a_i+\alpha = \sum_{i=1}^{n}\beta_i a_i+\beta$. Demostrar que $m_1 - m_2 \in \mathfrak{J}_S$ es equivalente a probar que las clases de m_1 y m_2 son iguales en el anillo cociente $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{J}_S$. Como $x_i - t^{a_i} \in \mathfrak{J}_S$, se tiene que $\overline{x_i} = \overline{t^{a_i}}$. Asi, podemos afirmar que:

$$\begin{aligned}
\overline{m_1} &= \overline{x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha}} \\
&= \overline{t^{\alpha_1 a_1}\ldots t^{\alpha_n a_n}t^{\alpha}} \\
&= \overline{t^{\sum_{i=1}^{n}\alpha_i a_i+\alpha}} \\
&= \overline{t^{\sum_{i=1}^{n}\beta_i a_i+\beta}} \\
&= \overline{t^{\beta_1 a_1}\cdots t^{\beta_n a_n}t^{\beta}} = \overline{x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta}} = \overline{m_2}
\end{aligned}$$

Por tanto, como $\overline{m_1} = \overline{m_2}$, tenemos que $m_1 - m_2 \in \mathfrak{J}_S$. □

Este resultado en conjunto con la teoría de bases de Gröbner nos permite presentar una proposición, la cual ofrece una condición necesaria y suficiente para la pertenencia a un semigrupo numérico.

Proposición 3.2. *Sea G una base de Gröbner de $\mathfrak{J}_S$ respecto de $>_{lex}$ con $t >_{lex} x_1 >_{lex} \cdots >_{lex} x_n$ y sea S un semigrupo numérico. Entonces:*

$$b \in S \iff \overline{t^b}^{G} \in \mathbb{K}[x_1,\ldots,x_n]$$

Demostración. " $\Rightarrow$ ") Sea $b \in S$. Entonces, existen $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ tales que $b = \sum_{i=1}^{n} \alpha_i a_i$ y consecuentemente, $t^b - x^{\alpha_1} \cdots x^{\alpha_n} \in \mathfrak{J}_S$.

Sabemos que el resto de la división de este polinomio por G no tiene ningún monomio en $LT(\mathfrak{J}_S)$. Además, como $\mathfrak{J}_S$ es un ideal binomial, en virtud del Lema 2.42, G está conformada por binomios y además, el resto de la división de un monomio entre dicha base es un monomio. Por tanto, podemos afirmar que $\overline{t^b}^G = x^\beta t^\gamma$. Supongamos que $\gamma \neq 0$. Es claro entonces que $x^\beta t^\gamma - t^b \in \mathfrak{J}_S$ y además $t^b - x^\alpha \in \mathfrak{J}_S$ luego $\left(x^\beta t^\gamma - t^b\right) + \left(t^b - x^\alpha\right) = x^\beta t^\gamma - x^\alpha \in \mathfrak{J}_S$ con $LM(x^\beta t^\gamma - x^\alpha) = x^\beta t^\gamma$. Tendríamos pues que $\overline{t^b}^G = x^\beta t^\gamma \in LM(\mathfrak{J}_S) \subseteq LT(\mathfrak{J}_S)$ lo cual es absurdo, luego necesariamente $\gamma = 0$ y $\overline{t^b}^G = x^\beta \in \mathbb{K}[x_1, \ldots, x_n]$.

" $\Leftarrow$ ") Supongamos que $\overline{t^b}^G \in \mathbb{K}[x_1, \ldots, x_n]$. Por las consideraciones anteriores, este resto es un monomio, luego podemos escribir $\overline{t^b}^G = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ con $\alpha_i \in \mathbb{N}$ y en consecuencia $t^b - x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathfrak{J}_S$. Por el Lema 3.1 se tiene que $b = \alpha_1 a_1 + \cdots + \alpha_n a_n \in S$. □

Este resultado nos proporciona un algoritmo para resolver el problema de pertenencia a un semigrupo. A continuación presentamos dicho algoritmo.

Algoritmo 3: Algoritmo para verificar la pertenencia a un semigrupo numérico S.

Entrada: $\{a_1, \ldots, a_n\}$ sistema generador del semigrupo numérico S, $b \in \mathbb{N}$.
Salida: 1 si $b \in S$, 0 en caso contrario.
1. Definir $\mathfrak{J}_S = \langle x_1 - t^{a_1}, \ldots, x_n - t^{a_n} \rangle$.
2. Calcular G base de Gröbner de $\mathfrak{J}_S$ respecto de $>_{lex}$ con $t > x_1 > \ldots > x_n$.
3. Calcular el resto $\overline{t^b}^G$.
si $\overline{t^b}^G \in \mathbb{K}[x_1, \ldots, x_n]$ **entonces**
  $\overline{t^b}^G = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$
  return 1
fin
en otro caso
  return 0
fin

Nótese que el algoritmo nos devuelve, en el caso de que se verifique la condición de pertenencia, un monomio $\overline{t^b}^G = x^{\alpha_1} \cdots x^{\alpha_n}$. Los coeficientes α_i con $1 \leq i \leq n$ son exactamente los que dan la escritura de b como combinación de los generadores del semigrupo numérico S, es decir, $b = \sum_{i=1}^{n} \alpha_i a_i$.

Analizando detenidamente la prueba anterior obtenemos aún más información. En caso de que b no pertenezca al semigrupo, podemos determinar cuál es la menor cantidad que hay que restarle a b para el que el resultado sí pertenezca al semigrupo. Este fenómeno se recoge en el siguiente resultado.

Proposición 3.3. *Sea $b \in \mathbb{N} - S$ y G una base de Gröbner respecto de $<_{lex}$ con $t > x_1 > \cdots > x_n$ tal que $\overline{t^b}^G = t^\gamma x^{\alpha_1} \cdots x^{\alpha_n}$ con $\gamma \geq 1$. Entonces, $b - i \notin S$ $\forall i < \gamma$ y $b - \gamma \in S$.*

Demostración. Como $\overline{t^b}^G = t^\gamma x^{\alpha_1} \cdots x^{\alpha_n}$ es claro que $t^b - t^\gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathfrak{J}_S$ donde $t^\gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n} \notin LM(\mathfrak{J}_S)$.

Supongamos por reducción al absurdo que existe $i \in \{0, \ldots, \gamma - 1\}$ tal que $b - i \in S$. Entonces, $\overline{t^{b-i}}^G = x_1^{\beta_1} \cdots x_n^{\beta_n}$ donde $\beta_i \in \mathbb{N}$, $1 \leq i \leq n$. Podemos afirmar entonces que $t^{b-i} - x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathfrak{J}_S$ y naturalmente $t^b - t^i x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathfrak{J}_S$. Dado que $\mathfrak{J}_S$ es un ideal, la diferencia de elementos de este pertenece también al ideal luego $g \coloneqq (t^b - t^i x_1^{\beta_1} \cdots x_n^{\beta_n}) - (t^b - t^\gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = t^\gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n} - t^i x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathfrak{J}_S$. Por hipótesis, $i < \gamma$ lo que implica que $LM(g) = t^\gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in LM(\mathfrak{J}_S)$ lo cual es absurdo.

Por tanto, $b - i \notin S$ $\forall i < \gamma$. Veamos ahora que $b - \gamma \in S$. En efecto, $t^b - t^\gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathfrak{J}_S$. Por el Lema 3.1, podemos escribir $b = \gamma + \alpha_1 a_1 + \cdots + \alpha_n a_n$ con $\alpha_i \in N$, $a_i \in S$, $1 \leq i \leq n$ y consecuentemente $b - \gamma = \alpha_1 a_1 + \cdots + \alpha_n a_n \in S$. □

Ejemplo 3.4. Consideramos el semigrupo numérico $S = \langle 7, 8, 10 \rangle$ y el anillo de polinomios $\mathbb{Q}[x, y, z, t]$ con el orden monomial $>_{lex}$ donde $t >_{lex} x >_{lex} y >_{lex} z$. El ideal asociado a S es $\mathfrak{J}_S = \langle x - t^7, y - t^8, z - t^{10} \rangle$ y mediante el algoritmo de Buchberger (Teorema 2.35) se tiene que una base de Gröbner de $\mathfrak{J}_S$ respecto a este orden es $G = \{y^5 - z^4, x^2 z - y^3, x^2 y^2 - z^3, x^4 - yz^2, tz^2 - x^3, ty^2 - xz, tx - y, t^2 y - z, t^4 z - x^2, t^7 - x\}$.

Queremos determinar si $19 \in S$. Para ello, consideramos el monomio t^{19}. Calculamos el resto de dividir dicho monomio entre G y obtenemos que $\overline{t^{19}}^G = tyz \notin \mathbb{Q}[x, y, z]$ luego en virtud del Teorema 3.2 tenemos que $19 \notin S$. Si ahora realizamos el mismo proceso para determinar si $18 \in S$, tenemos que $\overline{t^{18}}^G = yz \in \mathbb{Q}[x, y, z]$ luego por el Teorema 3.2, tenemos que $18 \in S$. En efecto, $18 = 10 + 8 \in S$.

3.2. Cálculo del conjunto de Apéry

En el primer capítulo tratamos el conjunto de Apéry con respecto a un elemento del semigrupo numérico S, el cual recordamos que se define como $Ap(S,b) = \{s \in S : s - b \notin S\}$. Vamos a estudiar qué relación existe entre este objeto y la teoría de bases de Gröbner.

Con el fin de simplificar la notación, introducimos una nueva graduación de $\mathbb{K}[x_1,\dots,x_n,t]$, el S-grado.

Definición 3.5. *Sea $S = \langle a_1,\dots,a_n\rangle$ un semigrupo numérico. Se define el S-grado de $\mathbb{K}[x_1,\dots,x_n,t]$ como $deg_S(x_i) = a_i, 1 \le i \le n$, $deg_S(t) = 1$ y $deg_S(k) = 0$, $\forall k \in \mathbb{K} - \{0\}$.*

El S-grado posee propiedades análogas a las del grado usual con respecto al producto de monomios.

Observación 3.6. La introducción del S-grado permite reescribir el resultado expuesto en el Lema 3.1 como sigue:

$$x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha} - x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta} \in \mathfrak{J}_S \iff deg_S(x_1^{\alpha_1}\cdots x_n^{\alpha_n}t^{\alpha}) = deg_S(x_1^{\beta_1}\cdots x_n^{\beta_n}t^{\beta})$$

Nota:. Denotaremos por $\mathfrak{I}$ al ideal definido como $\mathfrak{I} \coloneqq \mathfrak{J}_S \cap \mathbb{K}[x_1,\dots,x_n]$ y dado $b = \sum_{i=1}^{n}\alpha_i a_i \in S$ denotaremos por $\mathfrak{L}_b$ a $\mathfrak{L}_b \coloneqq \mathfrak{I} + \langle x^{\alpha}\rangle$ donde $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$.

Teorema 3.7 (Estructura de una base de Gröbner de $\mathfrak{L}_b$). *Sean $\ge$ un orden monomial en $\mathbb{K}[x_1,\dots,x_n]$, $\mathfrak{L}_b = \mathfrak{J} + \langle x^{\alpha}\rangle$, $b = deg_S(x^{\alpha})$ y sea $G_{\mathfrak{J}}$ una base de Gröbner de $\mathfrak{J}$ respecto de $\ge$ formada por binomios. Entonces, existen $m_1,\dots,m_r$ monomios tales que $G_{\mathfrak{J}} \cup \{m_1,\dots,m_r\}$ es una base de Gröbner de $\mathfrak{L}_b$. Además, $deg_S(m_i) \in b + S$.*

Demostración. Observamos que $G_{\mathfrak{J}} \cup \{x^{\alpha}\}$ es un sistema generador de $\mathfrak{L}_b$ y aplicando el algoritmo de Buchberger (Teorema 2.35), se tiene que $G_{\mathfrak{J}} \cup \{m_1,\dots,m_r\}$ donde $m_1,\dots,m_r$ son monomios es una base de Gröbner de $\mathfrak{L}_b$.
Si $x^{\beta} - x^{\gamma} \in \mathfrak{J}$ con $\beta,\gamma \in \mathbb{N}^n$, por el Lema 3.1 se tiene que $deg_S(x^{\beta}) = deg_S(x^{\gamma})$. Podemos calcular entonces el S-polinomio de $x^{\beta} - x^{\gamma}$ y un monomio x^{δ}, que resulta $S(x^{\beta} - x^{\gamma}, x^{\delta}) = \frac{-mcm(x^{\beta},x^{\delta})}{x^{\beta}}x^{\gamma}$. Aplicando el S-grado, obtenemos que:

$$\begin{aligned} &deg_S\left(\frac{mcm(x^{\beta},x^{\delta})}{x^{\beta}}x^{\gamma}\right) = deg_S\left(\frac{mcm(x^{\beta},x^{\delta})}{x^{\beta}}\right) + deg_S(x^{\gamma}) \\ &= deg_S\left(\frac{mcm(x^{\beta},x^{\delta})}{x^{\beta}}\right) + deg_S(x^{\beta}) = deg_S\left(\frac{mcm(x^{\beta},x^{\delta})}{x^{\beta}}x^{\beta}\right) \end{aligned}$$

$$= deg_S\left(mcm(x^\beta, x^\delta)\right) = deg_S\left(x^\delta \cdot x^{\overline{\delta}}\right) = deg_S(x^\delta) + deg_S(x^{\overline{\delta}}) \in b + S$$

Entonces, los S-grados de S-polinomios entre binomios y monomios pertenecen a $b + S$. Consideremos ahora un monomio $M = x^\delta$ tal que $deg_S(M) \in b + S$. Es claro que $\overline{M}^{G_{\mathfrak{L}_b}}$ es cero o un monomio en virtud del Lema 2.42. Si el resto fuera cero ya estaría. Distinguimos casos:

- Si se puede dividir M entre un binomio $B = x^\beta - x^\gamma$, al efectuar la división obtenemos que el resto es $x^\delta - x^{\delta-\beta}(x^\beta - x^\gamma) = x^{\delta-\beta+\gamma}$, luego $deg_S(x^{\delta-\beta}x^\gamma) = deg_S(x^{\delta-\beta}x^\beta) = deg_S(x^\delta) = deg_S(M) \in b + S$.
- Si el resto de la división es cero, la división se ha realizado entre algún monomio de $\{m_1, \ldots, m_r\}$.
- Si el resto de la división es un monomio, entonces la división se ha realizado entre un conjunto de binomios.

En cualquier caso, queda demostrado que $G_{\mathfrak{L}_b}$ está conformada por binomios y monomios de S-grado perteneciente a $b + S$. □

Este resultado nos permite decidir la pertenencia de un monomio al ideal $\mathfrak{L}_b$ fácilmente.

Lema 3.8 (Pertenencia de un monomio a $\mathfrak{L}_b$).

$$x^\gamma \in \mathfrak{L}_b \iff deg_S(x^\gamma) \in b + S$$

Demostración. " $\Leftarrow$ ") Sea $x^\gamma \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $deg_S(x^\gamma) \in b + S$. Entonces, $\sum_{i=1}^n \gamma_i a_i = b + \sum_{i=1}^n \mu_i a_i$ con $\gamma_i, \mu_i \in \mathbb{N} - \{0\}, 1 \leq i \leq n$. Dado que b es un elemento del semigrupo S, se tiene que $b = \sum_{i=1}^n \alpha_i a_i$ con $\alpha_i \in \mathbb{N}, 1 \leq i \leq n$. Así,

$$\sum_{i=1}^n \gamma_i a_i = \sum_{i=1}^n \alpha_i a_i + \sum_{i=1}^n \mu_i a_i = \sum_{i=1}^n (\alpha_i + \mu_i) a_i$$

Y en virtud del Lema 3.1, $x^\gamma - x^\alpha x^\mu \in \mathfrak{I} + \langle x^\alpha \rangle = \mathfrak{L}$, luego $x^\gamma \in \mathfrak{L}_b$.

" $\Rightarrow$ ") Sea $x^\gamma \in \mathfrak{L}_b$. Entonces, $\overline{x^\gamma}^{G_{\mathfrak{L}_b}} = 0$. Supongamos que existe un binomio $B = x^\beta - x^\delta \in G_{\mathfrak{L}_b}$ tal que $x^\beta \mid x^\gamma$. Entonces, realizando la división se obtiene que el resto es $x^\gamma - x^{\gamma-\beta}(x^\beta - x^\delta) = x^{\gamma-\beta+\delta}$ y en consecuencia $deg_S(x^\gamma) = deg_S(x^{\gamma-\beta+\delta})$. Siguiendo el algoritmo de división, eventualmente se dividirá por un monomio en cuyo caso el resto obtenido será $x^\gamma - x^{\gamma-\beta}x^\beta = 0$ y por tanto $deg_S(x^\gamma) = deg_S(x^\beta) + deg_S(x^{\gamma-\beta}) \in b + S$. □

Teorema 3.9. *Sean $\geq$ un orden monomial y $\mathfrak{B} = \{x^\gamma : x^\gamma \notin \langle LT(\mathfrak{L}_b)\rangle\}$. La correspondencia $\phi : \mathfrak{B} \longmapsto Ap(S, b)$ dada por $\phi(x^\gamma) = deg_S(x^\gamma)$ es una aplicación biyectiva.*

Demostración. Observamos por la Proposición 2.40 que las clases de los elementos de $\mathfrak{B}$ forman una base de $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{L}_b$. En primer lugar vamos a demostrar que ϕ está bien definida. En efecto, sea $x^\gamma \in \mathfrak{B}$. Aplicando la S-graduación, obtenemos que $deg_S(x^\gamma) = \sum_{i=1}^n \gamma_i a_i \in S$. Queda ver que $deg_S(x^\gamma) \in Ap(S,b)$. Supongamos por reducción al absurdo que $deg_S(x^\gamma) - b \in S$, luego $deg_S(x^\gamma) \in b + S$ lo que implica que $x^\gamma \in \mathfrak{L}$ y consecuentemente $LT(x^\gamma) = x^\gamma \in LT(\mathfrak{L})$ lo cual es absurdo. Por tanto, $deg_S(x^\gamma) - b \notin S$ y finalmente podemos afirmar que $deg_S(x^\gamma) \in Ap(S,b)$. Es evidente además que si tomamos $x^{\gamma_1}, x^{\gamma_2} \in \mathfrak{B}$ tales que $x^{\gamma_1} = x^{\gamma_2}$, entonces $\gamma_1 = \gamma_2$ y en consecuencia $deg_S(x^{\gamma_1}) = deg_S(x^{\gamma_2})$.

Veamos la inyectividad. Sean $x^{\gamma_1}, x^{\gamma_2} \in \mathfrak{B}$ tales que $\phi(x^{\gamma_1}) = \phi(x^{\gamma_2})$. Entonces, $deg_S(x^{\gamma_1}) = deg_S(x^{\gamma_2})$ lo que implica que $x^{\gamma_1} - x^{\gamma_2} \in \mathfrak{I} \subseteq \mathfrak{L}$. Supongamos por reducción al absurdo que $x^{\gamma_1} \neq x^{\gamma_2}$. En ese caso, si $x^{\gamma_1} \leq x^{\gamma_2}$ se tendría que $LM(x^{\gamma_1} - x^{\gamma_2}) = x^{\gamma_1} \in \langle LM(\mathfrak{L})\rangle \subseteq \langle LT(\mathfrak{L})\rangle$ lo cual es absurdo dado que $x^{\gamma_1} \in \mathfrak{B}$. Análogamente, si $x^{\gamma_2} \leq x^{\gamma_1}$ se tendría que $LM(x^{\gamma_1} - x^{\gamma_2}) = x^{\gamma_2} \in \langle LM(\mathfrak{L})\rangle \subseteq \langle LT(\mathfrak{L})\rangle$ resultando nuevamente en un absurdo. Por tanto, $x^{\gamma_1} = x^{\gamma_2}$.

Por último, veamos que ϕ es sobreyectiva. Sea $c \in Ap(S,b)$, entonces $c \in S$ luego existen $\beta_1,\ldots,\beta_n \in \mathbb{N}$ tales que $c = \sum_{i=1}^n \beta_i a_i$. Consideramos el resto $\overline{x^\beta}^{G_\mathfrak{L}}$. En principio, dicho resto puede ser cero o un monomio.

Supongamos que $\overline{x^\beta}^{G_\mathfrak{L}} = 0$ entonces $x^\beta \in \mathfrak{L}$ y su S-grado es $deg_S(x^\beta) = \sum_{i=1}^n \beta_i a_i \in b + S$. Podemos afirmar pues que $\sum_{i=1}^n \beta_i a_i - b = c - b \in S$. Esto es absurdo puesto que supusimos que $c \in Ap(S,b)$, luego el resto de la división de x^β por $G_\mathfrak{L}$ no puede ser cero. Por tanto, solo puede ocurrir que dicho resto sea un monomio x^γ, lo que quiere decir que la división se ha realizado únicamente entre elementos de $G_\mathfrak{I}$. Así, $x^\beta - x^\gamma \in \mathfrak{I}$ y $deg_S(x^\gamma) = deg_S(x^\beta) = c = \phi(x^\gamma)$. □

Como consecuencia de este resultado, se deduce el siguiente corolario.

Corolario 3.10. *El espacio vectorial $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{L}_b$ tiene dimensión finita. En particular,*

$$dim_\mathbb{K}\left(\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{L}_b\right) = b$$

Demostración. Por el Teorema 3.9, existe una biyección ϕ entre $Ap(S,b)$ y una base de $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{L}_b$ como espacio vectorial. Por tanto, el conjunto de Apéry y las bases tienen el mismo cardinal. Además, en virtud del Lema 1.19 se tiene que $Ap(S,b)$ tiene b elementos, luego $dim_\mathbb{K}\left(\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{L}_b\right) = \#\mathfrak{B} = \#Ap(S,b) = b$. □

Ejemplo 3.11. Sean $S = \langle 7,8,10\rangle$ un semigrupo numérico y el anillo $\mathbb{Q}[x,y,z,t]$ con el orden lexicográfico $>_{lex}$. Sabemos que $18 \in S$ puesto que $18 = 10 + 8$. Vamos a hallar $Ap(S,18)$. Consideremos el ideal $\mathfrak{J}_S = \langle x - t^7, y - t^8, z - t^{10}\rangle$.

Una base de Gröbner de $\mathfrak{J}_S$ es $G = \{y^5 - z^4, x^2z - y^3, x^2y - z^3, x^4 - yz^2, tz^2 - x^3, ty^2 - xz, tx - y, t^2x - z, t^4z - x^2, t^7 - x\}$ y $\overline{t^{18}}^G = yz$.

Consideremos $\mathfrak{L}_{18} = (\mathfrak{J}_S \cap \mathbb{Q}[x, y, z]) + \langle xy \rangle$. Una base de Gröbner de $\mathfrak{L}_{18}$ es $\bar{G} = \{z^4, yz, y^2, x^2z - y^3, x^2y^2 - z^3, y^4 - yz^2\}$ Además, una $\mathbb{Q}$-base de $\mathbb{Q}[x, y, z]/\mathfrak{L}_{18}$ como espacio vectorial es

$$\mathfrak{B} = \{1, x, y, z, x^2, xy, y^2, xz, z^2, x^3, x^2y, xy^2, y^3, xz^2, x^3y, z^3, xy^3, xz^3\}$$

Aplicando la biyección ϕ especificada en el Teorema 3.9, tenemos que:

$$\phi(\mathfrak{B}) = Ap(S, 18) = \{0, 7, 8, 10, 14, 15, 16, 17, 20, 21, 22, 23, 24, 27, 29, 30, 31, 37\}$$

Presentamos a continuación un algoritmo para realizar el cálculo del conjunto de Apéry respecto de un elemento del semigrupo numérico.

Algoritmo 4: Algoritmo para el cálculo de $Ap(S, b)$.

Entrada: $a_1, \ldots, a_n$ sistema generador de S, $b \in S$.
Salida: $Ap(S, b)$ conjunto de Apéry de S respecto a b.
1. Computar G una base de Gröbner de $\mathfrak{J}_S$ respecto de $>_{lex}$ con $t > x_1 > \ldots > x_n$.
2. Computar $q = \overline{t^b}^G$.
3. Hallar $G_{\mathfrak{J}} = G \cap \mathbb{K}[x_1, \ldots, x_n]$.
4. Hallar $G_{\mathfrak{L}_b}$ una base de Gröbner de $\mathfrak{L}_b = \langle G_{\mathfrak{J}}, q \rangle$.
5. Tomar $\mathfrak{B} = \{x^\alpha : x^\alpha \notin \langle LT(G_{\mathfrak{L}_b}) \rangle\}$.
6. Sea $\phi = deg_S$. Aplicar ϕ a todos los elementos de $\mathfrak{B}$. $Ap(S, b) = \phi(\mathfrak{B})$.
devolver $Ap(S, b)$

Nota:. Como $b \in S$, en el paso 2 del algoritmo se tiene que $\overline{t^b}^G = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in \mathbb{K}[x_1, \ldots, x_n]$ donde $b = \sum_{i=1}^n \alpha_i a_i$ (ver Proposición 3.2). En el paso 3, se obtiene una base de Gröbner de $\mathfrak{J} = \mathfrak{J}_S \cap \mathbb{K}[x_1, \ldots, x_n]$ (ver Teorema 2.38). En los pasos 4 y 5 se hallan una base de Gröbner de $\mathfrak{L}_b$ y una $\mathbb{K}$-base de $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{L}_b$ respectivamente (ver Proposición 2.40). Por último, y siguiendo el Teorema 3.9, en el paso 6 se calcula $Ap(S, b)$.

A

Apéndice

A.1. Implementación en SINGULAR

Dado el eminente carácter computacional de gran parte del trabajo, se han implementado dos rutinas en lenguaje `SINGULAR`. La primera de ellas, llamada `PerteneceSemig` determina si un número natural pertenece a un semigrupo numérico S y la segunda, llamada `Apery` determina el conjunto de Apéry de un semigrupo numérico S respecto a un elemento de él.

A.1.1. Pertenencia a un semigrupo numérico: `PerteneceSemig`

```
Entrada: intvec s un vector de enteros, int b un número natural.
Salida: 1 si b pertenece al semigrupo, 0 en caso contrario.
```

```
LIB "general.lib";
LIB "bfun.lib";
proc PerteneceSemig (intvec s, int b) {
   int n = nrows(s);
   ring r = 0, (t,x(1..n)), lp;
   ideal Js;

   for (int i = 1; i <= n; i++) {
       Js[i] = x(i) - t^(s[i]);
    }

  //Calculamos una base de Gröbner de Js.
      ideal I = std(Js);
      poly p = t^b;
```

```
    //Calculamos el resto de la división de p entre la base G.
         poly resto = reduce(p,I);
         if(leadexp(resto)[1] == 0)
         {
           print("El numero testeado pertenece al semigrupo.");
           return(1);
         }
         else
         {
           return(0);
         }
    } //Cierre PerteneceSemig
```

A continuación mostramos dos ejemplos de ejecución:

```
>intvec s = 7,8,10;
>PerteneceSemig(s,18);
El número testeado pertenece al semigrupo.
1

>PerteneceSemig(s,19);
El número testeado NO pertenece al semigrupo.
0
```

A.1.2. Cálculo del conjunto de Apéry: `Apery`

```
Entrada: intvec s un vector de enteros, int b un número natural.
Salida: 0 si b no pertenece al semigrupo.
En caso contrario, un vector de enteros intvec Ap con los elementos
del conjunto de Apéry de S respecto de b.
```

```
   proc Apery(intvec s, int b){
       //PerteneceSemig(s,b);
       if(PerteneceSemig(s,b) == 0)
       {
        print("El numero considerado no pertenece al semigrupo.");
       }
       else{
        int n = nrows(s);
        ring r = 0, (t,x(1..n)), lp;
        ideal Js;

        for (int i = 1; i <= n; i++) {
```

```
      Js[i] = x(i) - t^(s[i]);
     }

  poly q = reduce(t^b,std(Js));

  //Eliminamos la variable t del ideal Js.
  ideal L = eliminate(Js,t);
  ring r2 = 0, y(1..n), lp;
  //Morfismo entre r y r2
  map f = r, 0, y(1..n);

  //Imagen por f del ideal K y del polinomio q.
  ideal K = f(L);
  poly fq = f(q);
  ideal J = K, fq;

  print("K-Base del anillo cociente como espacio vectorial:");
  kbase(std(J));

 intvec ap;

 //Cálculo del S-grado de los monomios de la k-base.
    for (int j = 1; j <= b; j++){
      ap[j] = scalarProd(leadexp(kbase(std(J))[j]),s);
     }
   }
print("El conjunto de Apery respecto de b es");
ap;
} //Cierre Apery
```

Ejemplo de ejecución para calcular $Ap(S, 18)$ en $S = \langle 7, 8, 10 \rangle$:

```
intvec s = 7,8,10;
Apery(S,18);
El numero testeado pertenece al semigrupo.
K-Base del anillo cociente como espacio vectorial:
[1]=y(1)*y(3)∧3
[2]=y(3)∧3
[3]=y(1)*y(3)∧2
[4]=y(3)∧2
[5]=y(1)*y(3)
[6]=y(3)
[7]=y(1)*y(2)∧3
[8]=y(2)∧3
```

```
[9]=y(1)*y(2)∧2
[10]=y(2)∧2
[11]=y(1)∧3*y(2)
[12]=y(1)∧2*y(2)
[13]=y(1)*y(2)
[14]=y(2)
[15]=y(1)∧3
[16]=y(1)∧2
[17]=y(1)
[18]=1

El conjunto de Apery respecto de b es
37,30,27,20,17,10,31,24,23,16,29,22,15,8,21,14,7,0
```

Bibliografía

[1] Buchberger, B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universitat Insbruck (1965)

[2] Cox, D., Little, J. & O'Shea, D. *Ideals, Varieties and Algorithms.* Undergraduate Texts in Mathematics, Springer. (2015)

[3] Cruz, A. *Códigos y Semigrupos.* Trabajo de Fin de Máster, Universidad de Granada (2018)

[4] Decker W., Greuel, G.-M. & Pfister G. & Schönemann H. Singular *4-1-2 — A computer algebra system for polynomial computations.* http://www.singular.uni-kl.de (2019).

[5] Márquez–Campos, G., Ojeda, I. & Tornero, J.M. *On the computation of the Apèry set of numerical monoids and affine semigroups.* Semigroup Forum Volumen 91 (2015), nº1 pp. 139 - 158.

[6] Rosales, J.C. & García-Sánchez, P.A. *Numerical Semigroups.* Developments in Mathematics, Vol. 20 (2009).

[7] Sylvester, J. J.*Mathematical questions with their solutions.* Educational Times 41 (1884)

Numerical semigroups and associated ideals

Sección de Matemáticas
Universidad de La Laguna

Enrique José Padrón Alemán
Facultad de Ciencias · Sección de Matemáticas
Universidad de La Laguna
alu0100885781@ull.edu.es

Abstract

This manuscript aims to introduce the reader to both Numerical Semigroups and Gröbner Bases theories, showing some interactions between them. In the first chapter, we study the structure of numerical semigroups. We prove that every numerical semigroup is finitely generated and has a unique minimal set of generators. We also study several relevant sets associated to the semigroup as the Apéry set and the set of gaps. In the second chapter, we study classical Gröbner Bases theory. We first define a monomial order in the polynomial ring over a field. Then, we describe a division algorithm which allows us to generalise the Euclidean division and we use this tool to find generating systems for ideals with reasonably good properties. Finally, we approach two problems of Numerical Semigroups theory: the semigroup membership problem and the computation of the Apéry set, both of them applying tools given by Gröbner bases.

1. Numerical semigroups

Definition 1 *Let $(S,+)$ be a submonoid of $\mathbb{N}$. S is said to be a numerical semigroup if $\mathbb{N}-S$ is finite.*

We want to tackle the following problems:

- Computation of generating sets for S.
- Semigroup membership problem: Given $S=\langle a_1,\dots,a_n\rangle$ a numerical semigroup and $b\in\mathbb{N}$, we want to determine whether $b\in S$. That is, if there are $\alpha_1,\dots,\alpha_n\in\mathbb{N}$ such that $b=\sum_{i=1}^{n}\alpha_i a_i$.
- Computation of the Fröbenius number $F(S)=max(\mathbb{Z}-S)$.

Definition 2 *Let S be a numerical semigroup and $b\in S$. The Apéry set of b in S is $Ap(S,b)=\{s\in S : s-b\notin S\}$.*

We can use the Apéry set to solve all the problems mentioned above.

Theorem 1 *Let S be a numerical semigroup, $b\in S$.*

1. *$\big(Ap(S,b)-\{0\}\big)\cup\{b\}$ is a generating system for S.*
2. *$c\in S \iff c=w+\lambda b$ where $w\in Ap(S,b)$, $w\equiv c \pmod b$, $\lambda\in\mathbb{N}$.*
3. *$F(S)=max(Ap(S,b))-b$.*

2. Gröbner bases

A monomial in $\mathbb{K}[x_1,\dots,x_n]$ is an expression of the form

$$x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

where $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n$.

Definition 3 *A monomial order is a total order relation " $\geq$ " over the set of monomials M of $\mathbb{K}[x_1,\dots,x_n]$ veryfing:*

1. *If $x^\alpha, x^\beta, x^\gamma\in M$ and $x^\alpha\geq x^\beta$ then $x^\alpha x^\gamma \geq x^\beta x^\gamma$*
2. *$x^\alpha\geq 1, \forall x^\alpha\in M$.*

Definition 4 *Given $f=\sum a_\alpha x^\alpha$. We denote by $LM(f)$ its leading monomial, i.e., $LM(f)=max_{\geq}\{x^\alpha : a_\alpha\neq 0\}$.*

Definition 5 *A finite subset $G=\{g_1,\dots,g_t\}$ of a nonzero ideal $\mathfrak{I}\subseteq\mathbb{K}[x_1,\dots,x_n]$ is said to be a Gröbner basis if*

$$\langle LM(\mathfrak{I})\rangle = \langle LM(g_1),\dots,LM(g_t)\rangle$$

where $\langle LM(\mathfrak{I})\rangle = \langle LM(f) : f\in\mathfrak{I}-\{0\}\rangle$.

A Gröbner basis for an ideal is a generating system of the same ideal and it can be obtained by means of an algorithm (Buchberger's algorithm).

3. Main results

Given $S=\langle a_1,\dots,a_n\rangle$ a numerical semigroup and $b\in\mathbb{N}$. We define the following ideal in $\mathbb{K}[x_1,\dots,x_n,t]$:

$$\mathfrak{I}_S=\langle x_1-t^{a_1},\dots,x_n-t^{a_n}\rangle$$

Proposition 1 (Membership problem) *Let G be a Gröbner basis for $\mathfrak{I}_S$ with respect to $>_{lex}$ considering $t>x_1>\cdots>x_n$. Then,*

$$b\in S \iff \overline{t^b}^{G}\in\mathbb{K}[x_1,\dots,x_n]$$

where $\overline{t^b}^{G}$ is the remainder of the division of t^b by G.

We define a new grading in $\mathbb{K}[x_1,\dots,x_n,t]$ as $deg_S(x_i)=a_i, 1\leq i\leq n$, $deg_S(t)=1$. Also, for $b=\sum_{i=1}^{n}\alpha_i a_i\in S$, we define the ideal $\mathfrak{L}_b=(\mathfrak{I}_S\cap\mathbb{K}[x_1,\dots,x_n])+\langle x^\alpha\rangle$ where $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n$.

Theorem 2 (Computation of Ap(S,b)) *Let S be a numerical semigroup, $\geq$ a monomial order and $\mathfrak{B}=\{x^\gamma : x^\gamma\notin\langle LT(\mathfrak{L}_b)\rangle\}$. Then,*

$$\phi:\mathfrak{B}\longmapsto Ap(S,b)$$
$$x^\gamma\longmapsto deg_S(x^\gamma)$$

is a bijection.

4. Algorithms

Algorithm 1 Numerical semigroup membership

procedure
Input: $a_1,\dots,a_n$ generating system of S, $b\in\mathbb{N}$.
Output: 1 if $b\in\langle a_1,\dots,a_n\rangle$, or 0 otherwise.
  Define $\mathfrak{I}_S=\langle x_1-t^{a_1},\dots,x_n-t^{a_n}\rangle$.
  Compute G a Gröbner Basis for $\mathfrak{I}_S$ using
  $>_{lex}$ with $t>x_1>\dots>x_n$
  if $\overline{t^b}^{G}\in\mathbb{K}[x_1,\dots,x_n]$ **then**
    return $\overline{t^b}^{G}=x_1^{a_1}\cdots x_n^{a_n}$
  else
    return 0
  end if
end procedure

Algorithm 2 Computation of the Apéry set

procedure
Input: $a_1,\dots,a_n$ generating system for S, $b\in\S$.
Output: Apéry set of S with respect to b.
  if $b\notin S$ **then**
    return 0
  else
    Compute G a Gröbner Basis for $\mathfrak{I}_S$
    using $>_{lex}$ with $t>x_1>\cdots>x_n$
    Compute the remainder $q=\overline{t^b}^{G}$.
    $G_{\mathfrak{I}}=G\cap\mathbb{K}[x_1,\dots,x_n]$.
    $G_{\mathfrak{L}_b}$ a Gröbner basis for $\mathfrak{L}_b=\langle G_{\mathfrak{I}},q\rangle$.
    Consider $\mathfrak{B}=\{x^\alpha : x^\alpha\notin\langle LT(G_{\mathfrak{L}_b})\rangle\}$.
    Consider $\phi=deg_S$. $Ap(S,b)=\phi(\mathfrak{B})$.
  end if
  Return: $Ap(S,b)$.
end procedure

References

[1] Rosales, J.C. & García-Sánchez, P.A. *Numerical Semigroups*. Developments in Mathematics, Vol. 20 (2009).

[2] Cruz, A. (2018) *Códigos y Semigrupos*. Trabajo de Fin de Máster (Universidad de Granada)

[3] Cox, D. & Little, J. & O'Shea, D. *Ideals, Varieties and Algorithms*. Undergraduate Texts in Mathematics, Springer.

[4] Márquez–Campos G. & Ojeda I. & Tornero, J.M. *On the computation of the Apèry set of numerical monoids and affine semigroups*. Semigroup Forum Volumen 91 (2015), no. 1 pp. 139 - 158.

[5] Decker W. & Greuel, G.-M & Pfister G. & Schönemann H. *Singular 4-1-2 — A computer algebra system for polynomial computations*. http://www.singular.uni-kl.de (2019).