Universidad de El Salvador

Facultad de Ciencias Naturales y Matemática

Escuela de Matemática

Tema:

INTRODUCCIÓN A BASES ESTÁNDAR Y ALGUNAS APLICACIONES

Trabajo de graduación para obtener el título de Licenciado en Matemática

---

Autor:
Br. Vitelio Alexander Sola Gutiérrez

Asesora: Lic. María Cecilia Martínez Reyes
Asesor externo: MSc. Mario Alexis Ruiz Mejía

UNIVERSIDAD DE EL SALVADOR

RECTOR:
MSc. Roger Armando Arias

VICE-RECTOR ADMINISTRATIVO:
Ing. Juan Rosa Quintanilla

VICE-RECTOR ACADEMICO:
PhD. Raúl Ernesto Azcúnaga López

SECRETARIO GENERAL:
Ing. Francisco Alarcón
FISCAL:
Lic. Rafael Humberto Peña Marín

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

DECANO:
Lic. Mauricio Hernán Lovo Córdova

VICE-DECANO:
MSc. Zoila Virginia Guerrero

SECRETARIO:
MSc. Guillermo Morán

ESCUELA DE MATEMÁTICA

DIRECTOR DE ESCUELA:
Dr. Dimas Noé Tejada Tejada

ASESORA:
Lic. María Cecilia Martínez Reyes
ASESOR EXTERNO:
MSc. Mario Alexis Ruiz Mejía

Índice

Agradecimientos

Expreso sincero agradecimiento a Dios por permitirme estar un paso más cerca de la meta de convertirme en un profesional de la educación, brindándome la fuerza y perseverancia para seguir adelante. A mi familia por su apoyo, esfuerzo y sacrificio.

A mis asesores Lic. Cecilia Martínez y MSc. Mario Alexis Ruiz por brindarme su apoyo, tiempo y conocimiento.

A mis amigos y compañeros quienes compartieron su conocimiento, alegres y tristes momentos, infinitas gracias.

Introducción

Las bases estándar son una herramienta computacional muy potente que permite trabajar con ideales en el anillo $K[x_1, \ldots, x_n]$ de polinomios multivariados sobre un campo K, y pueden usarse para resolver diversos problemas. La noción de base estándar fue introducida originalmente por Buchberger en 1965, con el nombre de bases de Gröbner, las cuales se definen para los ideales polinomiales, con órdenes monomiales globales. Además, Buchberger describió un algoritmo (algoritmo de Buchberger) para calcular las bases de Gröbner, brindando técnicas computacionales que permiten trabajar con ideales en un anillo de polinomios en varias variables.

El presente trabajo se encuentra estructurado por capítulos. En el Capítulo 1, se presenta una generalización del algoritmo de la división, el cual resuelve el problema de descripción de un ideal, es decir, que cada ideal $I \subset K[x_1, \ldots, x_n]$ puede escribirse como $\langle f_1, \ldots, f_s \rangle$ para algunos $f_i \in K[x_1, \ldots, x_n]$, lo que permitirá introducir el concepto de bases de Gröbner.

En el Capítulo 2, se estudia la localización de un anillo de polinomios y el anillo asociado a un orden monomial, con el objetivo de introducir las bases estándar para órdenes locales; brindando además un algoritmo que permite calcularlas, específicamente el algoritmo de base estándar, que hace uso del algoritmo de Buchberger y el algoritmo del Cono Tangente de Mora.

En el Capítulo 3, tomando como base lo expuesto en los capítulos anteriores, se da respuesta a algunos problemas clásicos de ideales utilizando las bases estándar, tales como determinar la pertenencia de un polinomio a un ideal, eliminación de variables, construcción de bases para la intersección de ideales, determinar la pertenencia de un polinomio al ideal radical, y se introduce el problema de sistemas de ecuaciones polinomiales.

Objetivos

Objetivo general

Exponer detalladamente un estudio introductorio a las bases estándar de ideales, demostrando las principales propiedades y algoritmos que permiten estudiar la teoría de ideales desde una perspectiva computacional.

Objetivos específicos

- Generalizar el algoritmo de la división de polinomios, en el anillo de polinomios en n indeterminadas, permitiendo introducir las bases de Gröbner y sus propiedades.
- Hacer un estudio de conceptos fundamentales de los anillos de polinomios asociados a un orden monomial cualquiera y la construcción de formas normales para el cálculo de bases estándar.
- Desarrollar ejemplos que exhiban la aplicación de las bases estándar.

CAPÍTULO 1: Preliminares

En este capítulo se presenta una generalización del algoritmo de la división de polinomios a un anillo multivariado, el cual será la base para un estudio de las bases de Gröbner, que permitirá resolver diversos problemas, como la pertenencia de un polinomio al ideal o la descripción de un ideal (determinar un conjunto generador finito para un ideal).

1. Órdenes monomiales

Definición 1.1. Dado un anillo conmutativo A, se define:

I) Un *monomio* en n variables, como un producto de potencias de la forma:

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad \text{con} \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$$

El conjunto de monomios en n variables es denotado por:

$$\mathtt{Mon}(x_1, \ldots, x_n) = \mathtt{Mon}_n := \{x^\alpha : \ \alpha \in \mathbb{Z}_{\geq 0}^n\}$$

Notar que $\mathtt{Mon}$ es un semigrupo bajo la multiplicación, con elemento neutro $1 = x_1^0 \cdots x_n^0$. Un monomio x^α divide al monomio x^β, si $\alpha_i \leq \beta_i$ para todo i, además $x^\beta = x^\gamma x^\alpha$ para algún $\gamma = \beta - \alpha \in \mathbb{Z}_{\geq 0}^n$.

II) Un *término* es un monomio multiplicado por un coeficiente (un elemento de A),

$$ax^\alpha = ax_1^{\alpha_1} \cdots x_n^{\alpha_n}, \qquad a \in A$$

III) Un *polinomio* sobre el anillo A, es una combinación lineal finita de monomios, es decir, una suma finita de términos de la forma:

$$f = \sum_\alpha a_\alpha x^\alpha = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n}^{\text{finito}} a_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}; \qquad \text{con } a_\alpha \in A$$

Para $\alpha \in \mathbb{Z}_{\geq 0}^n$, sea $|\alpha| := \alpha_1 + \cdots + \alpha_n$, el *grado total del monomio* x^α. El entero $\mathtt{deg}(f) := \max\{|\alpha| \mid a_\alpha \neq 0\}$ es llamado *grado total del polinomio* f (si f es el polinomio cero entonces $\mathtt{deg}(f) = -1$).

IV) El *anillo de polinomios* $A[x] := A[x_1, \ldots, x_n]$ en n variables sobre A, es el conjunto de todos los polinomios con coeficientes en A en n indeterminadas $x_1, \ldots, x_n$. Con la suma y multiplicación usual:

$$\sum_{\alpha} a_\alpha x^\alpha + \sum_{\alpha} b_\alpha x^\alpha := \sum_{\alpha} (a_\alpha + b_\alpha) x^\alpha$$

$$\left(\sum_{\alpha} a_\alpha x^\alpha \right) \cdot \left(\sum_{\beta} b_\beta x^\beta \right) := \sum_{\gamma} \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta \right) x^\gamma$$

El anillo de polinomios $A[x_1, \ldots, x_n]$, es un anillo conmutativo con unidad $1 = x_1^0 x_2^0 \cdots x_n^0$, que identificamos con el elemento identidad $1 \in A$. Los elementos de $A \subset A[x_1, \ldots, x_n]$ son llamados polinomios constantes, se caracterizan por tener un grado menor o igual a cero, A es llamado el anillo base de $A[x]$. Para nuestro estudio nos enfocaremos en el anillo de polinomios $K[x] = K[x_1, \ldots, x_n]$ con coeficientes en el campo K. Y denotaremos por $K[x]^* = K^* = K - \{0\}$ al conjunto de unidades del anillo.

Observar que el monomio $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ (la notación x^α donde α es un vector, se le conoce como multinomio), se puede construir a partir de la n-upla de exponentes $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Esta observación establece una correspondencia uno a uno entre los monomios de $\mathtt{Mon}_n$ y $\mathbb{Z}^n_{\geq 0}$. Además, cualquier orden $>$ que se establezca en el conjunto $\mathbb{Z}^n_{\geq 0}$, se obtendrá un orden sobre el conjunto de monomios $\mathtt{Mon}_n$; si $\alpha > \beta$ según este orden, también diremos que $x^\alpha > x^\beta$.

Para comenzar, dado un polinomio, nos gustaría ser capaces de ordenar los términos sin ambigüedad, en orden descendente (o ascendente). Para hacer esto, debemos ser capaces de comparar cada par de monomios para establecer sus posiciones relativas correctas. Por lo tanto, exigiremos que nuestros ordenamientos sean *lineales* o *totales*; esto significa, que para cada par de monomios x^α y x^β, exactamente una de las tres afirmaciones siguientes debería ser cierta

$$x^\alpha > x^\beta, \qquad x^\alpha = x^\beta \qquad \text{o} \qquad x^\beta > x^\alpha.$$

Es importante tener en cuenta el efecto de la suma y producto en los polinomios, ya que cuando se suman polinomios, después de combinar términos semejantes, se puede simplemente reorganizar los términos presentes en el orden apropiado, por lo que las sumas no presentan dificultades.

Sin embargo, los productos son más sutiles, dado que la multiplicación en un anillo de polinomios se distribuye sobre la suma, basta con considerar lo que sucede cuando se multiplica un monomio por un polinomio. Si esto cambia el orden relativo de los términos, problemas significativos podrían resultar en cualquier proceso similar al del algoritmo de división en $K[x]$, en el cual se deben identificar los términos "principales" de los polinomios. Por lo tanto, exigiremos que todos los ordenamientos monomiales

tengan la siguiente propiedad adicional. Si $x^\alpha > x^\beta$ y x^γ es cualquier monomio, entonces requerimos que $x^\alpha x^\gamma > x^\beta x^\gamma$. En términos de los vectores exponentes, esta propiedad significa que si $\alpha > \beta$ en nuestro ordenamiento en $\mathbb{Z}^n_{\geq 0}$, entonces, para todo $\gamma \in \mathbb{Z}^n_{\geq 0}$,

$$\alpha + \gamma > \beta + \gamma$$

Considerando lo expuesto antes, se puede definir un orden monomial de la siguiente manera.

Definición 1.2. Un *orden monomial* o *orden de semigrupo* en $K[x_1, \ldots, x_n]$, es un ordenamiento total (o lineal) $>$ en el conjunto de monomios $\texttt{Mon}_n = \{x^\alpha : \ \alpha \in \mathbb{Z}^n_{\geq 0}\}$ en n variables que satisface:

$$x^\alpha > x^\beta \Longrightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

para todo $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$. Decir que $>$ es un orden monomial en el anillo de polinomios $K[x_1, \ldots, x_n]$, significa que $>$ es un ordenamiento monomial en $\texttt{Mon}(x_1, \ldots, x_n)$.

Los ordenamientos monomiales proporcionan una estructura extra en el conjunto de monomios y por lo tanto también en el anillo de polinomios. Desde un punto de vista práctico, un ordenamiento monomial $>$ permite escribir un polinomio $f \in K[x_1, \ldots, x_n]$ de manera ordenada y única como:

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \cdots + a_\gamma x^\gamma$$

con $x^\alpha > x^\beta > \ldots > x^\gamma$, donde ningún coeficiente es cero.

Definición 1.3. Sea $>$ un orden monomial fijo y $f \in K[x_1, \ldots, x_n]$, el polinomio $f \neq 0$ se puede escribir de manera única, como una suma finita de términos distintos de cero, de la siguiente manera:

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \cdots + a_\gamma x^\gamma$$

con $x^\alpha > x^\beta > \ldots > x^\gamma$ y $a_\alpha, a_\beta, \ldots, a_\gamma \in K$.

Así para todo $f \in K[x_1, \ldots, x_n]$, se define:

i) El *exponente principal* de f

$$\texttt{LE}(f) := \texttt{leadexp}(f) := \text{máx}\{\alpha \in \mathbb{Z}^n_{\geq 0} : \ a_\alpha \neq 0\}$$

(el máximo se toma con respecto a $>$).

ii) El *coeficiente principal* de f

$$\texttt{LC}(f) := \texttt{leadcoef}(f) := a_\alpha \in K$$

III) El *monomio principal* de f

$$\texttt{LM}(f) := \texttt{leadmonom}(f) := x^\alpha$$

(con coeficiente 1).

IV) El *término principal* o *cabeza* de f

$$\texttt{LT}(f) := \texttt{lead}(f) := \texttt{LC}(f) \cdot \texttt{LM}(f) = a_\alpha x^\alpha$$

V) La *cola* de f

$$\texttt{tail}(f) := f - \texttt{lead}(f) := a_\beta x^\beta + \cdots + a_\gamma x^\gamma$$

La más importante distinción entre órdenes monomiales se da cuando toda variable es mayor que la unidad del anillo, y son llamados órdenes globales. Si la unidad del anillo es mayor que toda variable, son llamados órdenes locales.

Definición 1.4. Sea $>$ un orden monomial en $\{x^\alpha : \ \alpha \in \mathbb{Z}^n_{\geq 0}\}$.

I) $>$ es llamado *orden global* si $x^\alpha > 1$ para todo $\alpha \neq (0, \ldots, 0)$.

II) $>$ es llamado *orden local* si $x^\alpha < 1$ para todo $\alpha \neq (0, \ldots, 0)$.

III) $>$ es llamado *orden mixto* si no es global ni local.

Es claro que si cambiamos el orden monomial al comparar dos monomios $x^\alpha, x^\beta \in K[x_1, \ldots, x_n]$, si $x^\alpha >' x^\beta$ y $x^\beta > x^\alpha$, entonces $>'$ es global si y solo si $>$ es local. Los órdenes locales y globales tienen propiedades diferentes.

Definimos los siguientes órdenes monomiales, para órdenes globales y locales, tomando $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$.

(1) **Órdenes globales:**

I) *Orden lexicográfico* $>_{lp}$:

$$\begin{aligned} x^\alpha >_{lp} x^\beta \ :\Longleftrightarrow \ & \exists\, 1 \leq i \leq n : \\ & \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i \end{aligned}$$

II) *Orden lexicográfico graduado invertido* $>_{dp}$:

$$\begin{aligned} x^\alpha >_{dp} x^\beta \ :\Longleftrightarrow \ & \texttt{deg}(x^\alpha) > \texttt{deg}(x^\beta) \\ & \text{o } (\texttt{deg}(x^\alpha) = \texttt{deg}(x^\beta) \text{ y } \exists\, 1 \leq i \leq n : \\ & \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i) \end{aligned}$$

III) *Orden lexicográfico graduado* $>_{Dp}$:

$$\begin{aligned} x^\alpha >_{Dp} x^\beta \ :\Longleftrightarrow\ & \mathtt{deg}(x^\alpha) > \mathtt{deg}(x^\beta) \\ & \text{o } (\mathtt{deg}(x^\alpha) = \mathtt{deg}(x^\beta) \text{ y } \exists\, 1 \le i \le n : \\ & \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i) \end{aligned}$$

(2) **Órdenes locales:**

I) *Orden lexicográfico negativo* $>_{ls}$:

$$\begin{aligned} x^\alpha >_{ls} x^\beta \ :\Longleftrightarrow\ & \exists\, 1 \le i \le n : \\ & \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i \end{aligned}$$

II) *Orden lexicográfico graduado invertido negativo* $>_{ds}$:

$$\begin{aligned} x^\alpha >_{ds} x^\beta \ :\Longleftrightarrow\ & \mathtt{deg}(x^\alpha) < \mathtt{deg}(x^\beta) \\ & \text{o } (\mathtt{deg}(x^\alpha) = \mathtt{deg}(x^\beta) \text{ y } \exists\, 1 \le i \le n : \\ & \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i) \end{aligned}$$

III) *Orden lexicográfico graduado negativo* $>_{Ds}$:

$$\begin{aligned} x^\alpha >_{Ds} x^\beta \ :\Longleftrightarrow\ & \mathtt{deg}(x^\alpha) < \mathtt{deg}(x^\beta) \\ & \text{o } (\mathtt{deg}(x^\alpha) = \mathtt{deg}(x^\beta) \text{ y } \exists\, 1 \le i \le n : \\ & \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i) \end{aligned}$$

Es importante notar que se ha fijado una enumeración $x_1, \ldots, x_n$ de las variables, cualquier otra enumeración conduce a un orden monomial diferente. Por ejemplo, si las variables son x e y, entonces se obtiene un orden *lp* (ordenamiento lexicográfico), con $x > y$ y un segundo con $y > x$. En el caso general de n variables, hay $n!$ ordenamientos *lp*. En lo que sigue, para cualquier ordenamiento se referirá al que tiene $x_1 > \ldots > x_n$ a menos que se indique lo contrario.

Definición 1.5. Sea $>_1$ un orden monomial en $\mathtt{Mon}(x_1, \ldots, x_n)$ y $>_2$ un orden monomial en $\mathtt{Mon}(y_1, \ldots, y_m)$. Entonces el *producto ordenado* u *orden de bloque* $>$, también denotado por $(>_1, >_2)$ en $\mathtt{Mon}(x_1, \ldots, x_n, y_1, \ldots, y_m)$, se define como

$$\begin{aligned} x^\alpha y^\beta > x^{\alpha'} y^{\beta'} \ :\Longleftrightarrow\ & x^\alpha >_1 x^{\alpha'} \\ & \text{o } (x^\alpha = x^{\alpha'} \text{ y } y^\beta >_2 y^{\beta'}) \end{aligned}$$

Si $>_1$ es un ordenamiento global entonces el producto ordenado, tiene la propiedad que los monomios que contienen a x_i, son siempre más grandes que los monomios que no

contienen a x_i. Si $>_1$ y $>_2$ son globales (respectivamente locales), entonces el producto ordenado es global (respectivamente local), al combinar un orden monomial local y uno global, surge un ordenamiento monomial mixto.

En este capítulo se trabajará únicamente con órdenes globales, retomando la definición de órdenes locales en los capítulos restantes. El siguiente lema permite caracterizar un ordenamiento monomial global.

Lema 1.6. Sea $>$ un ordenamiento monomial fijo, las siguientes condiciones son equivalentes:

I) $>$ es un buen orden.

II) $x_i > 1$ para $i = 1, \ldots, n$.

III) $x^\alpha > 1$ para todo $\alpha \neq (0, \ldots, 0)$, es decir $>$ es global.

IV) $\alpha \geq_{\text{nat}} \beta$ y $\alpha \neq \beta$ implica $x^\alpha > x^\beta$.

La última condición significa que $>$ es un refinamiento del *ordenamiento parcial natural* en $\mathbb{Z}^n_{\geq 0}$ definido por

$$(\alpha_1, \ldots, \alpha_n) \geq_{\text{nat}} (\beta_1, \ldots, \beta_n) \Longleftrightarrow \alpha_i \geq \beta_i \text{ para todo } i$$

Demostración.

- I) $\Rightarrow$ II) Si $x_i < 1$ para algún i, entonces $x_i^p < x_i^{p-1} < 1$, por definición de ordenamiento monomial. Produciendo un conjunto de monomios sin elemento más pequeño (recordemos que un conjunto cumple la propiedad del buen orden, si cada subconjunto no vacío tiene un elemento más pequeño con respecto a $>$), lo que contradice I). Por lo tanto $x_i > 1$ para $i = 1, \ldots, n$.

- II) $\Rightarrow$ III) Sea $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{>0}$ y $\alpha \neq (0, \ldots, 0)$. Como $x_i > 1$ para $i = 1, \ldots, n$ entonces $x_i^{\alpha_i} > 1$ con $\alpha_i \in \mathbb{Z}_{>0}$ (por ser un ordenamiento monomial). Así $x_1^{\alpha_1} > 1$ y $x_2^{\alpha_2} > 1$ entonces $x_1^{\alpha_1} \cdot x_2^{\alpha_2} > x_2^{\alpha_2} > 1$. Continuando de manera inductiva se sigue que $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots x_n^{\alpha_n} > 1$, para todo $\alpha \neq (0, \ldots, 0)$. Por lo tanto $>$ es un ordenamiento global.

- III) $\Rightarrow$ IV) Sea $\alpha, \beta \in \mathbb{Z}^n_{>0}$ y $\alpha \neq \beta$. Además $\alpha = (\alpha_1, \ldots, \alpha_n) \geq_{\text{nat}} \beta = (\beta_1, \ldots, \beta_n)$. Entonces $\gamma = \alpha - \beta \in \mathbb{Z}^n_{>0}$ y $\gamma \neq (0, \ldots, 0)$ por definición de ordenamiento natural, así $x^\alpha > 1$ implica $x^\gamma \cdot x^\beta > x^\beta$ y por lo tanto $x^\alpha = x^\gamma \cdot x^\beta > x^\beta$.

- IV) $\Rightarrow$ I) Sea M un conjunto no vacío de monomios por Lema de Dickson 3.5 existe un subconjunto finito $B \subset M$, tal que para cada $x^\alpha \in M$ existe un $x^\beta \in B$ tal que $\beta \leq_{\text{nat}} \alpha$. Por hipótesis, $x^\beta < x^\alpha$ o $x^\alpha = x^\beta$, como B es finito podemos comparar monomio a monomio con respecto a $>$. Así existe $\beta^* \in B$ tal que $\beta^* \leq \beta_i$, $\forall \beta_i \in B$. Entonces B contiene un elemento más pequeño de M con respecto a $>$. Por lo tanto $>$ es un buen orden.

□

El siguiente lema nos ayudará a entender lo que significa la condición de ordenamiento global de la parte (I) del Lema 1.

Lema 1.7. Una relación de orden $>$ en $\mathbb{Z}^n_{\geq 0}$, es un buen orden si y solo si cada secuencia estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

finalmente termina.

Demostración. Lo probaremos en forma contrarrecíproca: $>$ no es un buen orden si y solo si hay una secuencia infinita estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$.

Si $>$ no es un buen orden, entonces existe un subconjunto no vacío $S \subset \mathbb{Z}^n_{\geq 0}$, tal que "no tiene un elemento mínimo". Sea $\alpha(1) \in S$, como $\alpha(1)$ no es el elemento mínimo, podemos encontrar $\alpha(1) > \alpha(2)$, con $\alpha(2) \in S$. Entonces $\alpha(2)$ tampoco es el elemento mínimo, por lo que $\alpha(2) > \alpha(3)$ y $\alpha(3) \in S$.
Continuando de esta manera, obtenemos una secuencia infinitamente decreciente

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

Por el contrario, dada una secuencia infinita estrictamente decreciente, entonces $\{\alpha(1), \alpha(2), \alpha(3), \dots\}$ es un subconjunto no vacío de $\mathbb{Z}^n_{\geq 0}$ que no tiene elemento mínimo, y por lo tanto, $>$ no es un buen orden. □

La importancia de este lema se hará evidente en las secciones siguientes. Se usará para mostrar que varios algoritmos deben terminar porque en cada paso del algoritmo, algún término disminuye estrictamente respecto a un orden monomial fijo.

Terminaremos esta sección con una discusión sobre cómo se puede aplicar un orden monomial a los polinomios. Recordar que un polinomio de $K[x_1, \dots, x_n]$ es una combinación lineal finita de monomios, es decir, una suma finita de términos,

$$f = \sum_{\alpha} a_\alpha x^\alpha; \qquad \text{con } a_\alpha \in K$$

Si $f \in K[x_1, \dots, x_n]$ y se ha seleccionado un orden monomial $>$, entonces podemos ordenar los términos de f sin ambigüedad, con respecto al orden monomial $>$, comparando los monomios del polinomio.

Ejemplo 1.8. Sea $f = x^3 + x^3yz + xy^2 + y^5 + z^4 \in K[x, y, z]$, entonces:

- Con respecto al orden *lp*, el polinomio se ordena de la siguiente manera:

$$f = x^3yz + x^3 + xy^2 + y^5 + z^4$$

- Con respecto al orden *Dp*, el polinomio se ordena de la siguiente manera:

$$f = x^3yz + y^5 + z^4 + x^3 + xy^2$$

- Con respecto al orden *dp*, el polinomio se ordena de la siguiente manera:

$$f = y^5 + x^3yz + z^4 + x^3 + xy^2$$

- Con respecto al orden *ls*, el polinomio se ordena de la siguiente manera:

$$f = z^4 + y^5 + xy^2 + x^3 + x^3yz$$

- Con respecto al orden *Ds*, el polinomio se ordena de la siguiente manera:

$$f = x^3 + xy^2 + z^4 + x^3yz + y^5$$

- Con respecto al orden *ds*, el polinomio se ordena de la siguiente manera:

$$f = x^3 + xy^2 + z^4 + x^3yz + y^5$$

- Dado el polinomio $f = x^3yz + x^3 + xy^2 + y^5 + z^4$; con orden monomial *lp* se cumple lo siguiente:
  - El exponente principal $\texttt{LE}(f) = (3, 1, 1)$
  - El monomio principal $\texttt{LM}(f) = x^3yz$
  - El coeficiente principal $\texttt{LC}(f) = 1$
  - El término principal $\texttt{LT}(f) = x^3yz$
  - La cola del polinomio $\texttt{tail}(f) = x^3 + xy^2 + y^5 + z^4$

Lema 1.9. Sea $f, g \in K[x_1, \ldots, x_n]$ polinomios distintos de cero. Entonces:

I) $\texttt{LE}(fg) = \texttt{LE}(f) + \texttt{LE}(g)$

II) Si $f + g \neq 0$, entonces $\texttt{LE}(f + g) \leq \text{máx}\{\texttt{LE}(f), \texttt{LE}(g)\}$. Además, si $\texttt{LE}(f) \neq \texttt{LE}(g)$, entonces ocurre la igualdad.

Demostración. Como $f, g \in K[x_1, \ldots, x_n]$ entonces $f = \sum_{i=0}^{n} a_i x^i$ y $g = \sum_{i=0}^{m} b_i x^i$ con $\alpha_0 \neq 0$ y $\beta_0 \neq 0$. Sea $\texttt{LE}(f) = \alpha_0$ y $\texttt{LE}(g) = \beta_0$, se cumple que $\alpha_0 > \alpha_i$ para $i = 1, \ldots, n$ y $\beta_0 > \beta_i$ para $i = 1, \ldots, m$.

I) El producto $fg = a_0b_0x^{\alpha_0+\beta_0} + \texttt{tail}(fg)$ donde los términos de $\texttt{tail}(fg)$ son menores con respecto a $>$ y $a_0b_0 \neq 0$. Como $\alpha_0 > \alpha_i$, $\forall i = 1, \ldots, n$ y $\beta_0 > \beta_i$, $\forall i = 1, \ldots, m$, se cumple que $\alpha_0+\beta_0 > \alpha_i+\beta_0 > \alpha_i+\beta_i$ (por ser $>$ un orden monomial). Así $\alpha_0 + \beta_0$ es el máximo y por lo tanto $\texttt{LE}(fg) = \alpha_0 + \beta_0 = \texttt{LE}(f) + \texttt{LE}(g)$.

II) 1) Si $\alpha_0 > \beta_0$ o $\beta_0 > \alpha_0$, entonces

$$\texttt{LE}(f+g) = \texttt{LE}(f) = \alpha_0 = \text{máx}\{\texttt{LE}(f), \texttt{LE}(g)\}$$

$$\texttt{LE}(f+g) = \texttt{LE}(g) = \beta_0 = \text{máx}\{\texttt{LE}(f), \texttt{LE}(g)\}$$

2) Si $\alpha_0 = \beta_0$ pueden ocurrir dos casos

1) Si $\texttt{LT}(f) + \texttt{LT}(g) = 0$, entonces $\texttt{LE}(f+g) < \alpha_0$ y $\texttt{LE}(f+g) < \beta_0$ y por lo tanto $\texttt{LE}(f+g) \leq \text{máx}\{\texttt{LE}(f), \texttt{LE}(g)\}$

2) Si la suma de $\texttt{LT}(f) + \texttt{LT}(g) \neq 0$, entonces $\texttt{LE}(f+g) = \text{máx}\{\texttt{LE}(f), \texttt{LE}(g)\}$

□

2. Algoritmo de división en $K[x_1, \ldots, x_n]$

Se extenderá el algoritmo de división para polinomios en $K[x]$ al anillo de polinomios en n indeterminadas $K[x_1, \ldots, x_n]$. En el caso general, el objetivo es dividir $f \in K[x_1, \ldots, x_n]$ por $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. Como veremos, esto significa expresar f en la forma

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

donde los "cocientes" $a_1, \ldots, a_s$ y "resto" r se encuentran en $K[x_1, \ldots, x_n]$. Se deberá tener cuidado al decidir cómo caracterizar el resto. Aquí es donde utilizaremos los ordenamientos monomiales introducidos anteriormente. Luego veremos cómo se aplica el algoritmo de división al problema de pertenencia de un polinomio a un ideal.

La idea básica del algoritmo es la misma que en el caso de una variable: queremos cancelar el término principal de f (con respecto a un orden monomial fijo) multiplicando un f_i por un monomio apropiado y restando. Entonces este monomio se convierte en un término en el a_i correspondiente. En lugar de enunciar el algoritmo en general, primero se trabajará con un ejemplo para observar el procedimiento.

Ejemplo 2.1. Dividir el polinomio $f = x^2y + xy^2 + y^2$ por $f_1 = xy - 1$ y $f_2 = y^2 - 1$, utilizando el orden monomial lexicográfico.
Solución: Se quiere utilizar el mismo esquema de división de polinomios en una variable, con la diferencia que ahora hay varios divisores y cocientes. Enumerando los divisores f_1, f_2 y los cocientes a_1, a_2 verticalmente, tenemos la siguiente configuración:

$$\begin{array}{r} a_1: \\ a_2: \\ \hline f_1 = xy - 1 \\ f_2 = y^2 - 1 \end{array} \overline{\big)\; x^2y + xy^2 + y^2}$$

Los términos principales $\mathtt{LT}(f_1) = xy$ y $\mathtt{LT}(f_2) = y^2$ de los cuales solamente el término principal de f_1 divide al término principal de f; $\mathtt{LT}(f) = x^2y$. En el caso que ambos términos principales de f_1 y f_2 dividan al término principal de f, procedemos primero con el de f_1. Por lo tanto, dividimos x^2y entre xy, obteniendo x, y luego restamos $x \cdot f_1$ de f:

$$\begin{array}{rl} & a_1 : x \\ & a_2 : \\ f_1 = xy - 1 & \overline{\big)\; x^2y + xy^2 + y^2} \\ f_2 = y^2 - 1 & \underline{\;\; x^2y - x} \\ & \qquad\qquad xy^2 + x + y^2 \end{array}$$

Ahora repetimos el mismo procedimiento para $xy^2 + x + y^2$. Observemos que el término principal $\mathtt{LT}(xy^2 + x + y^2) = xy^2$, es divisible por los términos principales de ambos polinomios f_1 y f_2. Por lo que usaremos f_1, ya que aparece primero.

$$\begin{array}{rl} & a_1 : x + y \\ & a_2 : \\ f_1 = xy - 1 & \overline{\big)\; x^2y + xy^2 + y^2} \\ f_2 = y^2 - 1 & \underline{\;\; x^2y - x} \\ & \qquad\quad xy^2 + x + y^2 \\ & \qquad\quad \underline{\;\; xy^2 - y} \\ & \qquad\qquad\quad x + y^2 + y \end{array}$$

Observemos que ni $\mathtt{LT}(f_1) = xy$ ni $\mathtt{LT}(f_2) = y^2$ divide $\mathtt{LT}(x + y^2 + y) = x$. Sin embargo $x + y^2 + y$ no es el resto, ya que $\mathtt{LT}(f_2)$ divide a y^2, un monomio del polinomio $x + y^2 + y$. Por lo tanto, si movemos x al resto, podemos seguir dividiendo (esto es algo que nunca ocurre en el caso de una variable, puesto que si el término principal del divisor ya no divide el término principal de lo que queda bajo el radical, el algoritmo termina).

Para implementar esta idea, anexamos una columna a la derecha, donde escribiremos los términos que pertenecen al resto. Además, llamamos al polinomio bajo el radical dividendo intermedio. Luego continuamos dividiendo hasta que el dividendo intermedio sea cero. Realizamos el paso donde movemos x a la columna del resto

$$
\begin{array}{rl}
 & a_1 : x + y \\
 & a_2 : \qquad\qquad\qquad\qquad\qquad\qquad\quad r \\
\cline{2-2}
f_1 = xy - 1 \\
f_2 = y^2 - 1
\end{array}
\left.\begin{array}{l}
x^2y + xy^2 + y^2 \\
x^2y - x \\
\hline
\qquad xy^2 + x + y^2 \\
\qquad xy^2 - y \\
\hline
\qquad\quad x + y^2 + y \longrightarrow x \\
\hline
\qquad\quad y^2 + y
\end{array}\right.
$$

Ahora continuamos dividiendo. Si podemos dividir por $\mathtt{LT}(f_1)$ o $\mathtt{LT}(f_2)$, procedemos de la forma habitual, y si ninguno de los dos divide, movemos el término principal del dividendo intermedio a la columna del resto. A continuación se muestra el resto de la división:

$$
\begin{array}{rl}
 & a_1 : x + y \\
 & a_2 : 1 \qquad\qquad\qquad\qquad\qquad\qquad\quad r \\
\cline{2-2}
f_1 = xy - 1 \\
f_2 = y^2 - 1
\end{array}
\left.\begin{array}{l}
x^2y + xy^2 + y^2 \\
x^2y - x \\
\hline
\qquad xy^2 + x + y^2 \\
\qquad xy^2 - y \\
\hline
\qquad\quad x + y^2 + y \longrightarrow x \\
\hline
\qquad\quad y^2 + y \\
\qquad\quad y^2 - 1 \\
\hline
\qquad\qquad y + 1 \longrightarrow x + y \\
\hline
\qquad\qquad\quad 1 \longrightarrow x + y + 1 \\
\hline
\qquad\qquad\quad 0
\end{array}\right.
$$

Así, el resto es $x + y + 1$ y por lo tanto, podemos expresar el polinomio $f = x^2y + xy^2 + y^2$ de la siguiente manera:

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + (1) \cdot (y^2 - 1) + x + y + 1$$

Observemos que el resto es una suma de monomios, donde ninguno de estos monomios es divisible por los términos principales $\texttt{LT}(f_1)$ o $\texttt{LT}(f_2)$ y por lo tanto para todo x^α que pertenezca al resto, $\texttt{LT}(f_i)$ no divide x^α.

El ejemplo anterior es una ilustración de cómo funciona el algoritmo de la división. También nos muestra qué propiedad queremos que tenga el resto: ninguno de sus términos debe ser divisible por los términos principales de los polinomios por los que estamos dividiendo. Ahora podemos establecer de forma general del algoritmo de división.

Teorema 2.2. (**Algoritmo de la división en** $K[x_1, \ldots, x_n]$**).** Sea $>$ un orden monomial en $\mathbb{Z}^n_{\geq 0}$ y sea $F = (f_1, \ldots, f_s)$ una s-upla ordenada de polinomios en $K[x_1, \ldots, x_n]$. Entonces cada $f \in K[x_1, \ldots, x_n]$ se puede escribir como

$$f = a_1f_1 + \cdots + a_sf_s + r$$

con $a_i, r \in K[x_1, \ldots, x_n]$ para todo i, donde $r = 0$ o bien r es una combinación lineal de monomios con coeficientes en K, donde ninguno de estos monomios es divisible por $\texttt{LT}(f_i)$, $i = 1, \ldots, s$. Llamaremos a r el resto de f en la división por F. Además, si $a_if_i \neq 0$, entonces tenemos

$$\texttt{LE}(f) \geq \texttt{LE}(a_if_i)$$

.

Demostración. Probamos la existencia de $a_1, \ldots, a_s$ y r dando un algoritmo para su construcción y mostrando que funciona correctamente en cualquier entrada dada.

Algoritmo de división en $K[x_1, \ldots, x_n]$

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
while $p \neq 0$ do
    $i := 1$
    divisionoccurred:=false
    while $i \leq s$ and divisionoccurred:=false do
        if $\mathtt{LT}(f_i)$ divides $\mathtt{LT}(p)$, then
            $a_i := a_i + \mathtt{LT}(p)/\mathtt{LT}(f_i)$
            $p := p - (\mathtt{LT}(p)/\mathtt{LT}(f_i))f_i$
            divisionoccurred:=true
        else
            $i := i + 1$
     if divisionoccurred:=false then
        $r := r + \mathtt{LT}(p)$
        $p := p - \mathtt{LT}(p)$

Podemos relacionar este algoritmo con el ejemplo anterior al observar que la variable p representa el dividendo intermedio en cada etapa, la variable r representa la columna en el lado derecho y las variables $a_1, \ldots, a_s$ los cocientes enumerados anteriormente en el radical. Finalmente, la variable booleana "divisionoccurred" nos dice cuando un $\mathtt{LT}(f_i)$ divide el término principal del dividendo intermedio. Cada vez que pasamos por el bucle principal MIENTRAS, precisamente una de estas dos opciones suceda:

- (PASO DE DIVISIÓN) si un $\mathtt{LT}(f_i)$ divide a $\mathtt{LT}(p)$, entonces el algoritmo procede como en el caso de una variable,
- (PASO DE RESIDUO) si $\mathtt{LT}(f_i)$ no divide a $\mathtt{LT}(p)$, el algoritmo agrega $\mathtt{LT}(p)$ al resto.

Estos pasos corresponden exactamente a lo que se realizó en el ejemplo.

Para demostrar que el algoritmo funciona, primero mostraremos que se mantiene en cada etapa.

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{1}$$

Observemos que es claramente cierto para los valores iniciales de $a_1, \ldots, a_s, p$ y r. Ahora supongamos que (1) se mantiene en un paso del algoritmo. Si el siguiente paso es un "PASO DE DIVISIÓN", entonces algún $\mathtt{LT}(f_i)$ divide a $\mathtt{LT}(p)$, entonces $a_i' = a_i + \mathtt{LT}(p)/\mathtt{LT}(f_i)$ y $p' = p - (\mathtt{LT}(p)/\mathtt{LT}(f_i))f_i$ por lo tanto

$$f = a_1 f_1 + \cdots + a_i' f_i + \cdots + p' + r$$

ya que

$$\begin{aligned} a_i f_i + p =& (a_i + (\mathtt{LT}(p)/\mathtt{LT}(f_i)))f_i + (p - (\mathtt{LT}(p)/\mathtt{LT}(f_i))f_i) \\ =& a_i' f_i + p' \end{aligned}$$

lo anterior muestra que $a_i f_i + p$ no se modifica. Dado que todas las demás variables no se ven afectadas, (1) sigue siendo cierto en este caso. Por otro lado, si el siguiente paso es un "PASO DE RESIDUO", entonces p y r serán cambiados, pero la suma $p+r$ no se modifica

$$p + r = (p - \mathtt{LT}(p)) + (r + \mathtt{LT}(p))$$

como antes, la igualdad (1) aún se conserva.
Observemos que el algoritmo se detiene cuando $p = 0$. En esta situación, (1) se convierte en

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

Como los términos se agregan a r solo cuando no son divisibles por ninguno de los $\mathtt{LT}(f_i)$, se deduce que $a_1, \ldots, a_s$ y r tienen las propiedades deseadas cuando el algoritmo termina.

Finalmente, se debe mostrar que el algoritmo eventualmente termina. La observación clave es que cada vez que redefinimos la variable p, su exponente principal decrece (en relación con nuestro ordenamiento de términos) o se convierte en 0. Para ver esto, primero suponer un "PASO DE DIVISIÓN", p se redefine para ser

$$p' = p - \frac{\mathtt{LT}(p)}{\mathtt{LT}(f_i)} f_i$$

Por Lema 1.9 tenemos que

$$\mathtt{LT}\left(\frac{\mathtt{LT}(p)}{\mathtt{LT}(f_i)} f_i\right) = \frac{\mathtt{LT}(p)}{\mathtt{LT}(f_i)} \mathtt{LT}(f_i) = \mathtt{LT}(p)$$

de modo que p y $(\mathtt{LT}(p)/\mathtt{LT}(f_i))f_i$ tienen el mismo término principal. Por lo tanto, su diferencia p' debe tener un exponente principal estrictamente más pequeño cuando $p' \neq 0$. Luego, supongamos un "PASO DE RESIDUO", p se redefine para ser

$$p' = p - \mathtt{LT}(p).$$

Aquí, es claro que $\mathtt{LE}(p') < \mathtt{LE}(p)$ cuando $p' \neq 0$. Por lo tanto, en cualquier caso, el exponente principal debe disminuir. Si el algoritmo nunca terminara, obtendríamos una secuencia decreciente infinita de exponentes. La propiedad del buen orden de $>$, como se indica en Lema 1.7, asegura que esto no puede ocurrir. Por lo tanto, $p = 0$ debe ocurrir eventualmente, de modo que el algoritmo finalice después de una cantidad finita de pasos.

Queda por estudiar la relación entre $\mathtt{LE}(f)$ y $\mathtt{LE}(a_i f_i)$. Cada término en a_i tiene la forma $\mathtt{LT}(p)/\mathtt{LT}(f_i)$ para algún valor de la variable p. El algoritmo comienza con $p = f$, y acabamos de demostrar que el exponente principal de p disminuye. Esto muestra que $\mathtt{LT}(p) < \mathtt{LT}(f)$, después del primer paso del algoritmo.

Como $\mathtt{LT}(p) < \mathtt{LT}(f)$ durante el algoritmo de la división, y a_i tiene la forma $\mathtt{LT}(p)/\mathtt{LT}(f_i)$ para algún p, se cumple que $\mathtt{LE}(a_i f_i) = \mathtt{LE}(\mathtt{LT}(p) f_i/\mathtt{LT}(f_i))$. Pero en la parte donde se probó que el algoritmo termina, se demostró que $\mathtt{LT}(\mathtt{LT}(p) f_i/\mathtt{LT}(f_i)) = \mathtt{LT}(p)$ por lo que se cumple la siguiente cadena de igualdad:

$$\mathtt{LE}(a_i f_i) = \mathtt{LE}(\mathtt{LT}(p) f_i/\mathtt{LT}(f_i)) = \mathtt{LE}(p) < \mathtt{LE}(f)$$

y la igualdad se cumple cuando $\mathtt{LT}(p) = \mathtt{LT}(f)$, por lo tanto:

$$\mathtt{LE}(a_i f_i) \leq \mathtt{LE}(f).$$

Esto completa la prueba del teorema. □

Una primera propiedad importante del algoritmo de división en $K[x_1, \ldots, x_n]$ es que el resto no está determinado de forma única. Para ver cómo esto puede fallar cuando hay más de una variable, consideremos el siguiente ejemplo.

Ejemplo 2.3. Dividir el polinomio $f = x^2y + xy^2 + y^2$ por $f_1 = y^2 - 1$ y $f_2 = xy - 1$. Utilizando el orden lp con $x > y$. La diferencia con el Ejemplo 2.1 es el orden en que se están tomando los divisores.

$$\begin{array}{rl}
 & a_1 : x + 1 \\
 & a_2 : x \\
 & \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad} \qquad\qquad r \\
f_1 = y^2 - 1 & \big) \; x^2y + xy^2 + y^2 \\
f_2 = xy - 1 & \big) \; x^2y - x \\
 & \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad} \\
 & \qquad\qquad xy^2 + x + y^2 \\
 & \qquad\qquad xy^2 - x \\
 & \qquad\qquad \overline{\qquad\qquad\qquad\qquad} \\
 & \qquad\qquad\qquad 2x + y^2 \qquad \longrightarrow \quad 2x \\
 & \qquad\qquad\qquad \overline{\qquad\qquad\qquad} \\
 & \qquad\qquad\qquad\qquad y^2 \\
 & \qquad\qquad\qquad\qquad y^2 - 1 \\
 & \qquad\qquad\qquad\qquad \overline{\qquad\qquad} \\
 & \qquad\qquad\qquad\qquad\qquad 1 \quad \longrightarrow \quad 2x + 1 \\
 & \qquad\qquad\qquad\qquad\qquad \overline{\qquad} \\
 & \qquad\qquad\qquad\qquad\qquad 0
\end{array}$$

por lo tanto podemos expresar el polinomio f de la siguiente manera:

$$f = x^2y + xy^2 + y^2 = (x+1)(y^2-1) + (x)(xy-1) + 2x + 1$$

Si comparamos este resultado con el Ejemplo 2.1, observamos que el resto es diferente.

Los ejemplos anteriores muestran que el orden de la s-upla de polinomios $(f_1, \ldots, f_s)$ definitivamente importa, tanto en la cantidad de pasos que tomará el algoritmo para completar el cálculo y en los resultados que se obtendrán. El a_i y el r pueden cambiar si simplemente reorganizamos los f_i o se cambia el orden monomial.

Una buena característica del algoritmo de división en $K[x_1, \ldots, x_n]$ es la forma en que resuelve el problema de pertenencia al ideal, es decir, dado un ideal $I \subset K[x_1, \ldots, x_n]$ y $f \in K[x_1, \ldots, x_n]$; determinar si el polinomio $f \in I$. Si después de la división de f por $F = (f_1, \ldots, f_s)$ obtenemos un resto $r = 0$, observar que

$$f = a_1 f_1 + \cdots + a_s f_s$$

así, $f \in \langle f_1, \ldots, f_s \rangle$. Por lo tanto, $r = 0$ es una condición suficiente para la pertenencia al ideal. Sin embargo, como muestra el siguiente ejemplo, $r = 0$ no es una condición necesaria para estar en el ideal.

Ejemplo 2.4. Sea $f_1 = xy + 1$, $f_2 = y^2 - 1 \in K[x, y]$ con el orden lexicográfico *lp*. Dividimos $f = xy^2 - x$ por $F = (f_1, f_2)$, el resultado es

$$xy^2 - x = (y)(xy+1) + (0)(y^2-1) + (-x-y).$$

Cuando $F = (f_2, f_1)$, sin embargo, el resultado es

$$xy^2 - x = (x)(y^2-1) + (0)(xy+1) + 0$$

El segundo cálculo muestra que $f \in \langle f_1, f_2 \rangle$. Luego, el primer cálculo muestra que incluso si $f \in \langle f_1, f_2 \rangle$, aún es posible obtener un resto distinto de cero en la división mediante $F = (f_1, f_2)$.

Al tratar con una colección de polinomios $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, con frecuencia es deseable pasar al ideal I que generan. Esto permite la posibilidad de pasar de $f_1, \ldots, f_s$ a un conjunto de generadores diferentes para I. Entonces todavía podemos preguntarnos si podría haber un "buen" conjunto de generadores para I.. Para dicho conjunto, desearíamos que el resto de la división de los generadores "buenos" se determine de manera única y la condición $r = 0$ debería ser equivalente a la pertenencia en el ideal. Más adelante veremos que las bases de Gröbner tienen exactamente estas "buenas" propiedades.

Ejemplo 2.5. Dividir el polinomio $f = x^7y^2 + x^3y^2 - y + 1$ por $F = (xy^2 - x, x - y^3)$. Al usar el orden monomial lexicográfico *lp* obtenemos:

$$x^7y^2+x^3y^2-y+1 = (x^6+x^5y+x^4y^2+x^4+x^3y+x^2y^2)(xy^2-x)+(x^6+x^5y+x^4+x^3y)(x-y^3)-y+1$$

para obtener la expresión anterior se deben realizar muchos pasos en la división. Sin embargo utilizando el ordenamiento lexicográfico graduado Dp la cantidad de pasos se reduce considerablemente

$$
\begin{array}{rl|l}
 & a_1 : x^6 + x^2 & \\
 & a_2 : & r \\
\hline
f_1 = xy^2 - x & x^7y^2 + x^3y^2 - y + 1 & \\
f_2 = -y^3 + x & x^7y^2 - x^7 & \\
\hline
 & x^7 + x^3y^2 - y + 1 \quad \longrightarrow & x^7 \\
\hline
 & x^3y^2 - y + 1 & \\
 & x^3y^2 - x^3 & \\
\hline
 & x^3 - y + 1 \quad \longrightarrow & x^7 + x^3 \\
\hline
 & -y + 1 \quad \longrightarrow & x^7 + x^3 - y \\
\hline
 & 1 \quad \longrightarrow & x^7 + x^3 - y + 1 \\
\hline
 & 0 &
\end{array}
$$

podemos escribir a f de la siguiente manera:

$$x^7 + x^3y^2 + x^3y^2 - y + 1 = (x^6 + x^2)(xy^2 - x) + (0)(x - y^3) + x^7 + x^3 - y + 1$$

Observemos que en el ejemplo anterior queda claro que el orden monomial juega un papel muy importante a la hora de realizar la división.

3. Ideales monomiales y lema de Dickson

En esta sección, vamos a considerar el problema de "descripción de ideales" (¿puede cada ideal $I \subset K[x_1, \ldots, x_n]$ escribirse como $\langle f_1, \ldots, f_s \rangle$ para algunos $f_i \in K[x_1, \ldots, x_n]$?), para el caso especial de ideales monomiales. Esto requerirá un estudio cuidadoso de las propiedades de estos ideales. Para comenzar, definimos ideales monomiales en $K[x_1, \ldots, x_n]$.

Definición 3.1. Un ideal $I \subset K[x_1, \ldots, x_n]$ es un *ideal monomial* si hay un subconjunto $A \subset \mathbb{Z}^n_{\geq 0}$ (posiblemente infinito) de modo que I consiste en todos los polinomios que son sumas finitas de la forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, donde $h_\alpha \in K[x_1, \ldots, x_n]$. En este caso, denotaremos a $I = \langle x^\alpha : \ \alpha \in A \rangle$.

Un ejemplo de un ideal monomial es dado por $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subset K[x, y]$. Se darán ejemplos más interesantes de ideales monomiales más adelante.

Primero necesitamos caracterizar todos los monomios que se encuentran en un ideal monomial dado.

Lema 3.2. Sea $I = \langle x^\alpha : \ \alpha \in A \rangle$ un ideal monomial. Entonces, un monomio x^β se encuentra en I si y solo si x^β es divisible por x^α, para algún $\alpha \in A$.

Demostración. Si x^β es un múltiplo de x^α para algún $\alpha \in A$, entonces $x^\beta \in I$ por la definición de ideal.
Recíprocamente, si $x^\beta \in I$, entonces $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, donde $h_i \in K[x_1, \ldots, x_n]$ y $\alpha(i) \in A$. Si expandimos cada h_i como una combinación lineal de monomios, vemos que cada término en el lado derecho de la ecuación es divisible por algún $x^{\alpha(i)}$. Por lo tanto, el lado izquierdo x^β debe tener la misma propiedad. □

Notar que x^β es divisible por x^α exactamente cuando $x^\beta = x^\alpha \cdot x^\gamma$ para algún $\gamma \in \mathbb{Z}^n_{\geq 0}$. Esto es equivalente a que $\beta = \alpha + \gamma$. Por lo tanto, el conjunto

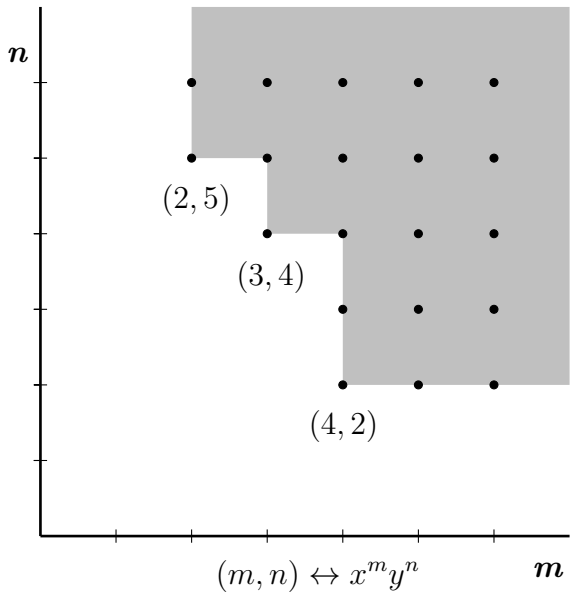
$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \ \gamma \in \mathbb{Z}^n_{\geq 0}\}$$

consiste en los exponentes de todos los monomios divisibles por x^α. Esta observación y el Lema 3.2 nos permiten dibujar ilustraciones de los monomios en un ideal monomial dado.

Por ejemplo, si $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$, entonces los exponentes de los monomios en I forman el conjunto

$$((4, 2) + \mathbb{Z}^2_{\geq 0}) \cup ((3, 4) + \mathbb{Z}^2_{\geq 0}) \cup ((2, 5) + \mathbb{Z}^2_{\geq 0})$$

Podemos visualizar este conjunto como la unión de los puntos enteros en tres copias traducidas del primer cuadrante en el plano:



Lema 3.3. Sea I un ideal monomial, y sea $f \in K[x_1, \ldots, x_n]$. Entonces los siguientes enunciados son equivalentes:

I) $f \in I$.

II) Cada término de f se encuentra en I.

III) f es una combinación K-lineal de los monomios en I.

Demostración. Las implicaciones $III) \Rightarrow II) \Rightarrow I)$ se cumplen por definición.
La prueba de $I) \Rightarrow III)$, sea $f \in I$, donde I es un ideal monomial. Entonces f se puede representar como una suma fina $f = \sum_{\alpha} h_\alpha x^\alpha$ donde $h_\alpha \in K[x_1, \ldots, x_n]$. Expandiendo el polinomio h_α

$$f = \sum_{\alpha} h_\alpha x^\alpha = \sum_{\alpha} \left(\sum c_\beta x^\beta \right) x^\alpha = \sum c_\beta x^\beta x^\alpha$$

así f es una K-lineal combinación de monomios de I. □

Corolario 3.4. Dos ideales monomiales son iguales si y solo si contienen los mismos monomios.

El resultado principal de esta sección es que todos los ideales monomiales de $K[x_1, \ldots, x_n]$, son finitamente generados.

Teorema 3.5. (**Lema de Dickson).** Sea $I = \langle x^\alpha : \ \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ un ideal monomial. Entonces I se puede escribir en la forma $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, donde $\alpha(1), \ldots, \alpha(s) \in A$. En particular, I tiene una base finita.

Demostración. (Por inducción en n, el número de variables).
Si $n = 1$, entonces I es generado por los monomios x_1^α, donde $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Sea $\beta \leq \alpha$ el elemento más pequeño de $A \subset \mathbb{Z}_{\geq 0}$. Entonces $\beta \leq \alpha$ para todo $\alpha \in A$, de modo que x_1^β divide a todos los demás generadores x_1^α. Por lo que se tendrá $I = \langle x_1^\beta \rangle$.

Ahora asumir que $n > 1$ y que el teorema es cierto para $n - 1$. Escribiremos las variables como $x_1, \ldots, x_{n-1}, y$, para que los monomios en $K[x_1, \ldots, x_{n-1}, y]$ se puedan escribir como $x^\alpha y^m$, donde $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ y $m \in \mathbb{Z}_{\geq 0}$.

Supongamos que $I \subset K[x_1, \ldots, x_{n-1}, y]$ es un ideal monomial. Para encontrar generadores para I, sea J el ideal en $K[x_1, \ldots, x_{n-1}]$ generado por los monomios x^α para los cuales $x^\alpha y^m \in I$ para algunos $m \geq 0$. Ya que J es un ideal monomial en $K[x_1, \ldots, x_{n-1}]$, nuestra hipótesis inductiva implica que una cantidad finita de los x^α's generan J, expresamos $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. El ideal J se puede entender como la "proyección" de I en $K[x_1, \ldots, x_{n-1}]$.

Para cada i entre 1 y s, la definición de J nos dice que $x^{\alpha(i)} y^{m_i} \in I$ para algún $m_i \geq 0$. Sea m el más grande de los m_i. Luego, para cada k entre 0 y $m - 1$, consideremos el ideal $J_k \subset K[x_1, \ldots, x_{n-1}]$ generado por los monomios x^β tal que $x^\beta y^k \in I$.
Se puede pensar en J_k como la "rebanada" de I generada por monomios que contiene a y exactamente a la k-ésima potencia. Utilizando de nuevo nuestra hipótesis inductiva, J_k tiene un conjunto finito de monomios tal que $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle$.

Afirmamos que I es generado por los monomios en la siguiente lista:

$$\begin{aligned}
\text{De } J\text{:} \quad & x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m, \\
\text{De } J_0\text{:} \quad & x^{\alpha(1)}, \ldots, x^{\alpha_0(s_0)}, \\
\text{De } J_1\text{:} \quad & x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y, \\
& \vdots \\
\text{De } J_{m-1}\text{:} \quad & x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1},
\end{aligned}$$

Primero notar que cada monomio en I es divisible por uno en la lista. Para ello, sea $x^\alpha y^p \in I$. Si $p \geq m$, entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha(i)} y^m$ por la construcción de J. Por otro lado, si $p \leq m - 1$, entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha_p(j)} y^p$ por la construcción de J_p. Del Lema 3.2 se deduce que los monomios anteriores generan un ideal que tiene los mismos monomios que I. Por Corolario 3.4, esto obliga a los ideales a ser iguales.

Para completar la demostración del teorema, necesitamos mostrar que el conjunto finito de generadores se puede elegir de un conjunto dado de generadores para el ideal. Si volvemos a escribir las variables como $x_1, \ldots, x_n$, entonces nuestro ideal monomial es $I = \langle x^\alpha : \ \alpha \in A \rangle \subset K[x_1, \ldots, x_n]$.

Necesitamos mostrar que I está generado por un número finito de x^α's, donde $\alpha \in A$. De lo anterior, sabemos que $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ para algunos monomios $x^{\beta(i)}$ en I. Como $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A \rangle$, Lema 3.2 nos dice que cada $x^{\beta(i)}$ es divisible por $x^{\alpha(i)}$ para algún $\alpha(i) \in A$. Desde aquí, es fácil mostrar que $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Tenemos que $\alpha(i) \in A$ implica $\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle \subset \langle x^\alpha : \alpha \in A \rangle = I$. Por otra parte, cada $x^{\beta(i)}$ es divisible por $x^{\alpha(i)}$ por Lema 3.2 $x^{\beta(i)} \in \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, y por lo tanto $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle \subset \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. □

Para comprender mejor cómo funciona la demostración del Teorema 3.5, apliquémoslo al ideal $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$ discutido anteriormente en la sección. En la ilustración de los exponentes, se puede observar que la "proyección" es $J = \langle x^2 \rangle \subset K[x]$. Ya que $x^2y^5 \in I$, tenemos $m = 5$. Luego obtenemos las "rebanadas" $J_k, 0 \leq k \leq 4 = m - 1$, generadas por monomios que contienen y^k:

$$J_0 = J_1 = \langle 0 \rangle$$

$$J_2 = J_3 = \langle x^4 \rangle$$

$$J_4 = \langle x^3 \rangle$$

Estas "rebanadas" son fáciles de ver usando la ilustración de los exponentes. Entonces según la demostración del Teorema 3.5 se tiene que $I = \langle x^2y^5, x^4y^2, x^4y^3, x^3y^4 \rangle$.

Observación 3.6. El Lema de Dickson es equivalente a la siguiente proposición: dado $A \subset \mathbb{Z}^n_{\geq 0}$, entonces existe un subconjunto finito $B \subset A$ que satisface:

$$\forall \alpha \in A,\ \exists \beta \in M \text{ tal que } \beta \leq_{\text{nat}} \alpha.$$

Recordemos que los monomios con exponente de la forma $\alpha + \mathbb{Z}^n_{\geq 0}$ son divisibles por los monomios x^α, es decir que para cualquier monomio con exponente en A existe al menos un monomio con exponente en B tal que lo divide.

Se probará ahora la equivalencia:

$\Rightarrow$: Asumiendo como cierto el lema de Dickson, se probará la observación. Sea $A \subset \mathbb{Z}^n_{\geq 0}$, y sea $I = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial , entonces I tiene una base finita, es decir $I = \langle x^{\beta_1}, \ldots, x^{\beta_s} \rangle$, donde $\beta_i \in A$, de aquí se tiene que para todo monomio $x^\alpha \in I$ existe un x^{β_i} que lo divide, es decir $\beta_i \leq_{\text{nat}} \alpha$, así tomando $B = \{\beta_1, \ldots, \beta_s\}$, este conjunto cumple que $\forall \alpha \in A,\ \exists \beta_i \in B$ tal que $\beta_i \leq_{\text{nat}} \alpha$.

$\Leftarrow$: Sea $I = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial, considerando al conjunto $A \subset \mathbb{Z}^n_{\geq 0}$, por la observación, existe un subconjunto finito $B = \{\beta_1, \ldots, \beta_s\} \subset A$, que cumple que $\forall \alpha \in A,\ \exists \beta_i \in B$ con $\beta_i \leq_{\text{nat}} \alpha$, es decir $(\beta_{i_1}, \ldots, \beta_{i_n}) \leq_{\text{nat}} (\alpha_1, \ldots, \alpha_n)$, o lo que es lo mismo $\beta_{i_j} \leq \alpha_j$ para todo $j = 1, \ldots, n$. Así para cualquier $x^\alpha \in A$, existe $\beta_i \in B$ tal

que $\beta_i \leq_{\text{nat}} \alpha$, es decir $x^{\beta_i} \mid x^{\alpha}$, y así se concluye que $I = \langle x^{\beta_1}, x^{\beta_2}, \ldots, x^{\beta_s} \rangle$, es decir I tiene una base finita.

El Teorema 3.5 resuelve el problema de descripción de un ideal, para el caso de ideales monomiales, ya que muestra que todo ideal monomial tiene una base finita. Esto a su vez, nos permite resolver el problema de pertenencia a un ideal para los ideales monomiales. Es decir, si $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, entonces se puede mostrar fácilmente que un polinomio dado f está en I si y solo si el resto de f en la división por $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ es cero.

También podemos usar el Lema de Dickson para probar el siguiente hecho importante acerca de los ordenamientos monomiales en $K[x_1, \ldots, x_n]$.

Corolario 3.7. Sea $>$ una relación en $\mathbb{Z}^n_{\geq 0}$ que satisface:

I) $>$ es un ordenamiento total en $\mathbb{Z}^n_{\geq 0}$.

II) Si $\alpha > \beta$ y $\gamma \in \mathbb{Z}^n_{\geq 0}$, entonces $\alpha + \gamma > \beta + \gamma$.

Entonces $>$ es un buen orden si y solo si $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Demostración. $\Rightarrow$: Suponiendo que $>$ es un buen orden, sea α_0 el elemento más pequeño de $\mathbb{Z}^n_{\geq 0}$. Basta con mostrar $\alpha_0 \geq 0$. Esto es fácil: si $0 > \alpha_0$, entonces por la hipótesis (II), podemos agregar α_0 a ambos lados para obtener $\alpha_0 > 2\alpha_0$, lo cual es imposible ya que α_0 es el elemento más pequeño de $\mathbb{Z}^n_{\geq 0}$.

$\Leftarrow$: Suponiendo que $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$, sea $A \subset \mathbb{Z}^n_{\geq 0}$ no vacío. Necesitamos mostrar que A tiene un elemento más pequeño. Como $I = \langle x^{\alpha} : \ \alpha \in A \rangle$ es un ideal monomial, el Lema de Dickson nos da $\alpha(1), \ldots, \alpha(s) \in A$ tal que $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Reetiquetando si es necesario, podemos suponer que $\alpha(1) < \alpha(2) < \ldots < \alpha(s)$. Afirmamos que $\alpha(1)$ es el elemento más pequeño de A. Para probar esto, tomemos $\alpha \in A$, entonces $x^{\alpha} \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, por Lema 3.2, x^{α} es divisible por algún $x^{\alpha(i)}$. Esto nos dice que $\alpha = \alpha(i) + \gamma$ para algún $\gamma \in \mathbb{Z}^n_{\geq 0}$. Entonces $\gamma \geq 0$ y por hipótesis (II) implican que

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1).$$

Por lo tanto, $\alpha(1)$ es el elemento más pequeño de A. □

4. El teorema de la base de Hilbert y las bases de Gröbner

En esta sección, se da una solución completa al problema de descripción de un ideal, es decir para un ideal $I \subset K[x_1, \ldots, x_n]$ cualquiera, conduciendo así a bases de ideales con propiedades "buenas" en relación con el algoritmo de división presentado antes.

La idea clave que se utiliza es que una vez elegido un orden monomial, cada $f \in K[x_1, \ldots, x_n]$ tiene un término principal único $\mathtt{LT}(f)$. Entonces, para cualquier ideal I, podemos definir su ideal de términos principales de la siguiente manera.

Definición 4.1. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal distinto de $\{0\}$.

i) Denotamos por $\mathtt{LT}(I)$ al conjunto de términos principales de elementos de I. Por lo tanto,
$$\mathtt{LT}(I) = \{cx^\alpha : \text{ existe } f \in I \text{ con } \mathtt{LT}(f) = cx^\alpha\}$$

ii) Denotamos por $\langle \mathtt{LT}(I) \rangle$ al ideal generado por los elementos de $\mathtt{LT}(I)$.

Ya hemos visto que los términos principales juegan un papel importante en el algoritmo de división. Esto nos hace señalar un punto muy sutil, pero importante con respecto a $\mathtt{LT}(I)$. Si se nos da un conjunto generador finito para I, digamos $I = \langle f_1, \ldots, f_s \rangle$, entonces $\langle \mathtt{LT}(f_1), \ldots, \mathtt{LT}(f_s) \rangle$ y $\mathtt{LT}(I)$ pueden ser ideales diferentes. Es cierto que $\mathtt{LT}(f_i) \in \mathtt{LT}(I) \subset \langle \mathtt{LT}(I) \rangle$ por definición, lo que implica $\langle \mathtt{LT}(f_1), \ldots, \mathtt{LT}(f_s) \rangle \subset \langle \mathtt{LT}(I) \rangle$. Sin embargo, $\langle \mathtt{LT}(I) \rangle$ puede ser estrictamente más grande. Para ver esto, consideremos el siguiente ejemplo.

Ejemplo 4.2. Sea $I = \langle f_1, f_2 \rangle$, donde $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$, y usando el ordenamiento monomial lexicográfico graduado Dp en $K[x, y]$. Entonces

$$x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2,$$

de modo que $x^2 \in I$. Así $x^2 = \mathtt{LT}(x^2) \in \langle \mathtt{LT}(I) \rangle$. Sin embargo, x^2 no es divisible por $\mathtt{LT}(f_1) = x^3$ o $\mathtt{LT}(f_2) = x^2y$, de modo que $x^2 \notin \langle \mathtt{LT}(f_1), \mathtt{LT}(f_2) \rangle$ por Lema 3.2. Por lo tanto $\langle \mathtt{LT}(f_1), \mathtt{LT}(f_2) \rangle \subset \langle \mathtt{LT}(I) \rangle$.

Demostrar que $\langle \mathtt{LT}(I) \rangle$ es un ideal monomial, nos permitirá aplicar los resultados de la sección anterior. En particular, se seguirá que $\langle \mathtt{LT}(I) \rangle$ es generado por una cantidad finita de términos principales.

Proposición 4.3. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal.

i) $\langle \mathtt{LT}(I) \rangle$ es un ideal monomial.

ii) Existen $g_1, \ldots, g_t \in I$ tal que $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$

Demostración.

i) Los monomios principales $\mathtt{LM}(g)$ de los elementos $g \in I - \{0\}$ generan el ideal monomial $\langle \mathtt{LM}(g) : \ g \in I - \{0\} \rangle$. Como $\mathtt{LM}(g)$ y $\mathtt{LT}(g)$ difieren en una constante distinta de cero, este ideal es igual a $\langle \mathtt{LT}(g) : \ g \in I - \{0\} \rangle = \langle \mathtt{LT}(I) \rangle$ (los ideales son cerrados bajo la multiplicación por escalares de K). Por lo tanto, $\langle \mathtt{LT}(I) \rangle$ es un ideal monomial.

II) Como $\langle \mathtt{LT}(I) \rangle$ es generado por los monomios $\mathtt{LM}(g)$ para $g \in I - \{0\}$, el Lema de Dickson nos dice que $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LM}(g_1), \ldots, \mathtt{LM}(g_t) \rangle$ para una cantidad finita de $g_1, \ldots, g_t \in I$. Como $\mathtt{LM}(g_i)$ y $\mathtt{LT}(g_i)$ difieren por una constante distinta de cero, se deduce que $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. Esto completa la prueba.

□

Definición 4.4. Un anillo es llamado Noetheriano si cada ideal es finitamente generado.

Está claro que todo campo es un anillo Noetheriano, es un hecho fundamental que todo anillo de polinomio $K[x_1, \ldots, x_n]$ sobre un campo K es un anillo de polinomios Noetheriano; que es el contenido del teorema de la base de Hilbert.

Ahora podemos usar la Proposición 4.3 y el algoritmo de división para probar la existencia de un conjunto finito de generadores para cada ideal del anillo multivariado de polinomios, dando así una respuesta afirmativa al problema de descripción de un ideal. Sea $I \subset K[x_1, \ldots, x_n]$ cualquier ideal y consideremos el ideal asociado $\langle \mathtt{LT}(I) \rangle$ como en la Definición 4.1 y seleccionado un orden monomial particular para usar en el algoritmo de división y tomar los términos principales.

Teorema 4.5. (Teorema de la base de Hilbert). Cada ideal $I \subset K[x_1, \ldots, x_n]$ tiene un conjunto generador finito. Es decir, $I = \langle g_1, \ldots, g_t \rangle$ para algunos $g_1, \ldots, g_t \in I$.

Demostración. Si $I = \{0\}$, el conjunto generador es $\{0\}$, el cual es finito. Si I contiene algún polinomio distinto de cero, entonces un conjunto generador $g_1, \ldots, g_t$ para I se puede construir de la siguiente manera. Por la Proposición 4.3, existen $g_1, \ldots, g_t \in I$ tal que $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. Probemos que $I = \langle g_1, \ldots, g_t \rangle$.
Está claro que $\langle g_1, \ldots, g_t \rangle \subset I$, ya que cada $g_i \in I$.
Por el contrario, sea $f \in I$ cualquier polinomio. Si aplicamos el algoritmo de división para dividir f por $g_1, \ldots, g_t$, entonces obtenemos una expresión de la forma:

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

donde ningún término de r es divisible por ninguno de los $\mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t)$. Entonces $r = 0$. Para ver esto, se debe tener en cuenta que $r = f - a_1 g_1 - \cdots - a_t g_t \in I$. Si $r \neq 0$ entonces $\mathtt{LT}(r) \in \langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$, y por Lema 3.2, se deduce que $\mathtt{LT}(r)$ debe ser divisible por $\mathtt{LT}(g_i)$ para algún i. Esto contradice el hecho que r es residuo, y en consecuencia $r = 0$.
Así

$$f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle$$

que muestra que $I \subset \langle g_1, \ldots, g_t \rangle$. Por lo tanto $I = \langle g_1, \ldots, g_t \rangle$. □

Además de resolver el problema de descripción de un ideal, la base $\{g_1, \ldots, g_t\}$ usada en el teorema anterior tiene la propiedad especial que $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$, ya que no todas las bases cumplen dicha propiedad.

Definición 4.6. Fijando un orden monomial. Un subconjunto finito $G = \{g_1, \ldots, g_t\}$ de un ideal I se dice que es una base de Gröbner si

$$\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$$

Corolario 4.7. Fijado un orden monomial. Entonces cada ideal $I \subset K[x_1, \ldots, x_n]$ distinto de $\{0\}$ tiene una base de Gröbner. Además, cualquier base de Gröbner para I, es una base para I.

Demostración. Dado un ideal I distinto de cero, el conjunto $G = \{g_1, \ldots, g_n\}$ construido en la demostración del Teorema 3.5 es una base de Gröbner por definición. Para probar que cualquier base de Gröbner para I es una base para I, debemos tener en cuenta que si $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$, el argumento del Teorema 3.5 muestra que $I = \langle g_1, \ldots, g_t \rangle$, de modo que G es una base para I. □

Ejemplo 4.8. Sea $I = \langle f_1, f_2 \rangle$, con $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Una base para I es $\{f_1, f_2\}$, entonces $\{f_1, f_2\}$, no es una base de Gröbner para I con respecto al orden monomial lexicográfico graduado *Dp*, ya que $x^2 \in \langle \mathtt{LT}(I) \rangle$, pero $x^2 \notin \langle \mathtt{LT}(f_1), \mathtt{LT}(f_2) \rangle$

Concluimos esta sección con dos aplicaciones del Teorema de la Base de Hilbert. El primero es una afirmación algebraica sobre los ideales en $K[x_1, \ldots, x_n]$.
Una cadena ascendente de ideales es una secuencia creciente anidada

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

Por ejemplo, la secuencia

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, \ldots, x_n \rangle$$

forma una cadena ascendente (finita) de ideales, si intentamos extender esta cadena incluyendo un ideal con más generadores, ocurrirá una de dos alternativas. Consideremos el ideal $\langle x_1, \ldots, x_n \rangle$ donde $f \in K[x_1, \ldots, x_n]$, si $f \in \langle x_1, \ldots, x_n \rangle$, entonces obtenemos $\langle x_1, \ldots, x_n \rangle$ de nuevo y nada ha cambiado. Si por otro lado $f \notin \langle x_1, \ldots, x_n \rangle$, entonces decimos $\langle x_1, \ldots, x_n, f \rangle = K[x_1, \ldots, x_n]$. En cualquier caso, la cadena ascendente se habrá estacionado después de un número finito de pasos, en el sentido de que todos los ideales posteriores a ese punto de la cadena serán iguales.

Teorema 4.9. (**La condición de cadena ascendente).** Sea $I_1 \subset I_2 \subset I_3 \subset \ldots$ una cadena ascendente de ideales en $K[x_1, \ldots, x_n]$. Entonces existe un $N \geq 1$ tal que

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

Demostración. Dada una cadena ascendente $I_1 \subset I_2 \subset I_3 \subset \ldots$, consideremos el conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Comenzamos mostrando que I también es un ideal en $K[x_1, \ldots, x_n]$. Primero, $0 \in I$ ya que $0 \in I_i$ para todo i. Ahora si $f, g \in I$, entonces por definición

$f \in I_i$ y $g \in I_j$ para algún i y j posiblemente diferentes. Sin embargo, ya que los I_i forman una cadena ascendente, si reetiquetamos de modo que $i \leq j$, entonces tanto f como g están en I_j. Ya que I_j es un ideal, la suma $f + g \in I_j$ y por lo tanto $f + g \in I$. Similarmente si $f \in I$ y $g \in K[x_1, \ldots, x_n]$, entonces $f \in I_i$ para algún i y $g \cdot f \in I_i \subset I$. Por lo tanto I es un ideal.

Según el teorema de la Base de Hilbert, el ideal I debe tener un conjunto finito generador: $I = \langle f_1, \ldots, f_s \rangle$. Pero cada uno de los generadores está contenido en alguno de los I_j, digamos $f_i \in I_{j_i}$ para algún $j_i, i = 1, \ldots, s$. Sea N el máximo de los j_i. Luego mediante la definición de cadena ascendente $f_i \in I_N$ para todo i. Por lo tanto tenemos:

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I$$

Como resultado la cadena se estabiliza con I_N. Todos los ideales posteriores son iguales. □

Observación 4.10. Cada conjunto no vacío de ideales $S \subset K[x_1, \ldots, x_n]$, tiene un elemento maximal (con respecto a la inclusión). En efecto, supongamos que el conjunto S no tiene un elemento maximal. Tomamos cualquier ideal de S, digamos I_1, ya que no es un ideal maximal podemos escoger un ideal $I_2 \subset S$ tal que $I_1 \subset I_2$ y $(I_1 \neq I_2)$. Continuando de esta manera, escogemos un ideal I_{N+1} tal que $I_N \subset I_{N+1}$ y $(I_N \neq I_{N+1})$. Formando así una cadena ascendente de ideales de S:

$$I_1 \subset I_2 \subset \cdots \subset I_N \subset I_{N+1} \subset \ldots$$

Lo cual contradice la condición de cadena ascendente. Por lo tanto el conjunto S tiene un elemento maximal.

La segunda consecuencia del teorema de la base de Hilbert será geométrica. Sabemos que las variedades afines son los conjuntos de soluciones de conjuntos finitos de ecuaciones polinomiales.

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : \ f_i(a_1, \ldots, a_n) = 0, \ \forall i\}$$

El teorema de la base de Hilbert muestra que tiene sentido hablar de la variedad afín definida por un ideal $I \subset K[x_1, \ldots, x_n]$.

Definición 4.11. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal. Denotaremos por $V(I)$ al conjunto

$$V(I) = \{(a_1, \ldots, a_n) \in K^n : \ f(a_1, \ldots, a_n) = 0, \ \forall f \in I\}$$

Aunque un ideal I distinto de cero contiene infinitamente muchos polinomios diferentes, el conjunto $V(I)$ aún se puede definir mediante un conjunto finito de ecuaciones polinomiales.

Proposición 4.12. $V(I)$ es una variedad afín. En particular, si $I = \langle f_1, \ldots, f_s \rangle$, entonces $V(I) = V(f_1, \ldots, f_s)$.

Demostración. Por el teorema de la base de Hilbert, $I = \langle f_1, \ldots, f_s \rangle$ para algún conjunto generador finito. Pretendemos que $V(I) = V(f_1, \ldots, f_s)$. Primero, ya que $f_i \in I$, si $f(a_1, \ldots, a_n) = 0$ para todo $f \in I$, entonces $f_i(a_1, \ldots, a_n) = 0$, así que $V(I) \subset V(f_1, \ldots, f_s)$.
Por otro lado sea $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ y sea $f \in I$, ya que $I = \langle f_1, \ldots, f_s \rangle$, podemos escribir $f = \sum_{i=1}^{s} h_i f_i$ para algún $h_i \in K[x_1, \ldots, x_n]$.
Pero entonces

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0 \end{aligned}$$

Entonces $V(f_1, \ldots, f_s) \subset V(I)$ y por lo tanto se cumple la igualdad □

5. Propiedades de las bases de Gröbner

Como se demostró antes, cada ideal $I \subset K[x_1, \ldots, x_n]$ tiene una base de Gröbner. En esta sección estudiaremos las propiedades y aprenderemos a detectar cuando una base es una base de Gröbner. Comenzamos mostrando que el comportamiento no deseado del algoritmo de la división en $K[x_1, \ldots, x_n]$ no ocurre cuando dividimos por los elementos de una base de Gröbner. Primero mostraremos que el resto está determinado de forma única cuando dividimos por una base de Gröbner.

Proposición 5.1. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para un ideal $I \subset K[x_1, \ldots, x_n]$ y sea $f \in K[x_1, \ldots, x_n]$. Entonces existe un único $r \in K[x_1, \ldots, x_n]$ con las siguientes propiedades:

i) Ningún término de r es divisible por ninguno de los $\mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t)$.

ii) Existe un $g \in I$ tal que $f = g + r$.

En particular, r es el resto de la división de f por G, sin importar como se enumeren los elementos de G cuando se usa el algoritmo de la división.

Demostración. Por el algoritmo de la división se tiene que $f = a_1 g_1 + \cdots + a_t g_t + r$, donde r satisface la condición I).
También podemos satisfacer II) estableciendo $g = a_1 g_1 + \cdots + a_t g_t \in I$. Esto prueba la existencia de r.
Para probar la unicidad, supongamos que $f = g + r = g' + r'$ satisface I) y II). Entonces $r - r' = g' - g \in I$, de modo que si $r \neq r'$, entonces $\mathtt{LT}(r - r') \in \langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. Por Lema 3.2 se deduce que $\mathtt{LT}(r - r')$ es divisible por algún $\mathtt{LT}(g_i)$. Esto es imposible, ya que ninguno de los términos de r y r', son divisibles por ninguno

de los $\mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t)$. Por lo tanto $r - r'$ debe ser cero, y se prueba la unicidad. La parte final se deriva de la unicidad de r. □

Aunque el resto r es único, incluso para una base de Gröbner los cocientes a_i producidos por el algoritmo de división $f = a_1g_1 + \cdots + a_tg_t + r$, pueden cambiar si enumeramos los generadores en un orden diferente.

Corolario 5.2. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para un ideal $I \subset K[x_1, \ldots, x_n]$. Entonces $f \in I$ si y solo si el residuo en la división de f por G es cero.

Demostración. Si el resto es cero, entonces $f \in I$.
Por el contrario, dado $f \in I$, entonces $f = f + 0$ satisface las condiciones de la Proposición 5.1 se sigue que cero es el resto de f en la división por G. □

El corolario anterior a veces es tomado como la definición de una base de Gröbner. Usando el Corolario 5.2, obtenemos un algoritmo para resolver el problema de pertenencia de un ideal, siempre que conozcamos una base de Gröbner para el ideal en cuestión, solo necesitamos calcular un resto con respecto a G para determinar si $f \in I$.

Definición 5.3. Escribiremos $\bar{f}^F$ para el resto de la división de f por la s-upla $F = (f_1, \ldots, f_s)$. Si F es una base de Gröbner para el ideal I entonces podemos considerar a F como un conjunto (sin ningún orden particular) por Proposición 5.1.

Definición 5.4. Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios distintos de cero, con $\mathtt{LM}(f) = x^\alpha$ y $\mathtt{LM}(g) = x^\beta$

I) Denotamos por $x^\gamma = \mathtt{lcm}(x^\alpha, x^\beta)$ al *mínimo común múltiplo* de los monomios x^α y x^β, que se define de la siguiente manera: $\gamma = (\gamma_1, \ldots, \gamma_n)$, donde $\gamma_i = \max(\alpha_i, \beta_i)$ para cada i.

II) El *S-polinomio* (spoly) de f y g es la combinación

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

Si $\mathtt{LM}(g)$ divide $\mathtt{LM}(f)$, entonces el S-polinomio es particularmente simple,

$$S(f, g) = f - \frac{\mathtt{LC}(f)}{\mathtt{LC}(g)} \cdot x^{\alpha-\beta} g$$

y $\mathtt{LM}(S(f, g)) < \mathtt{LM}(f)$

Ejemplo 5.5. Sea $f = x^3y^2 - x^2y^3$ y $g = 3x^4y + y^2$ en $\mathbb{R}[x, y]$ con el orden *Dp*. Entonces $\gamma = (4, 2)$ y

$$\begin{aligned} \mathtt{spoly}(f, g) =& \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ =& x \cdot f - (1/3) \cdot y \cdot g \\ =& -x^3y^3 + x^2 - (1/3)y^3 \end{aligned}$$

Un S-polinomio $\texttt{spoly}(f, g)$ está diseñado para producir la cancelación de los términos principales, de hecho el siguiente lema muestra que cada cancelación de términos principales entre polinomios del mismo exponente principal resulta de este tipo de cancelación.

Lema 5.6. Supongamos que tenemos una suma $\sum_{i=1}^{s} c_i f_i$, donde $c_i \in K$ y $\texttt{LE}(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$, $\forall i$. Si $\texttt{LE}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, entonces $\sum_{i=1}^{s} c_i f_i$ es una combinación lineal con coeficientes en K, de los S-polinomios $\texttt{spoly}(f_j, f_k)$ para $1 \leq j, k \leq s$. Además, cada $\texttt{spoly}(f_i, f_k)$ tiene exponente principal $< \delta$.

Demostración. Sea $d_i = \texttt{LC}(f_i)$, tal que $c_i d_i$ es el coeficiente principal de $c_i f_i$. Ya que $c_i f_i$ tiene exponente principal δ y su suma tiene un exponente principal más pequeño se deduce que $\sum_{i=1}^{s} c_i d_i = 0$.
Definimos $p_i := f_i/d_i$, y notar que p_i tiene coeficiente principal 1. Consideremos la suma telescópica

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i =& \sum_{i=1}^{s} c_i d_i p_i \\ =& c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \\ & (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s\end{aligned}$$

Ahora como $\texttt{LC}(f_i) = d_i$ y además $\texttt{LE}(f_i) = \delta$ tenemos $\texttt{LT}(f_i) = d_i x^\delta$, por lo que el mínimo común múltiplo de $\texttt{LM}(f_j)$ y $\texttt{LM}(f_k)$ es x^δ. Así

$$\texttt{spoly}(f_j, f_k) = \frac{x^\delta}{\texttt{LT}(f_j)} f_j - \frac{x^\delta}{\texttt{LT}(f_k)} f_k = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k = p_j - p_k \tag{2}$$

Utilizando esta ecuación y $\sum_{i=1}^{s} c_i d_i = 0$, la anterior suma telescópica se convierte en:

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i =& c_1 d_1 \texttt{spoly}(f_1, f_2) + (c_1 d_1 + c_2 d_2)\texttt{spoly}(f_2, f_3) \\ & + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})\texttt{spoly}(f_{s-1}, f_s)\end{aligned}$$

la cual es una suma de la forma deseada. Ya que p_j y p_k tienen exponente principal δ y coeficiente principal 1, la diferencia $p_j - p_k$ tiene exponente principal menor que δ (respecto al orden monomial $>$).
Por la ecuación (2), lo mismo se aplica a $\texttt{spoly}(f_j, f_k)$, y se demuestra el lema. □

Cuando $f_1, \ldots, f_s$ satisface la hipótesis de Lema 5.6, obtenemos una ecuación de la forma

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{jk} \texttt{spoly}(f_j, f_k).$$

Consideremos dónde ocurre la cancelación. En la suma de la izquierda, cada sumatorio $c_i f_i$ tiene exponente principal δ, por lo que la cancelación ocurre hasta después de sumarlos. Sin embargo, en la suma de la derecha, cada sumando $c_{jk}\texttt{spoly}(f_j, f_k)$ tiene exponente principal menor que δ, por lo que la cancelación ya se ha producido. Intuitivamente esto significa que todas las cancelaciones pueden ser contadas por los S-polinomios.

Teorema 5.7. Criterio de Buchberger. Sea I un ideal polinomial. Entonces una base $G = \{g_1, \ldots, g_t\}$ para I es una base de Gröbner para I si y solo si para todos los pares $i \neq j$, el residuo en la división de $\texttt{spoly}(g_i, g_j)$ por G (enumerados en algún orden) es cero.

Demostración.
$\Rightarrow$: Si G es una base de Gröbner, entonces $\texttt{spoly}(g_i, g_j) \in I$, y el resto de la división por G es cero por corolario 5.2.
$\Leftarrow$: Sea $f \in I$ un polinomio distinto de cero, debemos probar que si los S-polinomios tienen residuo cero en la división por G, entonces $\texttt{LT}(f) \in \langle \texttt{LT}(g_1), \ldots, \texttt{LT}(g_t) \rangle$. Antes de conocer los detalles de la prueba, se describirá la estrategia de la prueba.
Dado $f \in I = \langle g_1, \ldots, g_t \rangle$, existen polinomios $h_i \in K[x_1, \ldots, x_n]$ tal que

$$f = \sum_{i=1}^{t} h_i g_i \tag{1}$$

Por Lema 1.9, se sigue que

$$\texttt{LE}(f) \leq \text{máx}(\texttt{LE}(h_i g_i)) \tag{2}$$

si la igualdad no ocurre debe ocurrir alguna cancelación entre los términos en (1). El Lema 5.6 nos permitirá reescribir esto en términos de S-polinomios. Entonces, nuestra suposición de que los S-polinomios tienen residuos cero nos permitirá reemplazar los S-polinomios por expresiones que impliquen menos cancelaciones. Por lo tanto obtendremos una expresión para f que tenga menos cancelaciones de los términos principales. Continuando de esta manera, eventualmente se encontrará una expresión (1) para f donde la igualdad ocurre en (2). Entonces $\texttt{LE}(f) = \texttt{LE}(h_i g_i)$ para algún i, y se seguirá que $\texttt{LT}(f)$ es divisible por $\texttt{LT}(g_i)$. Esto mostrará que $\texttt{LT}(f) \in \langle \texttt{LT}(g_1), \ldots, \texttt{LT}(g_t) \rangle$, que es lo que se desea probar.

Ahora se darán los detalles de la prueba. Dada una expresión (1) para f, sea $m(i) = \texttt{LE}(h_i g_i)$, y definimos $\delta = \text{máx}(m(1), \ldots, m(t))$. Entonces la desigualdad (2) se convierte en $\texttt{LE}(f) \leq \delta$. Ahora consideremos todas las formas posibles en que f se puede escribir en la forma de (1). Para cada expresión, obtenemos un δ posiblemente diferente. Como

un orden monomial es un buen orden, podemos seleccionar una expresión (1) para f tal que δ es el mínimo.

Mostraremos que una vez que se elige este mínimo δ tenemos $\mathtt{LE}(f) = \delta$. Entonces la igualdad ocurre en (2), y como observamos, se sigue que $\mathtt{LT}(f) \in \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. Esto probaría el teorema.
Queda por mostrar que $\mathtt{LE}(f) = \delta$. La prueba se realizará por contradicción.
La igualdad solo puede fallar cuando $\mathtt{LE}(f) < \delta$. Para aislar los términos de exponente principal δ, escribiremos f de la siguiente manera:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathtt{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \end{aligned} \tag{3}$$

Los monomios que aparecen en la segunda y tercera suma de (3) tienen grado $< \delta$. Por lo tanto la suposición $\mathtt{LE}(f) < g$ significa que la primera suma también tiene exponente principal $< \delta$.

Sea $\mathtt{LT}(h_i) = c_i x^{\alpha(i)}$. Entonces la primera suma $\sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha_i} g_i$ tiene exactamente la forma descrita en Lema 5.6 con $f_i = x^{\alpha(i)} g_i$. Entonces por Lema 5.6 implica que esta suma es una combinación lineal de S-polinomios $\mathtt{spoly}(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$. Sin embargo

$$\begin{aligned} \mathtt{spoly}(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) =& \frac{x^\delta}{x^{\alpha(j)} \mathtt{LT}(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)} \mathtt{LT}(g_k)} x^{\alpha(k)} g_k \\ =& x^{\delta - \gamma_{jk}} \mathtt{spoly}(g_j, g_k) \end{aligned}$$

donde $x^{\delta - \gamma_{jk}} = \mathtt{lcm}(\mathtt{LM}(g_j), \mathtt{LM}(g_k))$. Por lo tanto existen constantes $c_{jk} \in K$ tal que

$$\sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} \mathtt{spoly}(g_j, g_k) \tag{4}$$

El siguiente paso es usar nuestra hipótesis de que el resto de $\mathtt{spoly}(g_j, g_k)$ en la división por $g_1, \ldots, g_t$ es cero. Usando el algoritmo de la división, esto significa que el S-polinomio se puede escribir de la forma

$$\mathtt{spoly}(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i \tag{5}$$

donde $a_{ijk} \in K[x_1, \ldots, x_n]$. El algoritmo de la división también nos dice que

$$\mathtt{LE}(a_{ijk} g_i) \leq \mathtt{LE}(\mathtt{spoly}(g_j, g_k)) \tag{6}$$

para todo i, j, k. Intuitivamente, esto dice que cuando el resto es cero, podemos encontrar una expresión para $\texttt{spoly}(g_j, g_k)$ en términos de G donde los términos principales no se cancelan todos.
Para aprovechar esto, multiplicamos la expresión por $\texttt{spoly}(g_j, g_k)$ por $x^{\delta-\gamma_{jk}}$ para obtener

$$x^{\delta-\gamma_{jk}}\texttt{spoly}(g_j, g_k) = \sum_{i=1}^{t} b_{ijk}g_i$$

donde $b_{ijk} = x^{\delta-\gamma_{jk}}a_{ijk}$. Entonces (6) y lema 5.6 implican que

$$\texttt{LE}(b_{ijk}g_i) \leq \texttt{LE}(x^{\delta-\gamma_{jk}}\texttt{spoly}(g_j, g_k)) < \delta \tag{7}$$

Si sustituimos la expresión anterior por $x^{\delta-\gamma_{jk}}\texttt{spoly}(g_j, g_k)$ en (4), obtenemos la ecuación

$$\sum_{m(i)=\delta} \texttt{LT}(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}\texttt{spoly}(g_j, g_k) = \sum_{j,k} c_{jk}\left(\sum_i b_{ijk}g_i\right) = \sum_i \tilde{h}_i g_i$$

que por (7) tiene la propiedad que para todo i

$$\texttt{LE}(\tilde{h}_i g_i) < \delta$$

Para el paso final de la prueba, sustituimos $\sum_{m(i)=\delta} \texttt{LT}(h_i)g_i = \sum_i \tilde{h}_i g_i$ en la ecuación (3) para obtener una expresión para f que es una combinación de los g_i, donde todos los términos tienen exponente principal $< \delta$. Esto contradice la minimalidad de δ y completa la prueba de teorema.

□

CAPÍTULO 2: Bases estándar

En este capítulo se trabajará con ordenes monomiales locales, y se mostrará que con este tipo de órdenes, el algoritmo de la división fracasa en la obtención de una base de Gröbner, y por lo tanto es necesario aplicar nuevas estrategias y algoritmos, para el cálculo de un conjunto generador finito para un ideal.

6. Anillos locales y localización

La localización es una técnica muy utilizada en álgebra conmutativa, que permite reducir preguntas sobre los anillos a una unión de problemas "locales" más pequeños. De manera general la localización de un anillo significa agrandar el anillo al permitir denominadores. La idea algebraica de la localización es entonces, hacer invertibles más (o incluso todos) los elementos diferentes de cero introduciendo fracciones, de la misma manera que se pasa de los números enteros $\mathbb{Z}$ a los números racionales $\mathbb{Q}$.

Definición 6.1. Un anillo K se dice que es *local*, si tiene exactamente un ideal maximal $\mathfrak{m}$. Además $K/\mathfrak{m}$ se llama el *campo de residuos* de K. También se pueden denotar los anillos locales por $(K, \mathfrak{m})$ o $(K, \mathfrak{m}, H)$ donde $H = K/\mathfrak{m}$.

Los campos son anillos locales. Un anillo polinomial $K[x_1, \ldots, x_n]$ con $n \geq 1$ sobre un campo K, sin embargo, nunca es local. Para ver esto, considerar para cualquier $(a_1, \ldots, a_n) \in K^n$ el ideal $\mathfrak{m}_a := \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Ya que $\varphi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$, $\varphi(x_i) := x_i - a_i$ es un isomorfismo que envía $\mathfrak{m}_0 = \langle x_1, \ldots, x_n \rangle$ a $\mathfrak{m}_a$, resulta que $K[x_1, \ldots, x_n]/\mathfrak{m}_a \cong K$ es un campo, por lo tanto $\mathfrak{m}_a$ es un ideal maximal. Como K tiene al menos dos elementos, K^n tiene al menos dos puntos diferentes y por lo tanto $K[x_1, \ldots, x_n]$ tiene al menos tantos ideales maximales como puntos K^n (los del tipo $\mathfrak{m}_a$).

Si K es algebraicamente cerrado, entonces los ideales $\mathfrak{m}_a$, $a \in K^n$ son todos ideales maximales de $K[x_1, \ldots, x_n]$.

Teorema 6.2. Todo anillo $A \neq 0$ contiene al menos un ideal maximal. Si $I \subsetneq A$ es un ideal, entonces existe un ideal maximal $\mathfrak{m} \subset A$ tal que $I \subset \mathfrak{m}$.

Demostración. Observar que la primera afirmación se sigue de la segunda con $I = 0$. Si I no es maximal, existe un $f_1 \in A$ tal que $I \subsetneq I_1 := \langle I, f_1 \rangle \subsetneq A$. Si I_1 no es

maximal, existe un f_2 tal que $I_1 \subsetneq I_2 = \langle I_1, f_2 \rangle \subsetneq A$. Continuando de esta manera, obtenemos una secuencia de ideales estrictamente crecientes $I \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$ que debe volverse estacionaria, digamos $I_m = I_n$ para $m \geq n$ y A es Noetheriano, según la Observación 4.10. Por lo tanto, I_n es maximal y contiene al ideal I. □

Lema 6.3. Sea A un anillo.

i) A es un anillo local si y solo si el conjunto de no-unidades es un ideal (que es entonces el ideal maximal).

ii) Sea $\mathfrak{m} \subset A$ un ideal maximal tal que cada elemento de la forma $1 + a$, $a \in \mathfrak{m}$ es unidad. Entonces A es local.

Demostración.

i) $\Rightarrow$: Si A es un anillo local entonces el conjunto de no-unidades es un ideal.
Sabemos que A es un anillo local, sea $\mathfrak{m}$ el único ideal maximal de A y sea I el conjunto de no-unidades de A.
Sean $a, b \in I$ elementos no-unidad, los ideales $\langle a \rangle$ y $\langle b \rangle$ son ideales propios de A. Como $\mathfrak{m}$ es el único ideal maximal de A, se sigue que $\langle a \rangle \subset \mathfrak{m}$ y $\langle b \rangle \subset \mathfrak{m}$. Por lo que $a - b \in \mathfrak{m}$, ya que $a, b \in \mathfrak{m}$ y $\mathfrak{m}$ es un ideal. Como $\mathfrak{m}$ es un ideal propio de A, $a - b \in I$.
También para cualquier $r \in A$ tenemos $ra \in \mathfrak{m}$, ya que $a \in \mathfrak{m}$ y $\mathfrak{m}$ es un ideal de A. Se sigue que ra es una no-unidad, ya que $\mathfrak{m}$ es un ideal propio. Así $ra \in I$. Además el conjunto I es un ideal de R.

$\Leftarrow$: Si el conjunto de no-unidades es un ideal entonces A es un anillo local.
Sea I el conjunto de no unidades en A, un ideal de A. Como $a \in A$ es una unidad, I es un ideal propio. Sea $\mathfrak{m}$ un ideal maximal arbitrario de A. Notar que cada elemento de $\mathfrak{m}$ es un elemento no-unidad de A, ya que $\mathfrak{m}$ es un ideal propio. Entonces tenemos $\mathfrak{m} \subset I$, ya que que $\mathfrak{m}$ es maximal se sigue que $\mathfrak{m} = I$

ii) Probaremos que el ideal maximal $\mathfrak{m}$ es el conjunto de elementos no-unidad de A, el resultado se sigue de A. Tomemos cualquier $u \in A/\mathfrak{m}$. entonces el ideal $\langle u, \mathfrak{m} \rangle$ generado por u y $\mathfrak{m}$ es estrictamente más grande que $\mathfrak{m}$ por lo tanto $\langle u, \mathfrak{m} \rangle = A$ por la maximilidad de $\mathfrak{m}$.
Entonces existe $v \in A$ y $a \in \mathfrak{m}$ tal que $1 = uv + a$, como $uv = 1 - a \in 1 + \mathfrak{m}$, se sigue de la suposición que uv es una unidad. Por lo tanto u es una unidad. Ya que $\mathfrak{m}$ contiene los elementos no-unidad, podemos observar que $\mathfrak{m}$ consiste de los elementos no-unidad de A. Entonces por I) se concluye que A es un anillo local.

□

Los anillos locales más comunes son los cuerpos, a continuación se introduce un procedimiento algebraico, llamado *localización*, que construye anillos locales a partir de un anillo.

La localización generaliza la construcción del campo de cociente: si A es un dominio entero, entonces el conjunto

$$\text{Quot}(A) := Q(A) := \left\{ \frac{a}{b} : \ a, b \in A, \ b \neq 0 \right\}$$

junto con las operaciones

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

es un campo, el cual es llamado *campo de cocientes* o *campo de fracciones* de A. Donde a/b denota la clase (a, b) bajo la relación de equivalencia

$$(a, b) \sim (a', b') :\Longleftrightarrow ab' = a'b$$

El mapeo $\phi : A \to Q(A)$, tal que $a \longmapsto a/1$ es un homomorfismo de anillo inyectivo e identificamos A con su imagen. Ya que $a/b = 0$ si y solo si $a = 0$, cada elemento $a/b \neq 0$ tiene un inverso b/a y además $Q(A)$ es un campo.

Observar que los denominadores en $Q(A)$ son los elementos del conjunto $S = A \setminus \{0\}$, además S cumple que $1 \in S$ y es cerrado bajo el producto. Esta noción se puede generalizar de la siguiente manera.

Definición 6.4. Sea A un anillo.

i) Un subconjunto $S \subset A$ es llamado *multiplicativo* o *multiplicativamente cerrado* si cumple:

   a) $1 \in S$ y $0 \notin S$

   b) $a \in S$ y $b \in S \ \Rightarrow \ ab \in S$

ii) Sea $S \subset A$ multiplicativamente cerrado. Definimos la *localización* o el *anillo de fracciones* $S^{-1}A$ del anillo A con respecto a S de la siguiente manera:

$$S^{-1}A := \left\{ \frac{a}{b} : \ a \in A, \ b \in S \right\}$$

donde a/b denota la clase de equivalencia del par $(a, b) \in A \times S$ con respecto a la siguiente relación de equivalencia:

$$(a, b) \sim (a', b') :\Longleftrightarrow \exists s \in S \ \text{ tal que } \ s(ab' - a'b) = 0$$

Además, en $S^{-1}A$ definimos una suma y producto como en el caso del campo de cocientes.

Proposición 6.5.

I) Las operaciones + y $\cdot$ en $S^{-1}A$ están bien definidas, por lo que $S^{-1}A$ es un anillo (conmutativo y con unidad $1 = 1/1$).

II) El mapeo $j : A \to S^{-1}A$, $a \longmapsto a/1$ es un homomorfismo de anillos que satisface:

a) $j(s)$ es una unidad en $S^{-1}A$ si $s \in S$.

b) $j(a) = 0$ si y solo si $as = 0$ para algún $s \in S$.

c) j es inyectivo si y solo si S consiste de no-divisores de cero.

d) j es biyectivo si y solo si S consiste de unidades.

III) $S^{-1}A = 0$ si y solo si $0 \in S$.

IV) Si $S_1 \subset S_2$ son multiplicativamente cerrados en A y consiste de no-divisores de cero, entonces $S_1^{-1}A \subset S_2^{-1}A$.

Demostración.

I) Probemos que las operaciones están bien definidas y además definen una estructura de anillo en $S^{-1}A = A \times S/\sim$. Si $(a, s) \sim (a'', s'')$ entonces existe $u \in S$ tal que $u(as'' - a''s) = 0$ por lo tanto

$$u((as' + a's)(s^{''}s') - (a^{''}s' + a's'')(ss')) = (s')^2 \cdot u(as^{''} - a^{''}s) = 0$$

$$u((aa')(s^{''}s') - (a^{''}a')(ss')) = a's' \cdot u(as^{''} - a^{''}s) = 0$$

y entonces $\dfrac{as' + a's}{ss'} = \dfrac{a^{''}s' + a's^{''}}{s^{''}s'}$ y $\dfrac{aa'}{ss'} = \dfrac{a^{''}a'}{s^{''}s'}$

II) a) Sea $s \in S$ entonces $j(s) = s/1$. Como $s/1 = 0$ si y solo si $\exists s_1 \in S$ tal que $s_1 s = 0$. Como $s_1, s \in S$ entonces $s_1 s \in S$ y además $0 \notin S$ por lo que $s_1 s$ es invertible y por lo tanto $j(s)$ es una unidad.

b) Por la definición de relación de equivalencia que se ha definido.

c) Si $x/1 = 0$, entonces hay una $u \in S$ tal que $xu = 0$ en A y, por lo tanto, $x = 0$, ya que no hay divisores de cero en S.

d) Si j es biyectivo, entonces S consiste solo de unidades, ya que $j(s)$ es una unidad para todo $s \in S$.

III) Si $0 \in S$ cualquier par $(a, s) \sim (0, 1)$ por definición. Si $0 \notin S$ es claro que $1/1 \neq 0/1$ en $S^{-1}A$.

IV) Sea $\dfrac{a}{b} \in S_1^{-1}A$, entonces $a, b \in A$ y $b \in S_1$; como $S_1 \subset S_2$ entonces $b \in S_2$, así $\dfrac{a}{b} \in S_2^{-1}A$.

□

Ejemplo 6.6. Sea A un anillo y $P \subset A$ un ideal primo, entonces $A \setminus P$ es un conjunto multiplicativamente cerrado, en efecto $0 \in P$ y $1 \notin P$, así $0 \notin A \setminus P$ y $1 \in A \setminus P$. Además si $a, b \in A \setminus P$ entonces $ab \in A \setminus P$, supongamos que $ab \notin A \setminus P$ entonces $ab \in P$, como P es un ideal primo $a \in P$ o $b \in P$. Por hipótesis $a, b \in A \setminus P$, entonces $a \notin P$ y $b \notin P$,lo cual es una contradicción, por lo tanto $ab \in A \setminus P$.

La localización del anillo A con respecto a $A \setminus P$ es denotado por A_P y

$$A_P = \left\{ \frac{a}{b} : \ a, b \in A, \ b \notin P \right\}$$

es llamada la localización de A con respecto al ideal primo P.
El conjunto

$$PA_P = \left\{ \frac{a}{b} : \ a \in P, \ b \notin P \right\}$$

es un ideal en A_P. Cualquier elemento $a/b \in A_P \setminus PA_P$ cumple que $a \notin P$, por lo tanto, $b/a \in A_P$ y, además, a/b es una unidad. Esto muestra que A_P es un anillo local con PA_P ideal maximal según el Lema 6.3. En particular, si $\mathfrak{m} \subset A$ es un ideal maximal, entonces $A_{\mathfrak{m}}$ es local con el ideal maximal $\mathfrak{m}A_{\mathfrak{m}}$.

El conjunto S de todos los no-divisores de cero de A es multiplicativamente cerrado. Para esto S, $S^{-1}A =: Q(A) =: \mathrm{Quot}(A)$ se llama el *anillo total de fracciones* o *el anillo total de cocientes* de A. Si A es un dominio entero, este es solo el *campo de cocientes* de A. Dos casos especiales pero importantes son los siguientes: si $K[x_1, \ldots, x_n]$ es el anillo de polinomios sobre un campo K, luego el campo de cocientes se denota por $K(x_1, \ldots, x_n)$,

$$K(x_1, \ldots, x_n) := Q(K[x_1, \ldots, x_n])$$

que también se llama el *campo de funciones* en n variables; los x_i también se llaman *parámetros*. La localización de $K[x] = K[x_1, \ldots, x_n]$ con respecto al ideal maximal $\langle x \rangle = \langle x_1, \ldots, x_n \rangle$ es

$$K[x]_{\langle x \rangle} = \left\{ \frac{f}{g} : \ f, g \in K[x], \ g(0) \neq 0 \right\}$$

Un hecho importante es que podemos calcular en este anillo sin denominadores explícitos, simplemente definiendo un orden monomial adecuado en $K[x_1, \ldots, x_n]$. De manera más general, podemos calcular en $K[x]_{\mathfrak{m}_a}$, $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, para cualquier $a = (a_1, \ldots, a_n) \in K^n$, trasladando nuestros datos polinomiales a $K[x]_{\langle x \rangle}$ a través del mapeo de anillos $x_i \longmapsto x_i + a_i$.

Lema 6.7. Sea $S \subset A$ multiplicativamente cerrado y $j : A \to S^{-1}A$ el homomorfismo canónico de anillos $a \mapsto a/1$.

I) Si $J \subset S^{-1}A$ es un ideal y $I = j^{-1}(J)$ entonces $IS^{-1}A = J$. En particular, si $f_1, \ldots, f_k$ genera I sobre A entonces $f_1, \ldots, f_k$ genera J sobre $S^{-1}A$.

II) Si A es Noetheriano, entonces $S^{-1}A$ es Noetheriano.

Demostración.

I) $\Rightarrow$: Probemos que $J \subset IS^{-1}A$, sea $f/s \in J$ entonces $f/1 = s \cdot f/s$, como J es un ideal y $s \in S^{-1}A$, entonces $f/1 \in J$ y por tanto $f \in j^{-1}(J) = I$. Además $f/s = f \cdot 1/s$, $f \in I$ y $1/s \in S^{-1}A$, por lo tanto $f/s \in IS^{-1}A$.

$\Leftarrow$: Probemos que $IS^{-1}A \subset J$, sea $g \in IS^{-1}A$ entonces $g = fh$, donde $f \in I$ y $h \in S^{-1}A$; como $f \in I$ entonces $f/1 \in J$. Así $g = f/1 \cdot h = f \cdot h/1$ como J es un ideal entonces $g \in J$.

II) Como el anillo A es Noetheriano, sus ideales son finitamente generados. Por I), $S^{-1}A$ también es Noetheriano.

□

7. Anillos asociados a órdenes monomiales

En esta sección se mostrará que los ordenamientos monomiales no globales conducen a nuevos anillos que son localizaciones del anillo de polinomios. Este hecho tiene consecuencias computacionales de largo alcance. Por ejemplo, al elegir un ordenamiento local, básicamente podemos hacer los mismos cálculos en la localización de un anillo de polinomios que con un orden global en el propio anillo polinómico. En particular, podemos calcular de manera efectiva en $K[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_k \rangle}$ para $k \leq n$.

Sea $>$ un orden monomial en el conjunto de monomios $\texttt{Mon}(x_1, \ldots, x_n) = \{x^\alpha : \alpha \in \mathbb{Z}^n_{\geq 0}\}$, y $K[x] = K[x_1, \ldots, x_n]$ el anillo polinomial en n variables sobre un campo K. Entonces, la función del monomio principal $\texttt{LM}$ tiene las siguientes propiedades para cualesquiera de los polinomios $f, g \in K[x] \setminus \{0\}$:

I) $\texttt{LM}(gf) = \texttt{LM}(g)\texttt{LM}(f)$

II) $\texttt{LM}(g+f) \leq \text{máx}\{\texttt{LM}(g), \texttt{LM}(f)\}$ con la igualdad si y solo si los términos principales de f y g no se cancelan.

En particular se sigue que

$$S_> := \{u \in K[x] \setminus \{0\} : \texttt{LM}(u) = 1\}$$

es multiplicativamente cerrado, en efecto puesto que $0 \notin S_>$, $1 \in S_>$ y $\forall u, v \in S_>$ cumplen $\texttt{LM}(u) = \texttt{LM}(v) = 1$, así $\texttt{LM}(uv) = \texttt{LM}(u)\texttt{LM}(v) = 1$ y por lo tanto $uv \in S_>$.

Definición 7.1. Para cualquier orden monomial $>$ en $\texttt{Mon}(x_1, \ldots, x_n)$, se define

$$K[x]_> := S_>^{-1}K[x] = \left\{ \frac{f}{u} : f, u \in K[x], \texttt{LM}(u) = 1 \right\}$$

la localización de $K[x]$ con respecto al conjunto multiplicativamente cerrado $S_>$, además $K[x]_>$ es llamado el anillo asociado a $K[x]$ y al orden monomial $>$.

Observación 7.2. Notar que $S_> = K^*$ (unidades del campo) si y solo si $>$ es un orden global y $S_> = K[x] \setminus \langle x_1, \ldots, x_n \rangle$ si y solo si $>$ es un orden local.

Lema 7.3. Sea K un campo, $K[x] = K[x_1, \ldots, x_n]$ y sea $>$ un orden monomial en $\mathtt{Mon}(x_1, \ldots, x_n)$. Entonces

I) $K[x] \subset K[x]_> \subset K[x]_{\langle x \rangle}$.

II) El conjunto de unidades en $K[x]_>$ está dado por

$$(K[x]_>)^* = \left\{ \frac{v}{u} : \ u, v \in K[x], \ \mathtt{LM}(v) = \mathtt{LM}(u) = 1 \right\}$$

y satisface $(K[x]_>)^* \cap K[x] = S_>$.

III) $K[x] = K[x]_>$ si y solo si $>$ es un orden global y $K[x]_> = K[x]_{\langle x \rangle}$ si y solo si $>$ es un orden local.

IV) $K[x]_>$ es un anillo Noetheriano.

Demostración.

I) Probemos que $K[x] \subset K[x]_>$. Definimos un homomorfismo de inclusión de la siguiente manera:

$$\begin{aligned} \phi : K[x] &\to K[x]_> \\ f &\mapsto f/1 \end{aligned}$$

Para todo $f/1$ es cero si y solo si $f = 0$. Implica que $\ker(\phi) = 0$. Por lo tanto ϕ es inyectivo, así $K[x] \subset K[x]_>$.
Probemos que $K[x]_> \subset K[x]_{\langle x \rangle}$. Definimos un homomorfismo de inclusión de la siguiente manera:

$$\begin{aligned} \phi : K[x]_> &\to K[x]_{\langle x \rangle} \\ f/u &\mapsto f/u \end{aligned}$$

Para todo f/u es cero si y solo si $f = 0$. Implica que $\ker(\phi) = 0$. Por lo tanto ϕ es inyectivo, así $K[x]_> \subset K[x]_{\langle x \rangle}$.

II) Si f/u es una unidad de $K[x]_>$, entonces existe un $h/v \in K[x]_>$ tal que $(f/u) \cdot (h/v) = 1$. Por lo tanto, $fh = uv$ y $\mathtt{LM}(fh) = \mathtt{LM}(uv) \Longrightarrow \mathtt{LM}(f)\mathtt{LM}(h) = 1$, lo que implica que $\mathtt{LM}(f) = 1$.

Probemos que $(K[x]_>)^* \cap K[x] = S_>$, sea $f \in (K[x]_>)^* \cap K[x]$,

$$\begin{aligned}
&\iff f \in (K[x]_>)^* \text{ y } f \in K[x] \\
&\iff f = u/v, \text{ tal que } \mathtt{LM}(u) = \mathtt{LM}(v) = 1 \text{ y } f \in K[x] \\
&\iff v \in K^* \text{ y } \mathtt{LM}(f) = \mathtt{LM}(u) = 1 \text{ y } f \in K[x] - \{0\} \\
&\iff f \in S_>
\end{aligned}$$

III) Probemos que $K[x]_> = K[x]$ si y solo si $>$ es global. Sea $>$ un orden global y $f/u \in K[x]_> = \{f/u : \ f, u \in K[x] \text{ y } u \in S_>\}$, como $>$ es global entonces $S_> = K^*$ si y solo si $u \in K^*$ y $f/u \in K[x]$. Por lo tanto $K[x] = K[x]_>$.

Probemos que $K[x]_> = K[x]_{\langle x \rangle}$ si y solo si $>$ es local. Sea $>$ un orden local y $f/u \in K[x]_> = \{f/u : \ f, u \in K[x] \text{ y } u \in S_>\}$, como $>$ es global entonces $S_> = K[x] - \langle x \rangle$ si y solo si $u \in K[x] - \langle x \rangle$ es decir $u(0) \neq 0$ así $f/u \in K[x]_{\langle x \rangle}$. Por lo tanto $K[x]_> = K[x]_{\langle x \rangle}$.

IV) Consecuencia inmediata de Lema 6.7.

□

En los siguientes ejemplos se describen algunos anillos asociados a órdenes monomiales.

Ejemplo 7.4. Sea $K[x, y] = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ y consideremos el orden producto $>= (>_1, >_2)$ en $\mathtt{Mon}(x_1, \ldots, x_n, y_1, \ldots, y_m)$, donde $>_1$ es global en $\mathtt{Mon}(x_1, \ldots, x_n)$ y $>_2$ es local en $\mathtt{Mon}(y_1, \ldots, y_m)$.

Por definición de bloques ordenados $>= (>_1, >_2)$, para establecer el orden de dos monomios primero comparamos las variables x_i, $i = 1, \ldots, n$ con el orden monomial $>_1$, en caso de ser igual comparamos las variables y_j, $j = 1, \ldots, m$ con el orden monomial $>_2$. Para todo monomio $x^\alpha y^\beta \in \mathtt{Mon}(x, y)$ tal que $\alpha \neq 0$ se tiene que $x^\alpha >_1 1$ ($>_1$ es global), por lo tanto para todo γ, $x^\alpha y^\gamma > 1$. Si $\alpha = 0$ entonces por definición de bloques ordenados tomamos $>_2$ en $\mathtt{Mon}(y_1, \ldots, y_m)$ por lo tanto $1 > y^\beta$ ($>_2$ es local), para todo $\beta \neq 0$. Se tiene que

$$x^\alpha y^\gamma > 1 > y^\beta \text{ para todo } \alpha, \beta \neq 0, \text{ para todo } \gamma$$

y por lo tanto $S_> = \{u \in K[x, y] - \{0\} : \mathtt{LM}(u) = 1\} = K^* + \langle y \rangle \cdot K[y]$, por lo anterior es un elemento de las unidades del campo más un polinomio en las variables $y_1, \ldots, y_m$.

Sea $K[x, y]_>$ la localización de $K[x, y]$ con respecto al conjunto multiplicativamente cerrado $S_>$ y $f \in K[x, y]_>$ observemos que $f = \dfrac{P(x, y)}{u + yQ(y)}$, $P(x, y) \in K[x, y]$ y $u +$

$yQ(y) \in S_> = K^* + \langle y \rangle \cdot K[y]$. Por lo tanto los elementos de $K[x,y]_>$ son polinomios en las indeterminadas $x_1, \ldots, x_n$ con coeficientes en $K[y]_{\langle y \rangle}$

$$K[x,y]_> = (K[y]_{\langle y \rangle})[x]$$

Ejemplo 7.5. Sea $>_1$ un orden local y $>_2$ un orden global, $>= (>_1, >_2)$, si $\alpha \neq 0$ entonces $1 > x^\alpha y^\gamma$, ya que $>= (>_1, >_2)$ entonces $1 > x^\alpha y^\beta$ si y solo si $1 >_1 x^\alpha$ (lo cual se cumple ya que $>_1$ es local). Si $\alpha = 0$ entonces $y^\beta > 1$, ya que $>= (>_1, >_2)$ entonces $y^\beta > 1$ si y solo si $y^\beta >_2 1$ (lo cual se cumple ya que $>_2$ es global). Por lo tanto

$$x^\alpha y^\gamma < 1 < y^\beta \text{ para todo } \alpha, \beta \neq 0, \text{ y para todo } \gamma$$

así, $S_> = K^* + \langle x \rangle K[x,y]$. Se obtiene la inclusión estricta $(K[x]_{\langle x \rangle})[y] \subset K[x,y]_> \subset K[x,y]_{\langle x \rangle}$, ya que $1/(1+xy)$ está en el segundo anillo, pero no en el primero y $1/y$ está en el tercer anillo, pero no en el segundo anillo.

Ejemplo 7.6. Si $>_1$ es global, $>_2$ arbitrario y $>= (>_1, >_2)$ por el orden de bloques si $\alpha \neq 0$ entonces $x^\alpha y^\gamma > 1$ para todo γ. Si $\alpha = 0$ entonces y^β depende de $>_2$, por lo tanto $S_>$ consiste de los elementos $u \in K[y]$ que satisfacen $\mathtt{LM}_{>_2}(u) = 1$. Si $>_2$ es local entonces $S_> = K^* + \langle y \rangle K[y]$, es el caso del Ejemplo 7.4 Si $>_2$ es global entonces $S_> = K^*$.

$$K[x,y]_> = (K[y]_{>_2})[x]$$

Este ordenamiento tiene la siguiente propiedad de eliminación para $x_1, \ldots, x_n$:

$$f \in K[x,y],\ \mathtt{LM}(f) \in K[y] \Rightarrow f \in K[y]$$

Definición 7.7. Un orden monomial $>$ en $K[x_1, \ldots, x_n]$ tiene la propiedad de eliminación para $x_1, \ldots, x_s$ (véase el Ejemplo 7.6), se llama ordenamiento de eliminación para $x_1, \ldots, x_s$.

Un ordenamiento de eliminación no necesita ser un producto ordenado sino que debe satisfacer $x_i > 1$ para $i = 1, \ldots, s$ (ya que, si $x_i < 1$ entonces $\mathtt{LM}(1 + x_i)$=1 pero $1 + x_i \notin K[x_{s+1}, \ldots, x_n]$), es decir, un ordenamiento de eliminación para $x_1, \ldots, x_s$ debe ser global en $\mathtt{Mon}(x_1, \ldots, x_s)$.

Dado que el orden lexicográfico es un orden global y si $f \in K[x_1, \ldots, x_n]$ y $\mathtt{LM}(f) \in K[x_i, \ldots, x_n]$ entonces $f \in K[x_i, \ldots, x_n]$, es un ordenamiento de eliminación para $x_1, \ldots, x_i$, para $i = 1, \ldots, n$.
La siguiente definición permitirá caracterizar los polinomios de $K[x]_>$.

Definición 7.8. Sea $>$ cualquier orden monomial:

I) Para $f \in K[x]_>$ tomamos $u \in K[x]$ tal que $\mathtt{LT}(u) = 1$ y $uf \in K[x]$. Se define:

$$\mathtt{LM}(f) := \mathtt{LM}(uf)$$

$$\texttt{LC}(f) := \texttt{LC}(uf)$$
$$\texttt{LT}(f) := \texttt{LT}(uf)$$
$$\texttt{LE}(f) := \texttt{LE}(uf)$$
$$\texttt{tail}(f) := f - \texttt{LT}(uf)$$

II) Para cualquier subconjunto $G \subset K[x]_>$ se define el ideal

$$L_>(G) := L(G) := \langle \texttt{LM}(g) : \ g \in G \setminus \{0\} \rangle_{K[x]}$$

$L(G) \subset K[x]$ es llamado el *ideal principal* de G.

Observación 7.9.

I) La Definición 7.8 (numeral I), es independiente de la elección de u. Si el orden es global $u \in K^*$ y $\texttt{LT}(u) = 1$ entonces $u = 1$ y si el orden es local entonces $u \in K^* + \langle x \rangle \cdot K[x]$. Recordar que $\texttt{LM}(fg) = \texttt{LM}(f)\texttt{LM}(g)$, así $\texttt{LM}(uf) = \texttt{LM}(u)\texttt{LM}(f) = \texttt{LM}(f)$.

II) Ya que $K[x]_> \subset K[x]_{\langle x \rangle} \subset K[[x]]$, donde $K[[x]]$ denota el anillo de serie formal de potencias, $K[[x]] := \left\{ \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha : \ a_\alpha \in K, \alpha \in \mathbb{N}^n \right\}$, con la suma y producto dados por:

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha + \sum_{\alpha \in \mathbb{N}^n} b_\alpha x^\alpha := \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) x^\alpha$$

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \cdot \sum_{\alpha \in \mathbb{N}^n} b_\alpha x^\alpha := \sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\alpha + \beta} a_\alpha b_\beta \right) x^\gamma$$

Podemos considerar $f \in K[x]_>$ como una serie formal de potencias. De ello se desprende fácilmente que $\texttt{LM}(f)$, respectivamente $\texttt{LT}(f)$, corresponde a un monomio único, respectivamente un término, en la expansión de la serie de potencias de f.

III) Notar que si I es un ideal, entonces $L(I)$ es el ideal generado por todos los monomios principales de todos los elementos de I y no solo por los monomios principales de un conjunto dado de generadores de I. Ver Ejemplo 7.10 parte 2.

Ejemplo 7.10.

1. Consideremos $\mathbb{Q}[x]$ con un ordenamiento local (en una variable todos los ordenamientos locales respectivamente globales coinciden). Para $f = 3x/(1+x) + x$, por

la Definición 7.8, sea $u = 1 + x$ ($u \in K[x]$ y $\mathtt{LM}(u) = 1$), entonces $uf = 4x + x^2$ y por lo tanto

$$\begin{aligned} \mathtt{LE}(f) &= \mathtt{LE}(uf) = 1 \\ \mathtt{LM}(f) &= \mathtt{LM}(uf) = x \\ \mathtt{LC}(f) &= \mathtt{LC}(uf) = 4 \\ \mathtt{LT}(f) &= \mathtt{LT}(uf) = 4x \\ \mathtt{tail}(f) &= -3x^2/(1+x) \end{aligned}$$

2. Sea $G = \{f, g\}$ con $f = xy^2 + xy$, $g = x^2y + x^2 - y \in \mathbb{Q}[x, y]$ y ordenamiento monomial *dp*. Si $I = \langle f, g\rangle$ entonces $L(G) \subsetneq L(I)$, ya que

$$xf - yg = x(xy^2 + xy) - y(x^2y + x^2 - y) = y^2 \in I$$

Así $\mathtt{LM}(y^2) = y^2 \in L(I)$, pero $y^2 \notin L(G) = \langle xy^2, x^2y\rangle$.

8. Formas normales y bases estándar

En esta sección se definen las bases estándar de un ideal $I \subset K[x]_>$, como un conjunto de polinomios del ideal I, tal que sus monomios principales generan el ideal principal $L(I)$, para cualquier orden monomial, es decir que las bases de Gröbner son un caso particular cuando el orden es global.

Además en la siguiente sección se proporciona un algoritmo para calcular bases estándar. Para ordenamientos globales, este es el algoritmo de Buchberger. Para los órdenes locales, es el algoritmo del cono tangente de Mora, que a su vez es una variante del algoritmo de Buchberger. El caso general es una variación del algoritmo de Mora.

A continuación, se hace énfasis en caracterizar axiomáticamente las formas normales, respectivamente las formas normales débiles, que desempeñan un papel importante en el algoritmo de base estándar. Estas generalizan la división con resto al caso de ideales, respectivamente a conjuntos finitos de polinomios.

En el caso de un ordenamiento global, para cualquier polinomio f y cualquier ideal I, existe una forma normal única $\mathtt{NF}(f \mid I)$ de f con respecto a I, tal que ningún monomio de $\mathtt{NF}(f \mid I)$ está en el ideal principal $L(I)$. Esto se puede usar para decidir, por ejemplo, si f está en el ideal I (si la forma normal es 0).

En el caso general, la propiedad anterior resulta ser demasiado fuerte. Por lo tanto, los requisitos para una forma normal deben debilitarse. Por ejemplo, para la decisión de si un polinomio está en un ideal o no, solo el término principal de una forma normal $\mathtt{NF}(f \mid I)$ es importante. Por lo tanto, para este propósito, basta con requerir que $\mathtt{NF}(f \mid I)$ sea 0 o tenga un término principal, que no esté en $L(I)$. Después de debilitar los requisitos, ya no hay una declaración de exclusividad para la forma normal. Nuestra

intención es mantener la definición de una forma normal lo más general posible. Se presentará un algoritmo de forma normal y un algoritmo de base estándar general, que muestra que las diferentes versiones de algoritmos de base estándar se deben a diferentes formas normales.

Sea $>$ un orden monomial fijo y sea en esta sección

$$R = K[x_1, \ldots, x_n]_>$$

la localización de $K[x] = K[x_1, \ldots, x_n]$ con respecto al orden monomial $>$. Se debe tener en cuenta que $R = K[x]_> = S_>^{-1}K[x]$ con $S_> = \{u \in K[x] \setminus \{0\} : \mathtt{LM}(u) = 1\}$, además $R = K[x]$ si $>$ es global y $R = K[x]_{\langle x \rangle}$ si $>$ es local. En cualquier caso, R se puede considerar como un subanillo de $K[[x]]$.

Definición 8.1. Sea $I \subset R$ un ideal.

I) Un conjunto finito $G \subset R$ es llamado *base estándar* de I si

$$G \subset I \text{ y } L(I) = L(G)$$

Es decir, G es una base estándar, si los monomios principales de los elementos de G generan el ideal principal de I, o en otras palabras, si para cualquier polinomio $f \in I \setminus \{0\}$, existe un $g \in G$ que satisface $\mathtt{LM}(g) \mid \mathtt{LM}(f)$.

II) Si $>$ es un orden monomial global, la base estándar es llamada base de Gröbner, que se estudió en la Sección 3 del Capítulo 1.

III) Si simplemente decimos que G es una base estándar, queremos decir que G es una base estándar del ideal $\langle G \rangle_R$ generado por G.

Definición 8.2. Sea $G \subset R$ cualquier conjunto.

I) G es *reducido*, si $0 \notin G$ y si $\mathtt{LM}(g) \nmid \mathtt{LM}(f)$ para cualquier par de elementos $f \neq g$ en G. Una base estándar reducida G también se llama *minimal*.

II) $f \in R$ se dice que es *completamente reducido* con respecto a G, si no hay monomio de la expansión de serie de potencias de f que esté contenido en $L(G)$.

III) G es *completamente reducido*, si G es reducido y si para cualquier $g \in G$, $\mathtt{LC}(g) = 1$ y la $\mathtt{tail}(g)$ es completamente reducida con respecto a G.

Observación 8.3.

I) Si $>$ es un ordenamiento global, entonces cualquier conjunto finito $G = \{g_1, \ldots, g_s\}$ puede transformarse en un conjunto reducido. Si $g_i, g_j \in G$ tal que $\mathtt{LM}(g_i) \mid \mathtt{LM}(g_j)$, entonces sustituimos g_j por $g_j - mg_i$, donde $\mathtt{LT}(g_j) = m \cdot \mathtt{LT}(g_i)$, el generado por $\langle g_1 \ldots, g_j - mg_i, \ldots, g_s \rangle$ es igual a $\langle G \rangle = \langle g_1, \ldots, g_s \rangle$, en efecto puesto que $g_j - mg_i \in \langle G \rangle$ y $g_j = (g_j - mg_i) + (mg_i) \in \langle g_1 \ldots, g_j - mg_i, \ldots, g_s \rangle$. El resultado se llama *inter-reducción* de G; genera el mismo ideal que G.

II) Cada base estándar G puede transformarse en una base reducida simplemente eliminando elementos de G: eliminar ceros y luego, sucesivamente, cualquier g tal que $\mathtt{LM}(g)$ es divisible por $\mathtt{LM}(f)$ para algún $f \in G\backslash\{g\}$. El resultado es nuevamente una base estándar. Por lo tanto, G es una base reducida (G es minimal).

III) Supongamos que $G \subset R$ es un conjunto reducido y $g \in G$. Si $\mathtt{tail}(g)$ no se reduce con respecto a G, la expansión de la serie de potencias de $\mathtt{tail}(g)$ tiene un monomio que es divisible por $\mathtt{LM}(g)$ o por $\mathtt{LM}(f)$ para algún $f \in G \setminus \{g\}$. Si $>$ es global, entonces ningún monomio de $\mathtt{tail}(g)$ es divisible por $\mathtt{LM}(g)$, ya que $>$ refina el ordenamiento parcial natural en $\mathbb{N}^n$, es decir, la $\mathtt{tail}(g)$ se reduce con respecto a $\{g\}$.

IV) Se deduce que una base de Gröbner $G \subset K[x]$, que consiste de polinomios mónicos, es completamente reducida si para cualquier $f \neq g \in G$, $\mathtt{LM}(g)$ no divide ningún monomio de f.

Más adelante veremos que las bases de Gröbner reducidas siempre se pueden calcular y son únicas, pero las bases estándar reducidas no se pueden encontrar en general (en un número finito de pasos).

Las siguientes dos definiciones son cruciales para el tratamiento de las bases estándar.

Definición 8.4. Sea $\mathcal{G}$ el conjunto de todas las listas finitas $G \subset R$.

$$\begin{aligned} \mathtt{NF} : R \times \mathcal{G} &\to R, \\ (f, G) &\mapsto \mathtt{NF}(f \mid G) \end{aligned}$$

es llamado una *forma normal* en R si para todo $G \in \mathcal{G}$,

0) $\mathtt{NF}(0 \mid G) = 0$.

Y, para todo $f \in R$ y $G \in \mathcal{G}$,

1) $\mathtt{NF}(f \mid G) \neq 0 \;\Rightarrow\; \mathtt{LM}(\mathtt{NF}(f \mid G)) \notin L(G)$.

2) Si $G = \{g_1, \ldots, g_s\}$, entonces $f - \mathtt{NF}(f \mid G)$ (o por abuso de notación f) tiene una *representación estándar* con respecto a $\mathtt{NF}(- \mid G)$, es decir,

$$f - \mathtt{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i, \;\; a_i \in R, \;\; s \geq 0,$$

cumpliendo $\mathtt{LM}\left(\sum_{i=1}^{s} a_i g_i\right) \geq \mathtt{LM}(a_i g_i)$ para todo i tal que $a_i g_i \neq 0$ (es decir que no todos los monomios principales se anulan), $\mathtt{NF}$ es llamada la *forma normal reducida* si además $\mathtt{NF}(f \mid G)$ es reducida con respecto a G.

Definición 8.5.

I) Un mapeo $\mathtt{NF} : R \times \mathcal{G} \to R$, como en la Definición 8.4, es llamada la *forma normal débil* en R si cumple las condiciones 0) y 1) de la Definición 8.4 y en lugar de la condición 2) cumple:

2') Para todo $f \in R$ y $G \in \mathcal{G}$ existe una unidad $u \in R^*$ tal que uf tiene una representación estándar con respecto a $\mathtt{NF}(- \mid G)$.

II) Una forma normal débil $\mathtt{NF}$ es llamada *polinomial* si, siempre que $f \in K[x]$ y $G \subset K[x]$, exista una unidad $u \in R^* \cap K[x]$ tal que uf tenga una representación estándar con $a_i \in K[x]$.

Observación 8.6.

I) La noción de formas normales débiles solo es interesante para ordenamientos no globales, ya que para ordenamientos globales se tiene que $R = K[x]$ y por lo tanto $R^* = K^*$. Incluso en general, si existe una forma normal débil $\mathtt{NF}$, entonces, teóricamente, existe también una forma normal $\widetilde{\mathtt{NF}}$

$$(f, G) \mapsto \frac{1}{u}\mathtt{NF}(f \mid G) =: \widetilde{\mathtt{NF}}(f \mid G)$$

para una elección apropiada de $u \in R^*$ (dependiendo de f y G). Sin embargo, estamos realmente interesados en las formas normales polinomiales, y para los ordenamientos no globales $1/u$ no es en general un polinomio, sino una serie de potencias. Debemos tener en cuenta que $R^* \cap K[x] = S_>$.

II) Considerar $f = y$, $g = (y - x)(1 - y)$, y $G = \{g\}$ en $R = K[x, y]_{\langle x,y\rangle}$ con ordenamiento local *ls*. Asumir $h := \mathtt{NF}(f \mid G) \in K[x, y]$ es una forma normal polinomial de f con respecto a G. Ya que $f \notin \langle G\rangle_R = \langle y - x\rangle_R$, tenemos $h \neq 0$, por 1) de la Definición 8.4 se tiene $\mathtt{LM}(h) \notin L(G) = \langle y\rangle$ (es decir $\mathtt{LM}(h)$ es constante o tiene la variable x). Además $h - y = h - f \in \langle y - x\rangle_R$ ($h - f$ es una combinación de elementos de G) y además el $\mathtt{LM}(h)$ no se anula con $\mathtt{LM}(f)$, si h es una unidad entonces $h - f \notin \langle y - x\rangle_R$, lo que implica $\mathtt{LM}(h) < 1$. Por lo tanto, obtenemos $h = xh'$ para algún h' (debido al ordenamiento elegido *ls*). Además, $y - xh' \notin \langle (y-x)(1-y)\rangle_{K[x,y]}$ (sustituir $(0, 1)$ por (x, y)) y, por lo tanto, no existe una forma normal polinomial de (f, G). Por otro lado, estableciendo $u = (1-y)$ y $h = x(1-y)$ luego $uy - h = (y-x)(1-y)$ y, por lo tanto, h es una forma normal débil polinomial.

III) Para aplicaciones (débiles) las formas normales son más útiles si G es una base estándar de $\langle G\rangle_R$. Lo demostraremos con una primera aplicación en el Lema 8.7.

IV) $f = \sum_i a_i g_i$ es una representación estándar significa que no puede producirse la cancelación de los términos principales $> \mathtt{LM}(f)$ entre el $a_i g_i$ y que $\mathtt{LM}(f) = \mathtt{LM}(a_i g_i)$ para al menos un i.

V) No se hace una distinción estrictamente entre listas y conjuntos (ordenados). Dado que, en la definición de forma normal, permitimos repeticiones de elementos en G, necesitamos listas, es decir, secuencias de elementos, en lugar de conjuntos. Suponemos que un dado un conjunto G se ordena (de alguna manera) cuando aplicamos $\mathtt{NF}(- \mid G)$.

VI) La existencia de una forma normal respectivamente una forma normal débil polinomial con respecto a $G \subset K[x]$ que se probará en el algoritmo NFBuchberger respectivamente en el algoritmo NFMora nos dice:
Para cualquier $f \in R$ existen polinomios $u, a_1, \ldots, a_s \in K[x]$ tal que

$$uf = \sum_{i=1}^{s} a_i g_i + h,\ \mathtt{LM}(u) = 1,$$

y satisface:

a) Si $h \neq 0$ entonces $\mathtt{LM}(h)$ no es divisible por $\mathtt{LM}(g_i)$, $i = 1, \ldots, s$

b) $\mathtt{LM}\left(\sum_{i=1}^{s} a_i g_i\right) \geq \mathtt{LM}(a_i g_i)$ para todo i con $a_i g_i \neq 0$ (y por lo tanto, la igualdad es válida para al menos un i). Además, si $>$ es global, la unidad u puede elegirse como 1.

Por lo tanto, la existencia de una forma normal débil es un teorema de división donde f (respectivamente uf) se divide por $G = \{g_1, \ldots, g_s\}$ con la parte principal $\sum_{i=1}^{s} a_i g_i$ y resto $h = \mathtt{NF}(f \mid G)$.

Lema 8.7. Sea $I \subset R$ un ideal, $G \subset I$ una base estándar de I y $\mathtt{NF}(- \mid G)$ una forma normal débil en R con respecto a G.

I) Para cualquier $f \in R$ tenemos $f \in I$ si y solo si $\mathtt{NF}(f \mid G) = 0$.

II) Si $J \subset R$ es un ideal con $I \subset J$, entonces $L(I) = L(J)$ implica $I = J$.

III) $I = \langle G \rangle_R$, es decir, la base estándar G genera a I como $R-$ideal.

IV) Si $\mathtt{NF}(- \mid G)$ es una forma normal reducida, entonces es única.

Demostración.

I) Si $\mathtt{NF}(f \mid G) = 0$ entonces $uf \in I$, ya que u es una unidad de R y además I es un ideal, entonces $u^{-1}(uf) = f \in I$. Por contrarecíproca, si $\mathtt{NF}(f \mid G) \neq 0$, entonces por definición $\mathtt{LM}(\mathtt{NF}(f \mid G)) \notin L(G) = L(I)$, así $\mathtt{NF}(f \mid G) \notin I$, lo que implica $f \notin I$, ya que $\langle G \rangle_R \subset I$.

II) Sea $f \in J$ y asumamos que $\mathtt{NF}(f \mid G) \neq 0$, por definición de $\mathtt{NF}$ y del hecho que G es una base estándar para I se tiene que $\mathtt{LM}(\mathtt{NF}(f \mid G)) \notin L(G) = L(I) = L(J)$, contradiciendo $\mathtt{NF}(f \mid G) \in J$. Por lo tanto, $f \in I$ por I).

III) Por hipótesis $L(I) = L(G)$, y dado que $G \subset I$ por ser I ideal de R, entonces $\langle G \rangle_R \subset I$. Además $L(G) \subset L(\langle G \rangle_R)$.

Así se tiene que $L(I) = L(G) \subset L(\langle G \rangle_R) \subset L(I)$, de aquí se deduce que $L(I) = L(\langle G \rangle_R)$, luego por II) se sigue que $I = \langle G \rangle_R$, es decir, G genera a I como R-ideal.

IV) Sea $f \in R$ y asumir que h, h' son dos formas normales reducidas de f con respecto a G. Entonces, ningún monomio de la expansión de la serie de potencias de h o h' es divisible por cualquier monomio de $L(G)$ y, además, $h - h' = (f - h') - (f - h) \in \langle G \rangle_R = I$. Si $h - h' \neq 0$, entonces $\mathtt{LM}(h - h') \in L(I) = L(G)$, una contradicción, ya que $\mathtt{LM}(h - h')$ es un monomio ya sea de h o h'.

□

Observación 8.8. Las propiedades anteriores son bien conocidas para las bases de Gröbner con $R = K[x]$. Para ordenamientos locales, es muy importante trabajar rigurosamente con R en lugar de $K[x]$. A continuación se muestra un ejemplo donde ninguna de las propiedades I), II) y III) del Lema 8.7 se cumple para $K[x]$, si los datos de entrada son polinomiales.

Sea $f_1 := x^{10} - x^9y^2$, $f_2 := y^8 - x^2y^7$, $f_3 := x^{10}y^7$, y consideremos el orden local ds en $K[x, y]$. Entonces $R = K[x, y]_{\langle x,y \rangle}$, $(1 - xy)f_3 = y^7 f_1 + x^9 y f_2$, y establecemos

$$I := \langle f_1, f_2 \rangle_R = \langle f_1, f_2, f_3 \rangle_R, \qquad I' := \langle f_1, f_2 \rangle_{K[x,y]}, \qquad J' := \langle f_1, f_2, f_3 \rangle_{K[x,y]}$$

y $G := \{f_1, f_2\}$. Entonces G es una base estándar reducida de I (ya que debemos multiplicar f_1 al menos con y^8 y f_2 con x^{10} para producir nuevos monomios, pero $L(G) \supset \langle x, y \rangle$). Si $\mathtt{NF}(- \mid G)$ es cualquier forma normal débil en R, entonces $\mathtt{NF}(f_3 \mid G) = 0$, ya que $f_3 \in I$. Por lo tanto

I) $\mathtt{NF}(f_3 \mid G) = 0$, pero $f_3 \notin I'$,

II) $I' \subset J'$, $L(I') = L(J')$, pero $I' \neq J'$

III) $G \subset J'$, pero $\langle G \rangle_{K[x]} \neq J'$

Nos concentramos primero en los ordenamientos que cumplen con ser un buen orden, las bases Gröbner y el algoritmo de Buchberger. Para describir el algoritmo de forma normal de Buchberger, necesitamos la noción de un S-polinomio (Definición 5.4), debido a Buchberger.

Para el algoritmo de forma normal, el S-polinomio solo se usará en la segunda forma, mientras que para el algoritmo de base estándar lo necesitamos en la forma general.

Algoritmo $\texttt{NFBuchberger}(G \mid \texttt{NF})$

Sea $>$ un orden global.

Input: $f \in K[x], G \in \mathcal{G}$
Output: $h \in K[x]$, una forma normal de f con respecto a G.

$h := f$;
while ($h \neq 0$ y $G_h = \{g \in G : \texttt{LM}(g)$ divide $\texttt{LM}(h)\} \neq \emptyset$)
    Elegimos cualquier $g \in G_h$;
    $h := \texttt{spoly}(h, g)$;
return h;

Demostración. Probemos que el algoritmo termina, se inicia con $h_0 = f$, en el i-ésimo paso del ciclo While $h_{i-1} \neq 0$ y $G_{h_{i-1}} \neq \emptyset$ (caso contrario el algoritmo termina) y se crea el S-polinomio

$$h_i = h_{i-1} - m_i g_i, \qquad \texttt{LM}(h_{i-1}) > \texttt{LM}(h_i)$$

donde m_i es un término que cumple $\texttt{LT}(m_i g_i) = \texttt{LT}(h_{i-1})$ y $g_i \in G$ (permitiendo repeticiones). Dado que $>$ es un buen orden, $\{\texttt{LM}(h_i)\}$ tiene un mínimo, que se alcanza en algún paso m (por Lema 1.7), por lo tanto el algoritmo termina.

Mostremos que el algoritmo permite construir una forma normal para f:

$$\begin{aligned} h_1 &= f - m_1 g_1 \\ h_2 &= h_1 - m_2 g_2 = f - m_1 g_1 - m_2 g_2 \\ &\vdots \\ h_m &= f - \sum_{i=1}^{m} m_i g_i \end{aligned}$$

satisface que $\texttt{LM}(f) = \texttt{LM}(m_1 g_1) > \texttt{LM}(m_i g_i) > \texttt{LM}(h_m)$. Esto prueba que $h := h_m$ es una forma normal de f con respecto a G. Además, si $h \neq 0$ entonces $G_h = \emptyset$ (el algoritmo termina) y por lo tanto $\texttt{LM}(h) \notin L(G)$. Esto demuestra que f tiene una forma normal, independientemente de la elección del $g \in G_{h_i - 1}$.

□

Notar que en el ciclo "mientras" la elección del $g \in G_h$ puede conducir a una función de forma normal diferente.

Ejemplo 8.9. Sea $>$ el ordenamiento *dp* en $\mathtt{Mon}(x, y, z)$, $f = x^3 + y^2 + 2z^2 + x + y + 1$ y $G = \{x, y\}$, encontrar la forma normal de Buchberger.

Solución.

PASO I. Sea $h_1 = f \neq 0$ y $G_{h_1} = \{x\} \neq \emptyset$. Elegimos un $g \in G_{h_1}$ en nuestro caso $g = x$ y hacemos $h_2 = \mathtt{spoly}(h_1, g)$

$$\begin{aligned} h_2 = \quad \mathtt{spoly}(h_1, g) &= f - (1) \cdot x^{(2,0,0)} \cdot g \\ \mathtt{spoly}(h_1, g) &= x^3 + y^2 + 2z^2 + x + y + 1 - x^3 \\ \mathtt{spoly}(h_1, g) &= y^2 + 2z^2 + x + y + 1 \end{aligned}$$

PASO II. Como $h_2 \neq 0$ y $G_{h_2} = \{y\} \neq \emptyset$. Elegimos un $g \in G_{h_2}$ en nuestro caso $g = y$ y hacemos $h_3 = \mathtt{spoly}(h_2, g)$

$$\begin{aligned} h_3 = \quad \mathtt{spoly}(h_2, g) &= h_2 - (1) \cdot x^{(0,1,0)} \cdot g \\ \mathtt{spoly}(h_2, g) &= y^2 + 2z^2 + x + y + 1 - y^2 \\ \mathtt{spoly}(h_2, g) &= y^2 + 2z^2 + x + y + 1 \end{aligned}$$

PASO III. Como $h_3 \neq 0$ y $G_{h_3} = \emptyset$ ya que $x \nmid \mathtt{LM}(h_3)$ y $y \nmid \mathtt{LM}(h_3)$. Por lo tanto el algoritmo termina y $\mathtt{NFBuchberger}(f \,|\, G) = h_3 = 2z^2 + x + y + 1$

Es fácil extender $\mathtt{NFBuchberger}$ a una forma normal reducida. O bien hacemos reducción de cola durante $\mathtt{NFBuchberger}$, es decir, establecemos

$$\begin{aligned} &h := \mathtt{spoly}(h, g); \\ &h := \mathtt{LT}(h) + \mathtt{NFBuchberger}(\mathtt{tail}(h) \,|\, G); \end{aligned}$$

en el bucle while, o reducir `tail` después de aplicar $\mathtt{NFBuchberger}$, como en el algoritmo siguiente. De hecho, el argumento es válido para cualquier forma normal con respecto a un ordenamiento global.

Algoritmo redNFBuchberger($G \mid \mathtt{NF}$)

Asumir que $>$ es un ordenamiento global.

Input: $f \in K[x], G \in \mathcal{G}$
Output: $h \in K[x]$, una forma normal reducida de f con respecto a G.

$h := 0$;
$g := f$;
while $(g \neq 0)$
    $g := \mathtt{NFBuchberger}(g \mid G)$;
    if $(g \neq 0)$
        $h := h + \mathtt{LT}(g)$;
        $g := \mathtt{tail}(g)$;
return $h/\mathtt{LC}(h)$;

Como $\mathtt{tail}(g)$ tiene un término principal estrictamente más pequeño que g, el algoritmo termina, ya que $>$ es un buen ordenamiento. Que el algoritmo se mantiene en cada paso se sigue directamente del algoritmo de NFBuchberger.

Ejemplo 8.10. Sea $>$ el ordenamiento dp en $\mathtt{Mon}(x, y, z)$, $f = x^3 + y^2 + 2z^2 + x + y + 1$ y $G = \{x, y\}$. Encontrar la forma normal reducida de Buchberger.

Solución.

PASO I. Sea $h_0 = 0$ y $g_0 = f \neq 0$. Entonces hacemos $g_1 = \mathtt{NFBuchberger}(g_0 \mid G)$, por Ejemplo 8.9 sabemos que $g_1 = \mathtt{NFBuchberger}(g_0 \mid G) = 2z^2 + x + y + 1$. Como $g_1 \neq 0$ entonces hacemos $h_1 = h_0 + \mathtt{LT}(g_1) = 0 + 2z^2$ y por lo tanto hacemos $g_2 = \mathtt{tail}(g_1) = x + y + 1$.

PASO II. Como $g_2 = x + y + 1 \neq 0$. Entonces hacemos $g_3 = \mathtt{NFBuchberger}(g_2 \mid G)$

- Sea $j_0 = g_2 = x + y + 1$, como $j_0 \neq 0$ y $G_{j_0} = \{x\} \neq \emptyset$. Elegimos $g \in G_{j_0}$; en nuestro caso $g = x$ y hacemos $j_1 = \mathtt{spoly}(j_0, g)$

$$\begin{aligned} j_1 = \ & \mathtt{spoly}(j_0, g) = \ g_2 - (1) \cdot x^{(0,0,0)} \cdot g \\ = \ & \mathtt{spoly}(j_0, g) = \ x + y + 1 - x \\ = \ & \mathtt{spoly}(j_0, g) = \ y + 1 \end{aligned}$$

- Como $j_1 = y + 1 \neq 0$ y $G_{j_1} = \{y\} \neq \emptyset$. Elegimos $g \in G_{j_1}$; en nuestro caso $g = y$ y hacemos $j_2 = \mathtt{spoly}(j_1, g)$

$$\begin{aligned} j_2 = \ & \mathtt{spoly}(j_1, g) = \ j_1 - (1) \cdot x^{(0,0,0)} \cdot g \\ & \mathtt{spoly}(j_1, g) = \ y + 1 - y \\ & \mathtt{spoly}(j_1, g) = \ 1 \end{aligned}$$

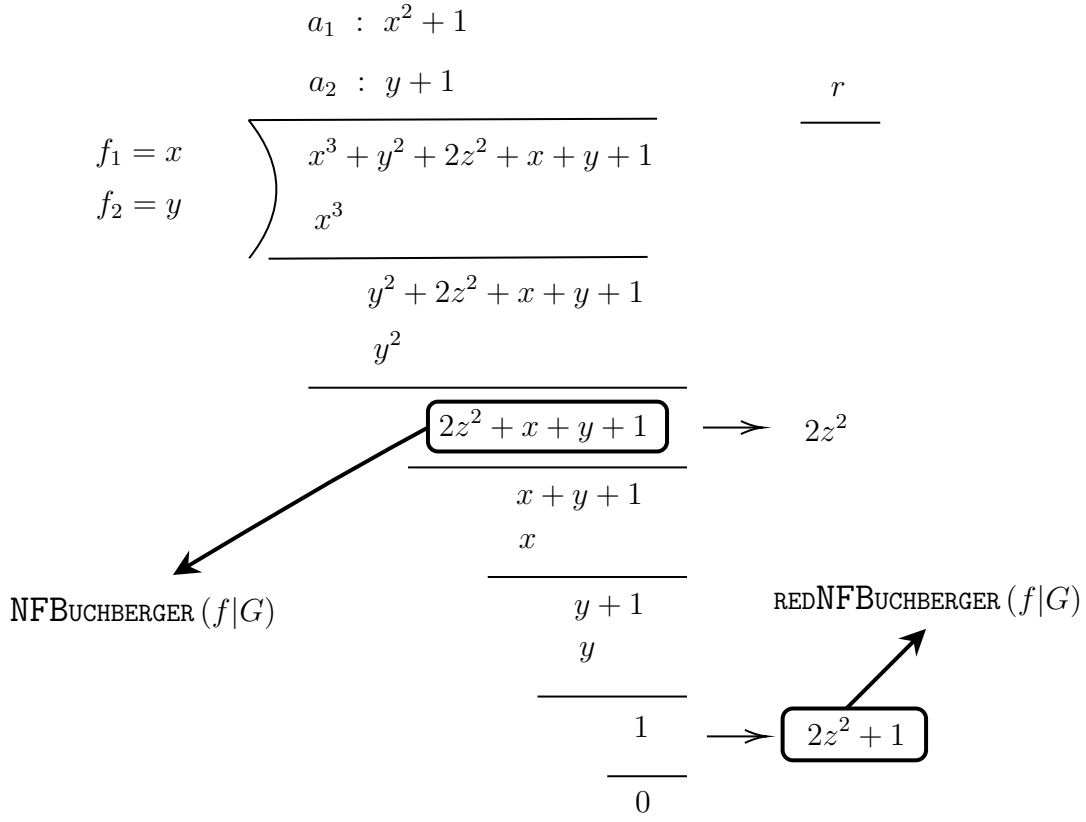
- Como $j_2 = 1 \neq 0$ pero $G_{j_2} = \emptyset$, por lo tanto $\texttt{NFBuchberger}(g_2 \,|\, G) = 1$

Como $g_3 \neq 0$ hacemos $h_2 = h_1 + \texttt{LT}(g_3) = 2z^2 + 1$ y por lo tanto hacemos $g_4 = \texttt{tail}(g_3) = 0$

PASO III. Como $g_4 = 0$ el algoritmo termina y por lo tanto $\texttt{redNFBuchberger}(f \,|\, G) = h_2/\texttt{LC}(h_2) = z^2 + 1/2$

Observemos que la forma normal de Buchberger para el caso de órdenes monomiales globales coincide con el algoritmo de la división estudiado en el Capítulo 1, el siguiente ejemplo nos muestra la relación.

Ejemplo 8.11.



Observar que en la última parte solo falta hacer mónico el polinomio $2z^2 + 1$, es decir $\texttt{redNFBuchberger}(f \,|\, G) = z^2 + 1/2$

9. Algoritmo de bases estándar

Sea $>$ un orden monomial fijo y sea en esta sección

$$R = K[x_1, \ldots, x_n]_>$$

la localización de $K[x]$, $x = \langle x_1, \ldots, x_n \rangle$ con respecto $>$. Recordemos que $R = S_>^{-1}K[x]$ con $S_> = \{u \in K[x] \setminus \{0\} : \ \mathtt{LM}(u) = 1\}$, y que $R = K[x]$ si $>$ es un orden global y $R = K[x]_{\langle x \rangle}$ si $>$ es un orden local. En cualquier caso, R puede ser considerado un subanillo del anillo de series de potencias formales $K[[x]]$.
La idea de muchos algoritmos de base estándar se puede formalizar de la siguiente manera:

Algoritmo $\textsc{Standard}(G \,|\, \mathtt{NF})$

Sea $>$ es cualquier ordenamiento monomial y $R := K[x_1, \ldots, x_n]_>$

Input: $G \in \mathcal{G}$, $\mathtt{NF}$ un algoritmo que regresa una forma normal débil.
Output: $S \in \mathcal{G}$, tal que S es una base estándar de $I = \langle G \rangle_R \subset R$.

$S := G$;
$P := \{(f, g) : \ f, g \in S, \ f \neq g\}$, el conjunto de pares;
while $(P \neq \emptyset)$
    Elegimos $(f, g) \in P$;
    $P := P \setminus \{(f, g)\}$;
    $h := \mathtt{NF}(\mathtt{spoly}(f, g) \,|\, S)$;
    if $(h \neq 0)$
        $P := P \cup \{(h, f) : \ f \in S\}$;
        $S := S \cup \{h\}$;
return S;

Para ver la terminación del algoritmo de bases estándar ($\textsc{Standard}$), debemos tener en cuenta que si $h \neq 0$ entonces $\mathtt{LM}(h) \notin L(S)$ por la propiedad (i) de $\mathtt{NF}$. Por lo tanto, obtenemos una secuencia estrictamente creciente de ideales monomiales $L(S)$ de $K[x]$ (ya que cuando $h \neq 0$ el polinomio h es agregado al conjunto S), que se vuelve estacionario, ya que $K[x]$ es Noetheriano.

Como $L(S)$ se vuelve estacionario después de una cantidad finita de pasos, tenemos que $\mathtt{NF}(\mathtt{spoly}(f, g) \,|\, S) = 0$ para $(f, g) \in P$ (al volverse estacionario el conjunto) y nuevamente, después de una cantidad finita de pasos, el conjunto de pares P quedará vacío. El algoritmo se mantiene en cada una de las etapas se deriva de la aplicación del criterio de base estándar fundamental de Buchberger que se muestra a continuación.

Observación 9.1. Si $\mathtt{NF}$ es una forma normal reducida y G es reducido, entonces S, según lo devuelto por $\textsc{Standard}(G, \mathtt{NF})$, es una base estándar reducida si eliminamos elementos cuyos monomios iniciales son divisibles por un monomio principal de otro elemento en S. Si G no se reduce, podemos aplicar una forma normal reducida después

a $(f, S \setminus \{f\})$ para todas las $f \in S$ para obtener una base estándar reducida.

Teorema 9.2. (**Criterio de Buchberger).** Sea $I \subset R$ un ideal y $G = \{g_1, \ldots, g_s\} \subset I$. Sea $\mathtt{NF}(- \mid G)$ una forma normal débil en R con respecto a G. Las siguientes condiciones son equivalentes:

I) G es una base estándar de I.

II) $\mathtt{NF}(f \mid G) = 0$ para todo $f \in I$.

III) Cada $f \in I$ tiene una representación estándar con respecto a $\mathtt{NF}(- \mid G)$.

IV) G genera I y $\mathtt{NF}(\mathtt{spoly}(g_i, g_j) \mid G) = 0$ para $i = 1, \ldots, s$.

Demostración. La implicación I) $\Rightarrow$ II) se probó en Lema 8.7, II)$\Rightarrow$ III) es claro que podemos escribir f como una combinación de elementos de G, III) $\Rightarrow$ IV) como $G \subset I$, entonces $\mathtt{spoly}(g_i \mid g_j) \in I$, por lo tanto tiene una representación estándar con respecto a G. Así $h := \mathtt{NF}(\mathtt{spoly}(g_i, g_j) \mid G) \in I$ y por lo tanto $h = 0$ o $\mathtt{LM}(h) \in L(G)$, entonces $h = 0$ caso contrario contradice la propiedad 1) de $\mathtt{NF}$. El hecho que G genera a I se sigue inmediatamente de 3). Para IV) $\Rightarrow$ I) solo se prueba para el caso de órdenes globales (ver Teorema 5.7), ya que la prueba general utiliza herramientas y teoría fuera de los objetivos de la investigación. □

Ejemplo 9.3. Sea $>$ el ordenamiento dp en $\mathtt{mon}(x, y)$, $\mathtt{NF} = \mathtt{NFBuchberger}$ y $G = \{x^2 + y, xy + x\}$. Encontrar una base estándar.

PASO I. Sea $S = G = \{x^2+y, xy+x\}$ y $P = \{(x^2+y, xy+x)\}$. Como $P \neq \emptyset$ entonces tomamos un $(f, g) \in P$ en nuestro caso $(x^2+y, xy+x)$, $P = P-\{(f, g)\} = \emptyset$ y $h = \mathtt{NFBuchberger}(\mathtt{spoly}(f, g) \mid S)$

- Encontrando $\mathtt{spoly}(f, g)$, el $\mathtt{lcm}(\mathtt{LM}(f), \mathtt{LM}(g)) = (2, 1)$

$$\begin{aligned} \mathtt{spoly}(f, g) &= x^{(0,1)} \cdot f - (1) \cdot x^{(1,0)} \cdot g \\ \mathtt{spoly}(f, g) &= (y)(x^2 + y) - (x)(xy + x) \\ \mathtt{spoly}(f, g) &= -x^2 + y^2 \end{aligned}$$

- Encontrando $\mathtt{NFBuchberger}(\mathtt{spoly}(f, g) \mid S) = \mathtt{NFBuchberger}(-x^2 + y^2 \mid S)$ con $S = \{x^2 + y, xy + x\}$
  - Sea $h_0 = -x^2 + y^2$ y $G_{h_0} = \{x^2 + y\}$. Tomamos un $g \in G_{h_0}$; $g = x^2 + y$ y hacemos $h_1 = \mathtt{spoly}(h_0, g)$

$$\begin{aligned} \mathtt{spoly}(h_0, g) &= h_0 - (-1)x^{(0,0)} \cdot g \\ \mathtt{spoly}(h_0, g) &= -x^2 + y^2 + x^2 + y \\ \mathtt{spoly}(h_0, g) &= y^2 + y \end{aligned}$$

  - Como $h_1 \neq 0$ pero $G_{h_1} = \emptyset$, entonces el algoritmo de $\mathtt{NFBuchberger}$ termina y por lo tanto $h = \mathtt{NFBuchberger}(\mathtt{spoly}(f, g) \mid S) = y^2+y$

Como $h = y^2 + y \neq 0$ entonces hacemos:
$P = \{(y^2 + y, x^2 + y), (y^2 + y, xy + x)\}$
$S = \{x^2 + y, xy + x, y^2 + y\}$

PASO II. Como $P \neq \emptyset$ tomamos $(f, g) \in P$ en nuestro caso $(y^2 + y, x^2 + y)$, $P = P - \{(f, g)\} = \{y^2 + y, x^2 + y\}$ y $h = \texttt{NFBuchberger}(\texttt{spoly}(f, g) \mid S)$

- Encontrando $\texttt{spoly}(f, g)$, el $\texttt{lcm}(\texttt{LM}(f), \texttt{LM}(g)) = (2, 2)$

$$\begin{aligned} \texttt{spoly}(f, g) = &\ x^{(2,0)} \cdot f - (1) \cdot x^{(0,2)} \cdot g \\ \texttt{spoly}(f, g) = &\ x^2(y^2 + y) - y^2(x^2 + y) \\ \texttt{spoly}(f, g) = &\ x^2 y - y^3 \end{aligned}$$

- Encontrando $\texttt{NFBuchberger}(\texttt{spoly}(f, g) \mid S) = \texttt{NFBuchberger}(x^2 y - y^3 \mid S)$ con $S = \{x^2 + y, xy + x, y^2 + y\}$.
  - Sea $h_0 = x^2 y - y^3$ y $G_{h_0} = \{x^2 + y, xy + x\}$. Tomamos un $g \in G_{h_0}$; $g = x^2 + y$ y hacemos $h_1 = \texttt{spoly}(h_0, g)$

$$\begin{aligned} \texttt{spoly}(h_0, g) = &\ h_0 - (1) x^{(0,1)} \cdot g \\ \texttt{spoly}(h_0, g) = &\ x^2 y - y^3 - y(x^2 + y) \\ \texttt{spoly}(h_0, g) = &\ -y^3 - y^2 \end{aligned}$$

  - Como $h_1 \neq 0$ y $G_{h_1} = \{y^2 + y\} \neq \emptyset$, entonces tomamos un $g \in G_{h_1}$; $g = y^2 + y$ y hacemos $h_2 = \texttt{spoly}(h_1, g)$

$$\begin{aligned} \texttt{spoly}(h_1, g) = &\ h_1 - (-1) x^{(0,1)} \cdot g \\ \texttt{spoly}(h_1, g) = &\ -y^3 - y^2 + y(y^2 + y) \\ \texttt{spoly}(h_1, g) = &\ 0 \end{aligned}$$

  - Como $h_2 = 0$ entonces $\texttt{NFBuchberger}(x^2 y - y^3 \mid S) = 0$

PASO III. Como $P \neq \emptyset$ tomamos $(f, g) \in P$ en nuestro caso $(y^2 + y, xy + x)$, $P = P - \{(f, g)\} = \emptyset$ y $h = \texttt{NFBuchberger}(\texttt{spoly}(f, g) \mid S)$

- Encontrando $\texttt{spoly}(f, g)$, el $\texttt{lcm}(\texttt{LM}(f), \texttt{LM}(g)) = (1, 2)$

$$\begin{aligned} \texttt{spoly}(f, g) = &\ x^{(1,0)} \cdot f - (1) \cdot x^{(0,1)} \cdot g \\ \texttt{spoly}(f, g) = &\ x(y^2 + y) - y(xy + x) \\ \texttt{spoly}(f, g) = &\ 0 \end{aligned}$$

- Encontrando $\texttt{NFBuchberger}(\texttt{spoly}(f, g) \mid S) = \texttt{NFBuchberger}(0 \mid S) = 0$

PASO IV. Como $P = \emptyset$ el algoritmo termina y por lo tanto $S = \{x^2 + y, xy + x, y^2 + y\}$ es una base estándar.

A continuación se presenta un algoritmo de forma normal general, ya que funciona para cualquier orden monomial. La idea básica se debe a Mora, pero el algoritmo que se presentará es más general, con una noción diferente de `ecart`.

Analicemos el algoritmo de Buchberger en el caso de un ordenamiento no global. Podemos suponer que en $K[x,y]$ tenemos $x_1,\ldots,x_n<1$, $y_1,\ldots,y_m>1$ $(m\geq 0)$.

Observemos la secuencia $m_i = c_i x^{\alpha_i} y^{\beta_i}$, $i\geq 1$, de términos construidos en el algoritmo NFBuchberger. Si $\mathtt{deg}_x(m_i)$ está acotado, entonces, dado que $>$ induce un buen orden en $K[y]$, el algoritmo se detiene después de una cantidad finita de pasos.

$$h = f - \sum_{i=1}^{s} a_i g_i,\ h, a_i \in K[y][[x]],$$

que se mantiene en $K[y][[x]]$. Sin embargo, este proceso no se detiene.

Observemos lo anterior con un ejemplo, sea $K[x]$ el anillo de polinomios en la variable x, con $x<1$, $f=x$ y $G=\{g=x-x^2\}$. Utilizando NFBuchberger se obtiene:
Sea $h_0=f$

PASO I. Como $h_0\neq 0$ y $G_{h_0}=\{x-x^2\}\neq\emptyset$. Tomamos $g=x-x^2\in G_{h_0}$ y
$$h_1 = \mathtt{spoly}(h_0,g) = x^2$$

PASO II. Como $h_1\neq 0$ y $G_{h_1}=\{x-x^2\}\neq\emptyset$.Tomamos $g=x-x^2\in G_{h_1}$ y
$$h_2 = \mathtt{spoly}(h_1,g) = x^3$$

PASO III. Como $h_2\neq 0$ y $G_{h_2}=\{x-x^2\}\neq\emptyset$.Tomamos $g=x-x^2\in G_{h_2}$ y
$$h_3 = \mathtt{spoly}(h_2,g) = x^4$$
$$\vdots$$

Observemos que el algoritmo NFBuchberger no acaba, puesto que el polinomio $h_i=x^{i+1}$ y cumple que el monomio principal de $x-x^2$ divide a h_i para $i\in\mathbb{N}$. Utilizando el algoritmo de la división es fácil ver que el algoritmo construye una serie.

$$\begin{array}{rl|l}
x & & x-x^2 \\
\cline{3-3}
-x+x^2 & & 1+x+x^2+\ldots \\
\cline{1-1}
x^2 & & \\
-x^2+x^3 & & \\
\cline{1-1}
x^3 & & \\
\vdots & &
\end{array}$$

$$x - \left(\sum_{i=1}^{\infty} x^i\right)(x - x^2) = 0$$

en $K[[x]]$, lo cual es cierto, ya que $\sum_{i=0}^{\infty} x^i = 1/(1-x)$ en $K[[x]]$. Sin embargo, el algoritmo construye una serie de potencias $\sum_{i=0}^{\infty} x^i$ que tiene infinitos términos y no la expresión racional $1/(1-x)$.

Para evitar series de potencias infinitas, debemos permitir una clase más amplia de elementos para la reducción, con el fin de crear una expresión estándar de la forma

$$uf = \sum_{i=1}^{s} a_i g_i + \mathtt{NF}(f \mid G)$$

Donde u es una unidad de R y además u, a_i y $\mathtt{NF}(f \mid G)$ son polinomios, en el caso de cuando los datos de entrada f y $G = \{g_1, \ldots, g_s\}$ son polinomios. En el ejemplo anterior llegamos a una expresión

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

en lugar de $x = \left(\sum_{i=o}^{\infty} x^i\right)(x - x^2)$, el algoritmo NFMora nos permitirá solventar este problema, la idea general es ir agregando el polinomio al conjunto de reductores, lo que permitirá obtener una factorización de la forma $1 + P(x)$.

Definición 9.4. Para $f \in K[x] \setminus \{0\}$ definimos ecart de f como

$$\mathtt{ecart}(f) = \mathtt{deg}(f) - \mathtt{deg}(\mathtt{LM}(f))$$

Notar que para un polinomio homogéneo f, tenemos que la $\mathtt{ecart}(f) = 0$.

Otra descripción de $\mathtt{ecart}(f)$ resulta ser bastante útil. Sea $f^{\mathtt{h}}$ la homogeneización de f con respecto a una nueva variable t (de modo que todos los monomios de f sean del mismo grado). Definimos en $\mathtt{Mon}(t, x_1, \ldots, x_n)$ un ordenamiento $>_{\mathtt{h}}$ por $t^p x^\alpha >_{\mathtt{h}} t^q x^\beta$ si $p + |\alpha| > q + |\beta|$ o si $p + |\alpha| = q + |\beta|$ y $x^\alpha > x^\beta$.

El ordenamiento $>_{\mathtt{h}}$ define un buen orden en $\mathtt{Mon}(t, x)$, ya que para todo $t^p x^\alpha \in \mathtt{Mon}(t, x)$ observemos que $t^p x^\alpha = 1$ si y solo si $p + |\alpha| = 0$ si y solo si $p = 0$ y $\alpha = (0, \ldots, 0)$. Sea $t^q x^\beta \in \mathtt{Mon}(t, x)$ y $(q, \beta_1, \ldots, \beta_n) \neq 0$, por definición de $>_{\mathtt{h}}$ tenemos que $q + |\beta| > 0 = 0 + |0|$, es decir $t^q x^\beta >_h 1$. Por lo tanto $>_{\mathtt{h}}$ es un buen orden en $\mathtt{Mon}(t, x)$.

Al homogeneizar un polinomio multiplicamos cada monomio de este por un t con exponente tal que sea igual al $\mathtt{deg}(f)$ menos el grado de cada monomio, para el caso del monomio principal esta es la $\mathtt{ecart}(f)$, es decir, el monomio principal de un polinomio en $K[t,x]$:

$$\mathtt{LM}_{>_\mathtt{h}}(f^\mathtt{h}) = t^{\mathtt{ecart}(f)}\mathtt{LM}_{>}(f)$$

en particular, $\mathtt{ecart}(f) = \mathtt{deg}_t\mathtt{LM}_{>_\mathtt{h}}(f^\mathtt{h})$.

Algoritmo $\mathtt{NFMora}(f \mid G)$

Asumir que $>$ es cualquier ordenamiento monomial.

Input: $f \in K[x]$, G una lista finita en $K[x]$.
Output: $h \in K[x]$, una forma normal débil polinomial de f con respecto a G.

$h := f$;
$T := G$;
while ($h \neq 0$ y $T_h := \{g \in T : \ \mathtt{LM}(g) | \mathtt{LM}(h)\} \neq \emptyset$)
    Elegimos $g \in T_h$ con $\mathtt{ecart}(g)$ mínima;
    if ($\mathtt{ecart}(g) > \mathtt{ecart}(h)$);
        $T := T \cup \{h\}$;
    $h := \mathtt{spoly}(h, g)$;
return h;

Si la entrada es homogénea, la `ecart` es siempre 0 y NFMora es igual a NFBuchberger. Si $>$ es un buen ordenamiento, entonces $\mathtt{LM}(g) \mid \mathtt{LM}(h)$ implica que $\mathtt{LM}(g) \leq \mathtt{LM}(h)$, por lo tanto, incluso si h se agrega a T durante el algoritmo, no se puede usar en reducciones adicionales. Por lo tanto, NFMora es lo mismo que NFBuchberger, pero con una estrategia de selección especial para los elementos de G.

Demostración. La terminación es más fácil de ver usando homogeneización: comencemos con $h =: f^\mathtt{h}$ y $T =: G^\mathtt{h} = \{g^\mathtt{h} : \ g \in G\}$. El bucle while se ve como sigue:

while ($h \neq 0$ y $T_h := \{g \in T : \ \mathtt{LM}(g) \mid t^\alpha\mathtt{LM}(h)$ para algún $\alpha\} \neq \emptyset$)
    Elegimos $g \in T_h$ con $\alpha \geq 0$ mínimo;
    if $\alpha > 0$;
        $T := T \cup \{h\}$;
    $h := \mathtt{spoly}(t^\alpha h, g)$;
    $h := (h|_{t=1})^\mathtt{h}$;
return $h|_{t=1}$;

Probemos que el polinomio $g \in T_h$ que se toma en el algoritmo de Mora funciona para el algoritmo homogeneizado, es decir obtenemos el mismo resultado.

Sea $h = f$ y $g \in T_h$ entonces $\mathtt{LM}_{>}(g) \,|\, \mathtt{LM}_{>}(h)$ y además g cumple con tener la `ecart` mínima (cuando homogeneizamos el polinomio, el t^α por el cual se debe multiplicar el monomio principal es el más pequeño).
Sean $h^{\mathtt{h}}$ y $g^{\mathtt{h}}$ los polinomios homogeneizados de h y g respectivamente, sus monomios principales son:

$$\mathtt{LM}_{>_{\mathtt{h}}}(h^{\mathtt{h}}) = t^{\mathtt{ecart}(h)}\mathtt{LM}_{>}(h)$$
$$\mathtt{LM}_{>_{\mathtt{h}}}(g^{\mathtt{h}}) = t^{\mathtt{ecart}(g)}\mathtt{LM}_{>}(g)$$

Probemos que el polinomio $g^{\mathtt{h}} \in T_h^{\mathtt{h}}$, primero observar que tenemos dos casos:

- Si $\mathtt{ecart}(h) \geq \mathtt{ecart}(g)$, entonces se debe multiplicar por t^0 y cumple que $\mathtt{LM}_{>_{\mathtt{h}}}(g^{\mathtt{h}})$ divide a $t^0\mathtt{LM}_{>_{\mathtt{h}}}(h^{\mathtt{h}})$ y $\alpha = 0$ es el mínimo exponente que satisface.

- Si $\mathtt{ecart}(g) > \mathtt{ecart}(h)$, ya que el polinomio g se ha tomado con `ecart` mínima entonces al homogeneizar, su monomio principal se está multiplicando por $t^{\mathtt{ecart}(g)}$ sabemos que dicho exponente es el más pequeño. El exponente de t^α por el cual debo multiplicar $\mathtt{LM}_{>_{\mathtt{h}}}(h^{\mathtt{h}})$ coincide con $\mathtt{ecart}(g) - \mathtt{ecart}(h) > 0$ y cumple con ser el mínimo y estrictamente mayor que cero, por lo tanto el polinomio $h^{\mathtt{h}}$ es agregado al conjunto T en el algoritmo homogeneizado.

Observar que el polinomio que obtenemos en el algoritmo homogeneizado coincide con el que obtenemos en el algoritmo original.

$$h_* = \mathtt{spoly}(h, g) = h - \frac{\mathtt{LC}(h)}{\mathtt{LC}(g)} x^{\alpha^* - \beta^*} g$$

$$h_*^{\mathtt{h}} = \mathtt{spoly}(t^\alpha h^{\mathtt{h}}, g^h) = t^\alpha h^{\mathtt{h}} - \frac{\mathtt{LC}(t^\alpha h^{\mathtt{h}})}{\mathtt{LC}(g^{\mathtt{h}})} x^{\alpha' - \beta'} g^{\mathtt{h}}$$

$\mathtt{LC}_{>_{\mathtt{h}}}(t^\alpha h^{\mathtt{h}}) = \mathtt{LC}_{>}(h^{\mathtt{h}}) = \mathtt{LC}_{>}(h)$ y $\mathtt{LC}_{>_{\mathtt{h}}}(g^{\mathtt{h}}) = \mathtt{LC}_{>}(g)$, ya que al homogeneizar hacemos coincidir los grados de los monomios pero sus coeficientes se mantienen. Al deshomogeneizar el polinomio $t^\alpha h^{\mathtt{h}}$ obtenemos el polinomio h, de manera similar al deshomogeneizar $g^{\mathtt{h}}$ obtenemos h. El exponente $\alpha' - \beta'$ coincide con $\alpha^* - \beta^*$ cuanto $t = 1$, puesto que $\alpha' = \mathtt{LE}(t^\alpha h^{\mathtt{h}}) = (\alpha + \mathtt{ecart}(h), \alpha_1^*, \ldots, \alpha_n^*)$ y $\beta' = \mathtt{LE}(g^{\mathtt{h}}) = (\mathtt{ecart}(g), \beta_1^*, \ldots, \beta_n^*)$, así $a' - \beta' = (\alpha + \mathtt{ecart}(h) - \mathtt{ecart}(g), \alpha_1^* - \beta_1^*, \ldots, \alpha_n^* - \beta_n^*)$. Por lo tanto el polinomio $h_*^{\mathtt{h}}$ coincide con el polinomio h_* obtenido en el algoritmo original.

Iniciamos con $T = \{g_1, \ldots, g_s\}$ y observemos que en el algoritmo homogeneizado para la primera entrada en el ciclo While el conjunto T tiene dos opciones: $T_1 = \{g_1, \ldots, g_s, h_1\}$ o $T_1 = T$.
Así:

$$L(T) \subset L(T_1) \text{ o } L(T) = L(T_1)$$

Siguiendo de esta forma en la entrada v-ésima al ciclo tendremos:

$$L(T_{v-1}) \subset L(T_v) \text{ o } L(T_{v-1}) = L(T_v)$$

De esta manera se forma una secuencia creciente de ideales $L(T_v)$. Como R es Noetheriano, existe un entero positivo N tal que $\mathtt{LT}(T_v)$ se vuelve estacionario para $v \geq N$, donde T_v denota el conjunto T después de la v-ésima vuelta en el ciclo While. El siguiente h, además, satisface $\mathtt{LM}(h) \in L(T_N) = L(T)$, de donde, $\mathtt{LM}(g)$ divide $\mathtt{LM}(h)$ para algún $g \in T$ y $\alpha = 0$ (puesto que los T_v son estacionarios para $v \geq N$, esto indica que $\alpha = 0$, de lo contrario estaríamos agregando elementos T y no sería estacionaria).
Es decir, T_v se vuelve estacionario para $v \geq N$ y el algoritmo continúa con un T fijo. Entonces termina, ya que $>$ es un buen ordenamiento en $K[t, x]$.

Para ver que el algoritmo funciona de manera correcta comencemos con $h_0 := f$ y $G = \{g_1, \ldots, g_s\}$, en el algoritmo original. Consideremos la v-ésima entrada en el ciclo While, entonces $h_v := \mathtt{spoly}(h_{v-1}, g_v^{'})$ para algún $g_v^{'} \in T_{v-1}$ tal que $\mathtt{LM}(g_v^{'}) \,|\, \mathtt{LM}(h_{v-1})$. Por lo tanto, existe algún término $m_v \in K[x]$, $\mathtt{LT}(m_v g_v^{'}) = \mathtt{LT}(h_{v-1})$, basta tomar el coeficiente por el cual se multiplica $g_v^{'}$ al obtener el S-polinomio de h_{v-1} y $g_v^{'}$. Por lo tanto

$$h_v = h_{v-1} - m_v g_v^{'}, \qquad \mathtt{LM}(h_{v-1}) = \mathtt{LM}(m_v g_v^{'}) > \mathtt{LM}(h_v)$$

Ahora para $g_v^{'}$ tenemos dos posibles resultados:

1. $g_v^{'} = g_i \in G = \{g_1, \ldots, g_s\}$ para algún i, o
2. $g_v^{'} \in T \setminus G \subset \{h_0, h_1, \ldots, h_{v-2}\}$, ya que en la $v-$ésima entrada se decide si h_{v-1} es agregado al conjunto T_v.

Supongamos, por inducción, que en los primeros $v-1$ pasos ($v \geq 1$) hemos construido representaciones estándar para f,

$$u_j f = \sum_{i=1}^{s} a_i^{(j)} g_i + h_j, \; u_j \in S_{>}, \; a_i^{(j)} \in K[x]$$

con $0 \leq j \leq v-1$.

En el caso base tomamos $u_0 := 1$ y $a_i^{(0)} = 0$, entonces $f = h_0$ lo cual es cierto.
Consideremos la representación estándar para $j = v-1$, en el caso que $g_v^{'} = g_i \in G \in$, entonces reemplazamos $h_{v-1} = h_v + m_v g_v^{'} = h_v + m_v g_i$

$$\begin{aligned} u_{v-1} f &= \sum_{i=1}^{s} a_i^{(v-1)} g_i + h_{(v-1)} \\ u_{v-1} f &= \sum_{i=1}^{s} a_i^{(v-1)} g_i + h_v + m_v g_i \\ u_{v-1} f &= \sum_{i=1}^{s} a_i^{(v)} g_i + h_v \end{aligned}$$

Como u_{v-1} sigue siendo un elemento de $S_>$ y $m_v + a_i^{(v-1)} \in K[x]$. Así $u_v f = \sum_{i=1}^{s} a_i^{(v)} g_i + h_v$ es una representación estándar.
Cuando $g_v^{'} \in T - G \subset \{h_0, \ldots, h_{v-2}\}$,

$$\begin{aligned} h_{v-1} &= h_v + m_v g_v^{'} \\ h_{v-1} &= h_v + m_v h_j, \qquad 0 \leq j \leq v-2 \\ h_{v-1} &= h_v + m_v \left(u_j f - \sum_{i=1}^{s} a_i^{(j)} g_i \right) \\ h_{v-1} &= h_v - m_v \left(\sum_{i=1}^{s} a_i^{(j)} g_i - u_j f \right) \end{aligned}$$

Sustituimos h_{v-1} por la expresión anterior

$$\begin{aligned} u_{v-1} f &= \sum_{i=1}^{s} a_i^{v-1} g_i + h_{v-1} \\ u_{v-1} f &= \sum_{i=1}^{s} a_i^{v-1} g_i + h_v - m_v \left(\sum_{i=1}^{s} a_i^{(j)} g_i - u_j f \right) \\ u_{v-1} f - m_v u_j f &= \sum_{i=1}^{s} a_i^{(v)} g_i + h_v \\ (u_{v-1} - m_v u_j) f &= \sum_{i=1}^{s} a_i^{(v)} g_i + h_v \end{aligned}$$

Se debe probar que $(u_{v-1} - m_v u_j) \in S_>$, sabemos que $\mathtt{LM}(m_v g_v^{'}) = \mathtt{LM}(h_{v-1})$, como $g_v^{'} = h_j$ entonces

$$\mathtt{LM}(m_v h_j) = \mathtt{LM}(h_{v-1}) < \mathtt{LM}(h_j)$$

Por lo tanto $\mathtt{LM}(m_v) < 1$, como $u_{v-1} \in S_>$ y $u_j \in S_>$, $\mathtt{LM}(u_{v-1}) = \mathtt{LM}(u_j) = 1$ pero $\mathtt{LM}(m_v) < 1$ entonces $\mathtt{LM}(u_{v-1} - m_v u_j) = 1 \in S_>$. Así

$$(u_{v-1} - m_v u_j) f = u_v f = \sum_{i=1}^{s} a_i^{(v)} g_i + h_v$$

tiene una representación estándar.

□

En el algoritmo se pueden realizar algunos arreglos adicionales, para que también devuelva $u \in S_>$ y los a_i. Ahora, el algoritmo de base estándar para ordenamientos monomiales arbitrarios se ve formalmente como sigue:

Algoritmo $\textsc{StandardBasis}(G \,|\, \texttt{NF})$

Sea $>$ es cualquier ordenamiento monomial en $R = K[x]_>$

Input: $G = \{g_1, \ldots, g_s\} \subset K[x]$
Output: $S = \{h_1, \ldots, h_t\} \subset K[x]$, tal que S es una base estándar del ideal $\langle G \rangle_R \subset R$.
$S := \textsc{Standard}(G, \texttt{NFMora})$;
return S;

Ejemplo 9.5. Sea $>$ el ordenamiento ds en $\texttt{Mon}(x, y, z)$, $f = x^2 + y^2 + z^3 + x^4 + y^5$ y $G = \{x, y\}$. Encontrar $\texttt{NFMora}(f \,|\, G)$.

Solución.

PASO I. Sea $h_1 = f = x^2 + y^2 + z^3 + x^4 + y^5$ y $T = G = \{x, y\}$. Como $h_1 \neq 0$ y $T_{h_1} = \{x\} \neq \emptyset$, entonces tomamos $g \in T_{h_1}$; $g = x$. Como la $\texttt{ecart}(g) = 0$ es menor que la $\texttt{ecart}(h_1) = 3$ entonces h_1 no se agrega al conjunto T_{h_1}. Ahora hacemos $h_2 = \texttt{spoly}(h_1, g)$

$$\begin{aligned} \texttt{spoly}(h_1, g) &= h_1 - (1)x^{(1,0)} \cdot g \\ \texttt{spoly}(h_1, g) &= x^2 + y^2 + z^3 + x^4 + y^5 - x(x) \\ \texttt{spoly}(h_1, g) &= y^2 + z^3 + x^4 + y^5 \end{aligned}$$

PASO II. Como $h_2 \neq 0$ y $T_{h_2} = \{y\} \neq \emptyset$, entonces tomamos $g \in T_{h_2}$; $g = y$. Como la $\texttt{ecart}(g) = 0$ es menor que la $\texttt{ecart}(h_2) = 3$ entonces h_2 no se agrega al conjunto T_{h_2}. Ahora hacemos $h_3 = \texttt{spoly}(h_2, g)$

$$\begin{aligned} \texttt{spoly}(h_2, g) &= h_2 - (1)x^{(0,1)} \cdot g \\ \texttt{spoly}(h_2, g) &= y^2 + z^3 + x^4 + y^5 - y(y) \\ \texttt{spoly}(h_2, g) &= z^3 + x^4 + y^5 \end{aligned}$$

PASO III. Como $h_3 \neq 0$ y $T_{h_3} = \emptyset$ el algoritmo termina y por lo tanto $\texttt{NFMora}(f \,|\, G) = z^3 + x^4 + y^5$

CAPÍTULO 3: Aplicaciones

Para el desarrollo de este capítulo, se han empleado las bases estándar para dar solución a problemas clásicos del álgebra moderna como lo son: la pertenencia al ideal, eliminación de variables, intersección de ideales y pertenencia al radical.

Para encontrar una forma normal, una base estándar e incluso calcular S-polinomios observamos que requieren de mucho tiempo y de mucha destreza en el cálculo aritmético, además a medida que los polinomios tienen más términos o el conjunto de generadores de un ideal es bastante grande, el cálculo aritmético aumenta, lo cual lleva a la necesidad de utilizar una herramienta que facilite la obtención de estos cálculos. Por lo que, para el desarrollo de los ejemplos de este capítulo se hace uso del software **Singular**, el cual es un sistema de álgebra computacional para cálculos polinomiales, con especial énfasis en álgebra conmutativa y no conmutativa, geometría algebraica y teoría de la singularidad. Permitiendo obtener resultados de forma eficiente y presentar así ejemplos con mayor dificultad.

10. Pertenencia de un ideal

Sea $K[x] = K[x_1, \ldots, x_n]$ un anillo de polinomios sobre un campo K, $>_0$ un ordenamiento monomial arbitrario y $R = K[x]_{>_0}$ el anillo asociado a $K[x]$ y $>_0$. Recordemos que $K[x] \subset R \subset K[x]_{\langle x \rangle}$, y que $R = K[x]_{\langle x \rangle}$ si y solo si $>_0$ es un orden local.

Sea `NF` una forma normal, `NFBuchberger` o `redNFBuchberger` si $>_0$ es un orden global y `NFMora` en el caso general.

El problema de pertenencia de un polinomio a un ideal nos dice:

Problema: dados $f, f_1, \cdots, f_r \in K[x]$ y sea $I = \langle f_1, \ldots, f_r \rangle_{K[x]_>}$. Se desea saber si el polinomio f está o no en el ideal I.

Solución: elegimos cualquier orden monomial $>$ tal que $R = K[x]_>$ y calculamos una base estándar $G = \{g_1, \ldots, g_s\}$ de I con respecto a $>$. Si `NF` es cualquier forma normal débil, entonces $f \in I$ si y solo si $\texttt{NF}(f \mid G) = 0$, lo cual se probó en Lema 8.7.

Dado que el resultado es independiente de la elección de `NF`, se utiliza, por razones

de eficiencia, una forma normal no reducida. Si $>_0$ es global, generalmente se elige *dp* y, si $>_0$ es local, entonces se prefiere *ls* o *ds*.

Ejemplo 10.1. Determinar si el polinomio $f = xy^3 - z^2 + y^5 - z^3 \in \mathbb{Q}[x, y, z]$ pertenece al ideal $I = \langle -x^3 + y, x^2y - z \rangle$.

Utilizando el orden monomial lexicográfico *lp*, sea $g_1 = -x^3 + y$ y $g_2 = x^2y - z$, primero observemos que $G = \{g_1, g_2\}$ no es una base de Gröbner, ya que $h = \texttt{spoly}(g_1, g_2) = -xz + y^2$ y el resto de la división de h por G es $-xz + y^2$ distinto de cero.

Calculamos una base de Gröbner para I, hacemos uso del algoritmo NFBuchberger y Standard para encontrar una base de Gröbner.

$S = G = \{g_1, g_2\}$
$P = \{(g_1, g_2)\}$

PASO I. Como $P \neq \emptyset$, tomamos $(g_1, g_2) \in P$ y:
$P = P - \{(g_1, g_2)\} = \emptyset$
$h_1 = \texttt{NFBuchberger}(\texttt{spoly}(g_1, g_2) \mid S) = -xz + y^2$
Como $h_1 \neq 0$ entonces:
$P = P \cup \{(h_1, g_1), (h_1, g_2)\} = \{(h_1, g_1), (h_1, g_2)\}$
$S = S \cup \{h_1\} = \{g_1, g_2, h_1\}$

PASO II. Como $P \neq \emptyset$, tomamos $(h_1, g_1) \in P$ y:
$P = P - \{(h_1, g_1)\} = \{(h_1, g_2)\}$
$h_2 = \texttt{NFBuchberger}(\texttt{spoly}(h_1, g_1) \mid S) = 0$

PASO III. Como $P \neq \emptyset$, tomamos $(h_1, g_2) \in P$ y:
$P = P - \{(h_1, g_2)\} = \emptyset$
$h_3 = \texttt{NFBuchberger}(\texttt{spoly}(h_1, g_2) \mid S) = xy^3 - z^2$
Como $h_3 \neq 0$ entonces:
$P = P \cup \{(h_3, g_1), (h_3, g_2), (h_3, h_1)\} = \{(h_3, g_1), (h_3, g_2), (h_3, h_1)\}$
$S = S \cup \{h_3\} = \{g_1, g_2, h_1, h_3\}$

PASO IV. Como $P \neq \emptyset$, tomamos $(h_3, g_1) \in P$ y:
$P = P - \{(h_3, g_1)\} = \{(h_3, g_2), (h_3, h_1)\}$
$h_4 = \texttt{NFBuchberger}(\texttt{spoly}(h_3, h_1) \mid S) = 0$

PASO V. Como $P \neq \emptyset$, tomamos $(h_3, g_2) \in P$ y:
$P = P - \{(h_3, g_2)\} = \{(h_3, h_1)\}$
$h_5 = \texttt{NFBuchberger}(\texttt{spoly}(h_3, g_2) \mid S) = 0$

PASO VI. Como $P \neq \emptyset$, tomamos $(h_3, h_1) \in P$ y:
$P = P - \{(h_3, h_1)\} = \emptyset$
$h_6 = \texttt{NFBuchberger}(\texttt{spoly}(h_3, h_1) \mid S) = y^5 - z^3$

Como $h_6 \neq 0$ entonces:
$P = P \cup \{(h_6, g_1), (h_6, g_2), (h_6, h_1), (h_6, h_3)\} = \{(h_6, g_1), (h_6, g_2), (h_6, h_1), (h_6, h_3)\}$
$S = S \cup \{h_6\} = \{g_1, g_2, h_1, h_3, h_6\}$

PASO VII. Como $P \neq \emptyset$, tomamos $(h_6, g_1) \in P$ y:
$P = P - \{(h_6, g_1)\} = \{(h_6, g_2), (h_6, h_1), (h_6, h_3)\}$
$h_7 = \texttt{NFBuchberger}(\texttt{spoly}(h_6, g_1) \,|\, S) = 0$

PASO VIII. Como $P \neq \emptyset$, tomamos $(h_6, g_2) \in P$ y:
$P = P - \{(h_6, g_2)\} = \{(h_6, h_1), (h_6, h_3)\}$
$h_8 = \texttt{NFBuchberger}(\texttt{spoly}(h_6, g_2) \,|\, S) = 0$

PASO IX. Como $P \neq \emptyset$, tomamos $(h_6, h_1) \in P$ y:
$P = P - \{(h_6, h_1)\} = \{(h_6, h_3)\}$
$h_8 = \texttt{NFBuchberger}(\texttt{spoly}(h_6, h_1) \,|\, S) = 0$

PASO X. Como $P \neq \emptyset$, tomamos $(h_6, h_3) \in P$ y:
$P = P - \{(h_6, h_3)\} = \emptyset$
$h_8 = \texttt{NFBuchberger}(\texttt{spoly}(h_6, h_3) \,|\, S) = 0$

PASO XI. Como $P = \emptyset$ el algoritmo termina y la base de Gröbner para el ideal I es:
$S = \{g_1, g_2, h_1, h_3, h_6\} = \{-x^3 + y, x^2y - z, -xz + y^2, xy^3 - z^2, y^5 - z^3\}$

Haciendo uso de la base encontrada, se verifica si el polinomio f se encuentra en I, para lo cual se calcula la forma normal de f con respecto a la base de Gröbner, es decir el resto de la división de f por G, que es $-2z^2$ por lo tanto el polinomio $f \notin I$.

Ahora asumir que $f \in I = \langle f_1, \ldots, f_k \rangle_R$. Entonces existen $u \in K[x] \cap R^*$, $a_1, \ldots, a_k \in K[x]$ tal que

$$uf = a_1 f_1 + \cdots + a_k f_k$$

Si $\{f_1, \ldots, f_k\}$ es una base estándar de I entonces en principio, el algoritmo de forma normal NFMora proporciona u y los a_i. Sin embargo, también es posible expresar f como una combinación lineal de los generadores arbitrarios dados $f_1, \ldots, f_k$.

Ejemplo 10.2. Determina si el polinomio $f = xy^{13} + y^{12} \in \mathbb{Q}[x, y]$ pertenece al ideal $I = \langle x^{10} + x^9y^2, y^8 - x^2y^7 \rangle$, utilizando el orden monomial *dp* escribimos f como combinación de los polinomios $g_1 = x^{10} + x^9y^2$ y $g_2 = y^8 - x^2y^7$, $f = y^7(g_1) + (x^7y^2 + x^8 + x^5y^3 + x^6y + x^3y^4 + x^4y^2 + xy^5 + x^2y^3 + y^4)(g_2)$.

En un anillo local podemos, en general, expresar uf como una combinación lineal polinomial de los generadores de I si $f \in I$.

Ejemplo 10.3. Determinar si el polinomio $f = yx^2 + yx \in \mathbb{Q}[x, y, z]$ con orden monomial *ds* está en el ideal $I = \langle x - x^2, y + x \rangle$.

Sea $G = \{g_1, g_2\} = \{x - x^2, y + x\}$ probemos que G no es una base estándar para el ideal I, sea $h = \texttt{spoly}(g_1, g_2) = -y - x^2$ y la forma normal de h con respecto a G es $-y - x^2$, por lo tanto G no es una base estándar.

Encontremos una base estándar para el ideal I:
$S := \{x - x^2, y + x\}$
$P := \{(x - x^2, y + x)\}$

PASO I. Como $P \neq \emptyset$, tomamos $(g_1, g_2) \in P$ y:
$P = P - \{(g_1, g_2)\} = \emptyset$
$h_1 = \texttt{NFMora}(\texttt{spoly}(g_1, g_2) \,|\, S) = -y - y2$
Como $h_1 \neq 0$ entonces:
$P = P \cup \{(h_1, g_1), (h_1, g_2)\} = \{(h_1, g_1), (h_1, g_2)\}$
$S = S \cup \{h_1\} = \{g_1, g_2, h_1\}$

PASO II. Como $P \neq \emptyset$, tomamos $(h_1, g_1) \in P$ y:
$P = P - \{(h_1, g_1)\} = \{(h_1, g_2)\}$
$h_2 = \texttt{NFMora}(\texttt{spoly}(h_1, g_1) \,|\, S) = 0$

PASO III. Como $P \neq \emptyset$, tomamos $(h_1, g_2) \in P$ y:
$P = P - \{(h_1, g_2)\} = \emptyset$
$h_3 = \texttt{NFMora}(\texttt{spoly}(h_1, g_2) \,|\, S) = 0$

PASO IV. Como $P = \emptyset$ el algoritmo termina y la base estándar para el ideal I es:
$S = \{g_1, g_2, h_1\} = \{x - x^2, x + y, -y - y^2\}$

Haciendo uso de la base encontrada se verifica si el polinomio f se encuentra en I, para lo cual se encuentra la forma normal de f con respecto a la base de estándar, $\texttt{NFMora}(f, S) = 0$ por lo tanto el polinomio $f \in I$.

11. Eliminación de variables

Para introducir la eliminación de variables veamos un ejemplo que permitirá tener una idea general.

Ejemplo 11.1. Sea $I \subset K[x, y, z]$ un ideal, tal que

$$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$$

entonces una de base de Gröbner para I, con ordenamiento *lp* está dada por

$$G = \{x + y + z^2 - 1, y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2\}$$

observemos que el polinomio $h = z^6 - 4z^4 + 4z^3 - z^2$ solo depende de la variable z, se han eliminado las variables x y y. El polinomio h cumple:

$$h \in I \cap K[z]$$

donde $I \cap K[z]$ consiste en todas las consecuencias de las ecuaciones que eliminan x y y. Generalizar esta idea lleva a la siguiente definición.

Definición 11.2. Dado el ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq K[x_1, \ldots, x_n]$, la k-ésima *eliminación del ideal* I_k es el ideal de $K[x_{k+1}, \ldots, x_n]$ definido por

$$I_k = I \cap K[x_{k+1}, \ldots, x_n].$$

Así, I_k consiste en todas las consecuencias de $f_1 = \cdots = f_s = 0$ que eliminan las variables $x_1, \ldots, x_k$. Es fácil ver que $I_k := I \cap K[x_{k+1}, \ldots, x_n]$ es un ideal de $K[x_{k+1}, \ldots, x_n]$, $0 \in I$ y $0 \in K[x_{k+1}, \ldots, x_n]$ entonces $0 \in I_k$. Sean $f, g \in I_k$ se tiene que $f, g \in I$ y $f, g \in K[x_{k+1}, \ldots, x_n]$ entonces $f + g \in K[x_{k+1}, \ldots, x_n]$ y por lo tanto $f + g \in I_k$. Si $f \in I_k$ y $g \in K[x_{k+1}, \ldots, x_n]$ se tiene que $f \in I$ y $f \in K[x_{k+1}, \ldots, x_n]$, entonces $f \cdot g \in I, K[x_{k+1}, \ldots, x_n]$ por lo tanto $f \cdot g \in I_k$.

Observemos que $I = I_0$ es la 0-ésima eliminación del ideal. Además diferentes ordenamientos de las variables conducen a diferentes ideales de eliminación.
Entonces estamos interesados en encontrar un conjunto generador para el ideal de eliminación, es decir, se quiere dar solución al siguiente problema (nos limitamos al caso del anillo polinomial).

Problema: dados $f_1, \ldots, f_s \in K[x] = K[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_s \rangle_{K[x]}$, se desea encontrar generadores para el ideal

$$I' = I \cap K[x_{k+1}, \ldots, x_n], \quad k < n$$

Diremos que los elementos del ideal I' se obtienen de $f_1, \ldots, f_s$ *eliminando* las variables $x_1, \ldots, x_k$. Para resolver este problema, es necesario un orden de eliminación global para las variables $x_1, \ldots, x_k$. Se puede usar el orden lexicográfico *lp*, que es un ordenamiento de eliminación para cada k, o construir un orden de eliminación que a menudo es bastante rápido.

Sea $>$ un ordenamiento arbitrario y sean $a_1, \ldots, a_k$ enteros positivos. Se define $>_a$ de la siguiente manera:

$$\begin{aligned} x^\alpha >_a x^\beta \quad :\Longleftrightarrow \quad & a_1\alpha_1 + \cdots + a_k\alpha_k > a_1\beta_1 + \cdots + a_k\beta_k \quad \text{o} \\ & a_1\alpha_1 + \cdots + a_k\alpha_k = a_1\beta_1 + \cdots + a_k\beta_k \quad \text{y} \quad x^\alpha > x^\beta \end{aligned}$$

Entonces $>_a$ es un ordenamiento de eliminación y $a = (a_1, \ldots, a_k)$ es llamado un *vector de peso extra*.
Si $>$ es un ordenamiento de eliminación arbitrario para $x_1, \ldots, x_k$, entonces

$$K[x_1, \ldots, x_n]_> = (K[x_{k+1}, \ldots, x_n]_{>'})[x_1, \ldots, x_k],$$

(ver Ejemplo 7.6), son los polinomios en las variables $x_1, \ldots, x_s$ con coeficientes en el anillo $K[x_{s+1}, \ldots, x_n]_{>'}$.

Ya que las unidades en $K[x]_>$ no involucran $x_1, \ldots, x_s$ (denotamos por $>'$, el ordenamiento en $\mathtt{Mon}(x_{s+1}, \ldots, x_n)$ inducido por $>$). Por lo tanto, $f \in K[x_{s+1}, \ldots, x_n]_{>'}$ para cualquier $f \in K[x_1, \ldots, x_n]_>$ tal que $\mathtt{LM}(f) \in K[x_{s+1}, \ldots, x_n]$.

El siguiente lema es la base para resolver el problema de eliminación.

Lema 11.3. Sea $>$ un ordenamiento de eliminación para $x_1, \ldots, x_s$ en el conjunto de monomios $\mathtt{Mon}(x_1, \ldots, x_n)$, y sea $I \subset K[x_1, \ldots, x_n]_>$ un ideal. Si $S = \{g_1, \ldots, g_k\}$ es una base estándar de I, entonces

$$S' := \{g \in S : \ \mathtt{LM}(g) \in K[x_{s+1}, \ldots, x_n]\}$$

es una base estándar de $I' := I \cap K[x_{s+1}, \ldots, x_n]_{>'}$. En particular, S' genera el ideal I'.

Demostración. Como $S' \subseteq I'$ entonces $L(S') \subseteq L(I')$. Para probar la otra inclusión $L(I') \subseteq L(S')$, tomamos un $f \in I'$ arbitrario y probamos que $\mathtt{LM}(f)$ divisible por $\mathtt{LM}(g)$ para algún $g \in S'$. Dado $f \in I' \subset I$ existen $g_i \in S$ tal que $\mathtt{LM}(g_i)$ divide $\mathtt{LM}(f)$, ya que S es una base estándar de I. Como $f \in K[x_{s+1}, \ldots, x_n]_>$, se tiene $\mathtt{LM}(f) \in K[x_{s+1}, \ldots, x_n]$ y por lo tanto $\mathtt{LM}(g_i) \in K[x_{s+1}, \ldots, x_n]$, es decir $g_i \in S'$. Por lo tanto $L(S') = L(I')$, así S' es una base estándar de I'. □

El problema general de eliminación puede plantearse, para cualquier anillo asociado a un ordenamiento monomial, de la siguiente manera. Recordar que el orden en la variable a eliminar debe ser global.

Problema: dados los polinomios $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, sea $I := \langle f_1, \ldots, f_k \rangle_R$ con $R := (K[x_{s+1}, \ldots, x_n]_>)[x_1, \ldots, x_s]$ para algún orden monomial $>$ en $\mathtt{Mon}(x_{s+1}, \ldots, x_n)$. Encontrar los generadores para el ideal $I' := I \cap K[x_{s+1}, \ldots, x_n]_>$.

Solución: elegimos un ordenamiento de eliminación $>$ para $x_1, \ldots, x_s$ en $\mathtt{Mon}(x_1, \ldots, x_n)$, lo que induce un orden en $\mathtt{Mon}(x_{s+1}, \ldots, x_n)$, y calculamos una base estándar $S = \{g_1, \ldots, g_k\}$ de I. Por Lema 11.3, aquellos g_i, para los cuales $\mathtt{LM}(g_i)$ no involucran $x_1, \ldots, x_s$, genera I' (es una base estándar para I').

Ejemplo 11.4. Sea $I = \langle x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1\rangle \subset \mathbb{Q}[x, y, z]$ un ideal, encontrar los ideales de eliminación, con el ordenamiento lexicográfico.
Encontramos una base de Gröbner para I,

$$G = \left\{x + 2z^3 - 3z, y^2 - z^2 - 1, z^4 - \frac{3}{2}z^2 + \frac{1}{2}\right\}$$

tenemos que $I = \langle G\rangle$, utilicemos el proceso para resolver el problema planteado antes.

- Para $I_0 = I \cap \mathbb{Q}[x, y, z] = I = \langle G\rangle$.
- Para $I_1 = I \cap \mathbb{Q}[y, z]$ con base de Gröbner $G_1 = G \cap \mathbb{Q}[y, z] = \left\{y^2 - z^2 - 1, z^4 - \frac{3}{2}z^2 + \frac{1}{2}\right\}$.
  Así $I_1 = \left\langle y^2 - z^2 - 1, z^4 - \frac{3}{2}z^2 + \frac{1}{2}\right\rangle$.
- Para $I_2 = I \cap K[z]$ con base de Gröbner $G_2 = G \cap \mathbb{Q}[z] = \left\{\frac{3}{2}z^2 + \frac{1}{2}\right\}$. Así $I_2 = \left\langle \frac{3}{2}z^2 + \frac{1}{2}\right\rangle$

Ejemplo 11.5. Sea $I = \langle t^2 + x^2 + y^2 + z^2, t^2 + 2x^2 - xy - z^2, t + y^3 - z^3\rangle \subset \mathbb{Q}[t, x, y, z]$ con orden monomial *dp*, encontrar el ideal de eliminación de la variable t, es decir $I_t = I \cap K[x, y, z]$.
Se calcula una base de Gröbner $G = \{3x^2 - xy - y^2 - 2z^2, t^2 + 4x^2 - xy - z^2, y^3 - z^3 + t\}$ para el ideal I. Una base de Gröbner para el ideal $I_t = I \cap K[x, y, z]$ es $G' = \{3x^2 - xy - y^2 - 2z^2\}$.
Por lo tanto $I_t = \langle 3x^2 - xy - y^2 - 2z^2\rangle$

12. Intersección de ideales

Dados dos ideales y un conjunto de generadores, para cada uno, nos gustaría poder calcular un conjunto de generadores para la intersección.

Definición 12.1. La intersección $I \cap J$ de dos ideales I y J en $K[x_1, \ldots, x_n]$, es el conjunto de polinomios que pertenecen tanto a I como a J.

Proposición 12.2. Si I y J son ideales en $K[x_1, \ldots, x_n]$, entonces $I \cap J$ es un ideal.

Demostración. Observemos que $0 \in I \cap J$ ya que $0 \in I$ y $0 \in J$. Si $f, g \in I \cap J$, entonces $f, g \in I$ así $f + g \in I$ y $f, g \in J$ así $f + g \in J$ (puesto que I, J son ideales), por lo tanto $f + g \in I \cap J$. Sea $f \in I \cap J$ y $h \in K[x_1, \ldots, x_n]$, ya que $f \in I$ y I es un ideal, se tiene que $h \cdot f \in I$. Además $f \in J$ y J es un ideal, se tiene que $h \cdot f \in J$. Así $h \cdot f \in I \cap J$. Por lo tanto $I \cap J$ es un ideal. □

Problema: dados $f_1, \ldots, f_r, h_1, \ldots, h_s \in K[x]$ y $>$ un ordenamiento monomial, sea $I_1 = \langle f_1, \ldots, f_r \rangle_{K[x]_>}$ y $I_2 = \langle h_1, \ldots, h_s \rangle_{K[x]_>}$. Deseamos encontrar generadores para $I_1 \cap I_2$.

Para dar solución a este problema necesitamos el siguiente Lema.

Lema 12.3. Sean $I_1 = \langle f_1, \ldots, f_r \rangle_{K[x]_>}$ y $I_2 = \langle h_1, \ldots, h_s \rangle_{K[x]_>}$ y consideremos el ideal

$$J := \langle tf_1, \ldots, tf_r, (1-t)h_1, \ldots, (1-t)h_s \rangle_{K[x]_>[t]},$$

donde t es una variable extra. Entonces $I_1 \cap I_2 = J \cap K[x]_>$.

Demostración. Sea $f \in I_1 \cap I_2$, entonces $f = \sum_{i=1}^{r} \xi_i f_i \in I_1$ y $f = \sum_{j=1}^{s} \eta_j h_j \in I_2$, donde $\xi_i, \eta_j \in K[x]_>$. Observar que f se puede escribir de la siguiente manera:

$$f = tf + (1-t)f = \sum_{i=1}^{r} \xi_i t f_i + \sum_{j=1}^{s} \eta_j (1-t) h_j \in J \cap K[x]_>.$$

Si $f \in J \cap K[x]_>$, entonces

$$f = \sum_{i=1}^{r} \xi_i t f_i + \sum_{j=1}^{s} \eta_j (1-t) h_j$$

Ya que $f \in K[x]_>$ es independiente de t, se tiene que

$$f = \sum_{i=1}^{r} \xi_i|_{(t=1)} f_i \quad \text{y} \quad f = \sum_{j=1}^{s} \eta_j|_{(t=0)} h_j$$

Es decir, $f \in I_1 \cap I_2$.

□

Solución:

El resultado anterior nos proporciona un algoritmo para calcular la intersección de ideales. Si $I_1 = \langle f_1, \ldots, f_r \rangle$ y $I_2 = \langle g_1, \ldots, g_s \rangle$, consideramos el ideal

$$\langle tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s \rangle \subset K[x_1, \ldots, x_n]_>$$

y calculamos una base estándar respecto de un orden que elimina a t, y después calculamos el primer ideal de eliminación y por Lema 11.3 tendremos una base estándar de $I_1 \cap I_2$. Veamos algunos ejemplos, los cálculos se realizan en Singular.

Ejemplo 12.4. Dados los ideales de $I, J \subset \mathbb{Q}[y, x]$, con $I = \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle$ y $J = \langle x, y^2 - 4 \rangle$. Encontrar un conjunto generador para el ideal $I \cap J$, utilizando el orden monomial *lp*.

Consideremos el ideal $J := \langle t(2x^4 - 3x^2y + y^2 - 2y^3 + y^4), (1-t)x, (1-t)(y^2-4)\rangle$, encontramos una base estándar G para J.

$$\begin{aligned} G =&\{y^4x - 2y^3x + y^2x - 3yx^3 + 2x^5, y^6 - 2y^5 - 3y^4 - 3y^3x^2 + 8y^3 + 2y^2x^4 - 4y^2 + \\ &12yx^2 - 8x^4, 36t + 2y^5 + y^4 - 8y^3 - 6y^2x^2 + 5y^2 + 4yx^4 - 15yx^2 + 10x^4 - 36\} \end{aligned}$$

Utilizando eliminación de variables con orden monomial *lp* se tiene que una base para el ideal $J \cap \mathbb{Q}[x, y]$ es el conjunto:

$$G' = \{y^4x - 2y^3x + y^2x - 3yx^3 + 2x^5, y^6 - 2y^5 - 3y^4 - 3y^3x^2 + 8y^3 + 2y^2x^4 - 4y^2 + 12yx^2 - 8x^4\}$$

Por lo tanto G' es una base para $I_1 \cap I_2$.

Ejemplo 12.5. Sea I_1, I_2 ideales de $K[x, y, z]$, tal que $I_1 = \langle x, y\rangle$ y $I_2 = \langle y^2, z\rangle$, utilizando el orden monomial *dp*, encontrar un conjunto de generadores para el ideal $I_1 \cap I_2$.

Sea el ideal $J = \langle t(x), x(y), (1-t)y^2, (1-t)z\rangle$, encontramos una base estándar para el ideal J. Sea $G = \{yz, xz, tz - z, y^2, ty, tx\}$ una base estándar de J, utilizando eliminación de variables se tiene que una base para el ideal $J \cap K[x]_>$ es el conjunto $G' = \{yz, xz, y^2\}$, por lo tanto el conjunto generador para $I_1 \cap I_2$ es G'.

13. Pertenencia al radical

Definición 13.1. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal. El *radical* de I, denotado por $\sqrt{I}$ es el conjunto

$$\sqrt{I} := \{f \in K[x_1, \ldots, x_n] : \exists m \in \mathbb{N},\ f^m \in I\}$$

Observación 13.2. Notar que $I \subseteq \sqrt{I}$, puesto que $f \in I$ entonces $f^1 \in I$ y por lo tanto $f \in \sqrt{I}$ por definición.

Lema 13.3. Si I es un ideal de $K[x_1, \ldots, x_n]$, entonces $\sqrt{I}$ es un ideal de $K[x_1, \ldots, x_n]$.

Demostración. De la observación anterior se sabe que $I \subseteq \sqrt{I}$. Probemos que $\sqrt{I}$ es un ideal, sean $f, g \in \sqrt{I}$. Entonces existen enteros positivos m y l tal que $f^m, g^l \in I$. Por la expansión binomial de $(f+g)^{m+l-1}$ cada término tiene un factor $f^i g^j$ con $i+j = m+l-1$. Ya sea que $i \geq m$ o $j \geq l$, ya sea f^i o g^j pertenece a I y cada término en la expansión binomial está en I. Por lo tanto $(f+g)^{m+l-1} \in I$ y además $f + g \in \sqrt{I}$. Finalmente sea $f \in \sqrt{I}$ y $h \in K[x_1, \ldots, x_n]$. Entonces $f^m \in I$ para algún entero $m \geq 1$, ya que I es un ideal, se tiene que $(h \cdot f)^m = h^m f^m \in I$. Por lo tanto, $hf \in \sqrt{I}$. Esto prueba que $\sqrt{I}$ es un ideal. □

Se quiere encontrar una solución al siguiente problema.

Problema: sean $f_1, \ldots, f_k \in K[x]_>$, $>$ un ordenamiento en $\texttt{Mon}(x_1, \ldots, x_n)$ y $I = \langle f_1, \ldots, f_k \rangle_{K[x]_>}$. Dado $f \in K[x]_>$ queremos decidir si $f \in \sqrt{I}$.

El siguiente lema, que se le conoce como el *truco de Rabinowitsch*, es la base para resolver el problema anterior.

Lema 13.4. Sea A un anillo, $I \subset A$ un ideal y $f \in A$. Entonces

$$f \in \sqrt{I} \Longleftrightarrow 1 \in \tilde{I} := \langle I, 1 - tf \rangle_{A[t]}$$

donde t es una variable adicional nueva.

Demostración. $\Longrightarrow$: Sea $f \in \sqrt{I}$, entonces $f^m \in I$ entonces $t^m f^m \in \tilde{I}$ y, por lo tanto, $1 = t^m f^m + (1 - t^m f^m) = t^m f^m + (1 - tf)(1 + tf + \cdots + t^{m-1} f^{m-1}) \in \tilde{I}$.
$\Longleftarrow$: Si $1 \in \tilde{I}$. Sin pérdida de generalidad, podemos suponer que f no es nilpotente (no existe algún entero positivo n tal que $f^n = 0$), ya que de lo contrario $f \in \sqrt{I}$.
Por hipótesis, existen $f_1, \ldots, f_k \in I$ y $a_i(t) = \sum_{j=0}^{d_i} a_{ij} t^j \in A[t]$, $i = 0, \ldots, k$ tal que

$$1 = \sum_{i=1}^{k} a_i(t) f_i + a_0(t)(1 - tf)$$

Ya que f no es nilpotente podemos reemplazar t por $1/f$ y obtenemos

$$1 = \sum_i a_i \left(\frac{1}{f} \right) f_i = \sum_{i,j} a_{ij} f^{-j} f_i$$

en la localización A_f, ver sección 1.4. Multiplicando por f^m, para m suficientemente grande, obtenemos $f^m = \sum_{i,j} (a_{ij} f^{m-j}) f_i \in I$ (incluso en A, no solo en A_f). □

Solución: Por el Lema anterior, se tiene $f \in \sqrt{I}$ si y solo si

$$1 \in J := \langle f_1, \ldots, f_k, 1 - tf \rangle_{(K[x]_>)[t]},$$

donde t es una nueva variable.
Para resolver el problema, elegimos en $\texttt{Mon}(t, x_1, \ldots, x_n)$ un ordenamiento de eliminación para t induciendo $>'$ en $\texttt{Mon}(x_1, \ldots, x_n)$ tal que $K[x]_{>'} = K[x]_>$ y calcular una base estándar G de J. Entonces $f \in \sqrt{I}$ si y solo si $1 \in J$, además $1 \in L(J) = L(G)$ si y solo si G contiene un elemento g con $\texttt{LM}(g) = 1$.

Ejemplo 13.5. Sea $f = x + y + z$ y $I = \langle x^5, xy^3, y^7, z^3 + xyz \rangle \subset K[x, y, z]$ un ideal. Utilizando el orden monomial *dp*, se quiere determinar si el polinomio $f \in \sqrt{I}$.
Utilizando lo expuesto antes, definimos el ideal $J := \langle x^5, xy^2, y^7, z^3 + xyz, 1 - tx - ty - tz \rangle$ una base estándar para J es $G = \{1\}$ utilizando el orden monomial *dp*. Por lo tanto $f \in \sqrt{I}$.

14. El problema de resolver ecuaciones polinomiales

En esta sección se muestra una introducción de cómo aplicar la técnica de bases de Gröbner para resolver sistemas de ecuaciones polinomiales en varias variables, esta parte se deja como motivación para futuras investigaciones, ya que se hace uso de teoría que está fuera de los objetivos de esta investigación.

Ejemplo 14.1. Consideremos las siguientes ecuaciones:

$$\begin{aligned} x^2+y^2+z^2 &= 1 \\ x^2+z^2 &= y \\ x &= z \end{aligned}$$

en $\mathbb{C}^3$. Estas ecuaciones determinan el ideal $I = \langle x^2+y^2+z^2-1, x^2+z^2-y, x-z\rangle \subset \mathbb{C}[x,y,z]$, se quieren encontrar todos los puntos en $V(I)$. La Proposición 4.12 implica que podemos calcular $V(I)$ utilizando cualquier base de I. Entonces, veamos qué sucede cuando usamos una base de Gröbner.

Una base de Gröbner reducida para I con respecto al orden lexicográfico es:

$$\begin{aligned} g_1 &= x-z \\ g_2 &= -y+2z^2 \\ g_3 &= z^4+(1/2)z^2-1/4 \end{aligned}$$

Si examinamos los polinomios de la base, se observa que el polinomio g_3 depende solo de la variable z. Para encontrar sus raíces, resolvemos para z^2 mediante la fórmula cuadrática y tomamos raíces cuadradas, obteniendo cuatro valores para z:

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5}-1}$$

Cuando estos valores de z se sustituyen en las ecuaciones $g_2 = 0$ y $g_1 = 0$, esas dos ecuaciones se pueden resolver de forma única para las variables y y x, respectivamente. Las soluciones son:

$$x_1 = z_1 = \frac{1}{2}\left(\sqrt{\sqrt{5}-1}\right) \quad \text{y} \quad y_1 = \frac{1}{2}\left(\sqrt{5}-1\right)$$

$$x_2 = z_2 = \frac{1}{2}\left(\sqrt{-\sqrt{5}-1}\right) \quad \text{y} \quad y_2 = \frac{1}{2}\left(-\sqrt{5}-1\right)$$

$$x_3 = z_3 = -\frac{1}{2}\left(\sqrt{\sqrt{5}-1}\right) \quad \text{y} \quad y_3 = \frac{1}{2}\left(\sqrt{5}-1\right)$$

$$x_4 = z_4 = -\frac{1}{2}\left(\sqrt{-\sqrt{5}-1}\right) \quad \text{y} \quad y_4 = \frac{1}{2}\left(-\sqrt{5}-1\right)$$

Por lo tanto, hay cuatro soluciones en total de $g_1 = g_2 = g_3 = 0$, dos reales y dos complejas. Como $V(I) = V(g_1, g_2, g_3)$ por la Proposición 4.12, se han encontrado todas las soluciones de las ecuaciones originales.

El ejemplo anterior nos muestra una idea general de cómo resolver sistemas de ecuaciones y el papel importante que juega la teoría de las bases de Gröbner para resolverlos.

Conclusiones

La generalización del algoritmo de la división a un anillo en n indeterminadas, puede considerarse como una generalización imperfecta comparada con su contraparte en una variable, al perder propiedades importantes tales como unicidad del resto, unicidad del cociente, entre otras; para el caso de un orden global, permite introducir la teoría de las bases de Gröbner y recuperar algunas de las propiedades importantes al utilizar el algoritmo, tal como la unicidad del resto al dividir por una base de Gröbner.

El algoritmo de Buchberger aunque es una herramienta de gran alcance, no es suficiente cuando el orden monomial no cumple con ser un buen orden, por lo que es necesario generalizar el concepto de resto (forma normal) y recurrir al algoritmo de base estándar, que esencialmente consiste en una modificación del procedimiento de reducción de Buchberger, permitiendo obtener resultados para cualquier orden monomial.

Las bases de estándar son un componente teórico muy importante de la teoría de anillos moderna, que permite resolver una gran cantidad de problemas, como la pertenencia de un polinomio a un ideal, pertenencia de un polinomio al radical, eliminación de variables, intersección de ideales, entre otros.

Referencias

[1] M.F. Atiyah, I.G. MacDonald, and G.P. Xufré. *Introducción al álgebra conmutativa*. Publicaciones científicas y de tecnología aplicada. Reverté, 1973.

[2] O. Bachmann, G.M. Greuel, C. Lossen, G. Pfister, and H. Schönemann. *A Singular Introduction to Commutative Algebra*. Springer Berlin Heidelberg, 2012.

[3] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015.

[4] W. Decker and G. Pfister. *A First Course in Computational Algebraic Geometry*. AIMS Library of Mathematical Sciences. Cambridge University Press, 2013.

[5] K. Ueno and K. Nomizu. *An Introduction to Algebraic Geometry*. Translations of mathematical monographs. American Mathematical Society, 1997.